IBM® WebSphere Commerce®

访问控制指南

版本 5.4

IBM® WebSphere Commerce®

访问控制指南

版本 5.4

注意:

在使用本资料及其支持的产品之前，请务必阅读“声明”部分中的信息。

第一版（2002 年 3 月），第二次修订（2002 年 4 月）

本版本适用于下列产品:

IBM WebSphere Commerce 商务版 Windows NT 和 Windows 2000 版版本 5.4

IBM WebSphere Commerce 商务版 AIX 版版本 5.4

IBM WebSphere Commerce 商务版 Solaris Operating Environment Software 版版本 5.4

IBM WebSphere Commerce Studio 商务开发者版 Windows NT 和 Windows 2000 版版本 5.4

IBM WebSphere Commerce 专业版 Windows NT 和 Windows 2000 版版本 5.4

IBM WebSphere Commerce 专业版 AIX 版版本 5.4

IBM WebSphere Commerce 专业版 Solaris Operating Environment Software 版版本 5.4

IBM WebSphere Commerce Studio 专业开发者版 Windows NT 和 Windows 2000 版版本 5.4

以及上面所列产品的所有后续发行版和修订版，直到在新版本中另有声明为止。确认您正在使用本产品级别的正确版本。

通过您当地的 IBM 代表或 IBM 分部可订购出版物。以下地址不备有出版物。

IBM 欢迎您提出宝贵意见。您可以将意见通过以下任何一种方式发送给我们:

1. 发送电子邮件到下面列出的网络地址。如果需要答复，请在电子邮件中提供您完整的网络地址。

   因特网: torrcf@ca.ibm.com
2. 通过邮件寄往以下地址:

   IBM Canada Ltd. Laboratory
   B3/KB7/8200/MKM
   8200 Warden Avenue
   Markham, Ontario, Canada L6G 1C7

当您发送信息给 IBM 后，即授予 IBM 非专有权，IBM 可以它认为合适的任何方式使用或分发此信息，而无须对您承担任何责任。

在何处查找信息

WebSphere Commerce™ 具有描述完整的电子交易解决方案的联机和硬拷贝信息。并且，与 WebSphere Commerce 捆绑在一起的软件产品提供了进一步信息，这些信息描述了软件的特定功能部件和功能。此部分对于何处查找各种类型的信息提供了简要概述。

WebSphere Commerce 出版物

- 《*IBM™® WebSphere Commerce 基础版本 5.4*》
- 《*IBM™ WebSphere Commerce 程序员指南版本 5.4*》
- 《*IBM™ WebSphere Commerce Windows NT™® 和 Windows™® 2000 版快速入门，版本 5.4*》
- 《*IBM™ WebSphere Commerce Studio 商务开发者版 Windows NT™ 和 Windows™ 2000 版安装指南，版本 5.4*》
- 《*IBM™ WebSphere Commerce 迁移指南版本 5.4*》

关于对这些出版物的更新，请参阅以下 Web 地址:
`http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html`

WebSphere Commerce 联机帮助

WebSphere Commerce 联机帮助由可使用 Web 浏览器查看的联机信息组成。还将联机信息的摘要编译到相关主题区域 PDF（可移植文档格式）文档中。

可使用以下地址从运行 Internet Explorer 版本 5.5 或更高版本的 Web 浏览器访问联机帮助:

`http://`*`host_name`*`/wchelp/`，其中 *`host_name`* 是 WebSphere Commerce 机器的名称。

并且，在 Windows 上，可如下从**开始**菜单访问帮助:

开始 – > 程序 – > IBM® WebSphere Commerce– > 文档

Web 上的进一步信息

支持

要查找支持信息（包括新闻组、FAQ、技术注解、疑难解答信息和下载），请访问以下 Web 地址:

Business

`http://www.ibm.com/software/webservers/commerce/wc_be/support.html`

Professional

`http://www.ibm.com/software/webservers/commerce/wc_pe/support.html`

软件合作伙伴

有许多软件合作伙伴提供了增强 WebSphere Commerce 的产品和服务。关于这些合作伙伴的信息，请访问以下 Web 地址:
`http://www.ibm.com/software/webservers/commerce/community` 并单击 “Software Developers” 链接。

Redbooks™™

要查找更多高级技术信息，请访问 Redbooks Web 站点（位于 `http://www.ibm.com/redbooks`）并搜索 WebSphere Commerce。

开始之前

《*IBM WebSphere Commerce 版本 5.4 访问控制指南*》旨在面向希望管理对其 WebSphere Commerce 站点的访问的站点管理员。商店管理员可为他们担当该角色的组织实体执行有限的访问管理。

本指南提供了对访问管理的介绍，包括对以下内容的概述: 组织和用户、访问控制策略及其层次结构和关系，以及随产品封装的缺省策略。本指南还提供了范围广泛的方案以帮助希望对其现有的策略进行基本定制的站点管理员，并且提供了用于测试已修改策略和为性能作考虑的指南。

本书分为以下部分:

『**第 1 章: 概述**』对 WebSphere Commerce 的访问控制系统的关键功能部件的简要概述，以及对自 WebSphere Commerce 的前发行版以来所作更改的描述。

『**第 2 章: 入门**』对访问管理的介绍，包括如何定义组织和用户、组织和用户如何与访问控制策略相关、访问控制策略的基本结构，以及如何阅读和识别 WebSphere Commerce 管理控制台中 XML 格式的策略的关键部分。

『**第 3 章: 访问控制概念**』关于组织及其子组织的结构、如何授予用户对系统的访问权、对缺省角色的描述以及相关术语的概念性信息。

『**第 4 章: 定制访问控制策略**』对于资源级别和基于角色的策略及其关系和层次结构的深入研究。

『**第 5 章: 访问控制方案**』一系列不同的方案，说明如何对随 WebSphere Commerce 附带的缺省访问控制策略进行基本修改。

『**第 6 章: 使用 XML 文件定制访问控制策略**』对使用 XML 定制访问控制策略各部分的研究。包含将策略信息从 XML 文件装入到访问控制数据库表以及将策略信息从访问控制数据库表抽取到 XML 文件的循序渐进过程。

『**附录: 缺省访问控制策略表**』安装时装入系统的所有缺省访问控制策略的完整列表。

假定

本指南假定您已在站点上成功安装和配置了 IBM WebSphere Commerce 版本 5.4，且您对 WebSphere Commerce 管理控制台工具具有站点管理员访问权。商店管理员能够使用 WebSphere Commerce 管理控制台工具管理其组织实体的访问控制策略，但是不能管理策略的组成部分（例如操作组和资源组），因为这些组成部分是系统范围的实体。

本指南还假定您的系统符合运行 WebSphere Commerce 的所有软件和硬件需求。关于安装 WebSphere Commerce（包括先决条件）的更多信息，请参阅《*IBM WebSphere Commerce 版本 5.4 安装指南*》。

本书中使用的约定

本书使用以下约定:

黑体字 指示图形用户界面（GUI）控件，例如字段名、按钮或菜单选项。

等宽字 指示完全按显示原样输入文本以及目录路径的示例。

斜体字 用于强调字以及要替换为您自己的值的变量。

表示可帮助您完成任务的附加信息。

NT 指示特定于 WebSphere Commerce Windows NT ® 版的信息。

2000 指示特定于 WebSphere Commerce Windows ® 2000 版的信息。

AIX 指示特定于 WebSphere Commerce AIX® ® 版的信息。

Solaris 表示特定于 WebSphere Commerce Solaris Operating Environment software 版的信息。

Linux 表示特定于 WebSphere Commerce Linux 版的信息。

400 指示特定于 WebSphere Commerce IBM Eserver iSeries™™ 400® ®（以前称为 AS/400® ®）版的信息

Professional 表示特定于 WebSphere Commerce 专业版的信息。

Business 表示特定于 WebSphere Commerce 商务版的信息。

目录

第 1 章 访问控制简介

电子交易的角色不仅改变了公司做生意的方式，而且显著地增加了公司可期望与其顾客和业务伙伴建立的关系的种类。对于将提高的价值提供给现有的顾客，以及为渴望从因特网的能力和增加的效率中得益的新顾客铺平道路来说，Web 是关键因素。当获得在 Web 上做生意的明显优势和增加顾客群的巨大潜力的同时，也带来了在维护高度安全环境、授权适当的交易以及简化工作过程时的管理业务流程和贸易模式的挑战。

访问控制的特点是通过基于用户活动及其对于产品和服务的业务关系而管理用户参与系统的方式，来监视其工作过程的能力。例如，您可能仅希望已注册到站点的顾客才能查看商店中的拍卖产品并对这些拍卖产品投标。类似地，您可能授权图形设计者定制您的商店页面，但是您可能限制他们不能管理产品目录的实际内容。

WebSphere Commerce 通过包含在实例创建时自动装入到系统的两百多个缺省访问控制策略，提供了用于访问管理的合适工具。这些策略致力于您的业务所需的许多典型访问控制需求，甚至可以定制以适合您自己的电子交易解决方案。

管理对电子市场中活动的访问权是保护公司的金融资产和资源的不可或缺的组成部分，它用于确保站点的已核准成员之间的安全商务交易，以及验证在线运作的合法性。访问控制在电子交易环境中变得格外关键，在这里，对您的业务的切入点很大程度上受到通过 Web 而开始的顾客关系的影响。

WebSphere Commerce 版本 5.4 中的新功能

关于在 WebSphere Commerce 中添加的其它新功能和增强的列表，请参阅《*IBM WebSphere Commerce 版本 5.4 新功能指南*》。

增强的用户界面

除了可从管理控制台的“访问管理”菜单访问策略编辑页面之外，WebSphere Commerce 现在还提供了用于查看策略及其相关操作组、访问组和资源组的附加查看器页面。策略查看页面无缝地集成到管理控制台用户界面中，且能够使用已添加到现有的策略编辑页面中的按钮来访问这些页面。

细粒度控制

前发行版的 WebSphere Commerce Suite 提供了“粗粒度”访问控制，它使您可以定义谁可调用系统中的什么功能。例如，在前发行版的 WebSphere® Commerce Suite 中，可能使用了粗粒度访问控制允许买方通过调用“取消订单”功能来取消订单。

现在在 WebSphere Commerce 中，还通过定义谁可对哪个商业对象实例（也称为“资源”）调用什么功能，提供了“细粒度”访问控制能力。在同一示例中，您不仅能够允许买方取消订单，还可以限制买方仅对其自己的订单（而不是其它用户的订单）调用取消订单功能。

所添加的细粒度访问控制能力与粗粒度访问控制组合在一起，提供了更大范围的访问管理以及对用户在站点上受允许执行活动进行细微调整的能力。

独立管理的组件

在前发行版的 WebSphere Commerce Suite 中，细粒度的访问控制是构建到系统代码中的，这要求更改代码以建立资源级别的策略定制。

现在，WebSphere Commerce 通过修改 XML 文件中的访问控制策略（可使用包含在管理控制台工具中的策略查看器界面或使用标准的文本编辑器来修改这些文件），具体化了粗粒度和细粒度访问控制。

因为现在粗粒度和细粒度访问控制策略是独立于产品代码提供的，因此调整访问管理以适合业务需求则要求更改包含在 XML 文件中的信息，而不是更改产品代码。

适应新的业务过程

在今天瞬息万变的市场中，快速定制业务环境的能力在维持竞争力、适合市场变化以及适应新的业务过程中扮演了重要角色。通过将粗粒度和细粒度策略具体化，希望对系统访问的各个级别作的更改可通过修改策略（而不是通过定制代码）快速而容易地完成。更为重要的是，通过将先前仅对雇佣服务团队提供的细粒度策略展示出来，您的组织现在可自己来执行对策略的许多基本修改，减少了为 Web 站点定制 WebSphere Commerce 的附加成本。

可伸缩性

因为组织随时间而变化和成长，因此对系统的访问必须也适应这些变化。随着新雇员的加入，更改了角色和责任，他们的访问级别必须作相应更改以允许其执行要求其执行的活动。然而跟踪每个单个用户活动的任务可能是非常消耗时间且十分困难的，甚至是不可行的。

然而，使用 WebSphere Commerce，可以通过使用访问组（其成员资格是通过一系列共享的*属性*定义的）而不是通过其身份，来隐式地管理授予系统访问权。对用户指定了角色，并根据其角色给予访问权。例如，用户 A、B 和 C 可能指定为“买方”角色，且可以使用适当的访问控制策略，给予所有买方取消未装运的订单的能力。如果用户 A 离开了组织，则可删除用户 A 的角色信息，而对于用户 B 和 C 来说，将取消订单与买方角色相关联的访问控制策略保持不变。

隐式地授予对系统的用户访问的能力是用于管理活动的强有力方法，且需要少得多的时间和精力。此外，管理访问控制所需的精力大小取决于希望更改的策略数，而不是系统大小、属于组织的用户数或所执行业务活动的级别。运行在系统上的访问控制策略对小型和大型组织都可适用。因此，运行在 WebSphere Commerce 上的访问控制策略的可伸缩性使您的公司能够继续变化和成长，而不妨碍运作的结构或效率。

访问控制对您意味着什么

访问控制使您能够管理业务工作流程并确保用户仅执行与其角色和责任相应的那些活动。WebSphere Commerce 不仅提供了现成可用的缺省策略，而且还提供了用于定制策略以适应业务需要的工具和功能。

下表仅概括了几个示例用以说明简单的修改是怎样定制对业务环境的访问的。

缺省情况下允许用户执行的操作	定制后允许用户执行的操作
顾客可以自注册。	只有卖方管理员才可以注册新顾客。

买方可以显示他们创建的 RFQ。	如果 RFQ 导致了签署合同，则只有卖方才可显示 RFQ。
如果订单处于未决状态，则只有顾客才能取消其创建的订单。	如果产品总价小于 ￥1000，则客户服务代表也可以取消处于未决状态的订单。
创建订单的人可以修改该订单。	只有来自买方组织的具有“购买方”角色的用户才能修改已创建的订单。
客户代表可以显示所有帐户。	客户代表仅可显示活动的帐户。
具有“后勤部经理”角色的雇员可以创建和修改实现中心。	具有“后勤部经理”角色的雇员可以创建但是不能修改实现中心。

在下一章中，将详细探讨如何创建组织和用户以及访问控制策略。

第 2 章 入门

在前一章中，您已了解了访问控制在电子交易中所扮演的重要角色，以及它在提高通过 Web 开展业务的效率和可靠性方面的重要优点。

在本章中，将讨论 WebSphere Commerce 中访问管理的基本点（例如定义组织和用户），以及访问控制策略如何用于管理这些组织及其用户在系统中执行的活动。在简要地概述了设置组织和用户将执行的步骤之后，将深入地探讨访问控制策略以及它们在 WebSphere Commerce 中的作用，并对其中一个访问控制策略作详细研究。

本章分为以下部分:

- 定义组织和用户
- 理解访问控制
- 如何着手使用访问控制？

定义组织和用户

对于站点管理员，安装和配置 WebSphere Commerce 之后的首要任务之一就是设置和管理对电子交易站点的访问。这包括创建将参与站点的组织以及定义将成为这些组织的成员的用户。

在某些情况下，加入站点的组织可以是买方组织，或者，也可以让与您的业务有“商家到消费者”关系的顾客注册到站点。无论您是管理“商家到商家”还是“商家到消费者”站点，定义站点的组织结构是管理成员对您的系统所拥有的访问类型的重要步骤。

在本部分中，将提供定义站点的结构所需要执行的高级步骤。如果已设置了组织和用户，则可跳至有关访问控制的下一部分。否则，请使用本部分作为前期规划的指南。

关于创建组织、用户和角色的更多详细信息，请参阅可从以下“Technical Library”页面获得的联机帮助:

Business

```
http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html
```

Professional

```
http://www.ibm.com/software/webservers/commerce/wc_pe/lit-tech-general.html
```

还建议您参阅《*IBM WebSphere Commerce 基础指南版本 5.4*》。

定义卖方组织

通常，卖方组织是在 WebSphere Commerce 站点上拥有一个或多个商店的组织。卖方组织还可以拥有子组织或部门，这些子组织或部门也可拥有一个或多个商店。例如，销售时装商品的样本商店“流行时尚”可能拥有女装分支和男装分支，它们分别拥有独立的网上商店。

现在假定您正在设置不拥有任何子组织的卖方组织。要设置卖方组织，这里有一个您需要执行步骤的大致概括:

1. 创建新组织。创建新组织时，将为该组织创建简要表，包括组织名称、描述、地址和联系人以及组织类型。
2. （可选）定义卖方组织内的哪些任务需要核准，例如订单处理或用户注册。此步骤仅对于“商家到商家”站点是必需的。关于核准文档，请参阅产品联机帮助。
3. 为新组织指定角色。一个组织仅可担当已指定给其父组织的角色。因为根组织是所有其它组织的上级组织，因此必须对它指定所有可能的角色。WebSphere Commerce 提供了一组缺省角色，您可立即开始使用这些角色。因为您创建的是卖方组织，因此您可能指定的典型角色包括卖方管理员、商店管理员、商店开发者和卖方等。请参阅第 11 页的『角色』以获取缺省角色列表。
4. 创建用户。与组织相似，将为每个用户创建简要表，包括用户名、联系信息和指定给该用户的角色。指定角色时，您将从前一步指定给组织的角色的列表中选择角色。

上面概述的所有步骤都可由站点管理员通过管理控制台中的“访问管理”菜单执行。

注: 在 WebSphere Commerce 专业版中，只能有一个卖方组织。

定义买方组织

如果正在运行“商家到商家”站点，则可以有属于站点的一个或多个买方组织。（如果正在运行“商家到消费者”站点，则让单个买方注册到缺省组织）。在确立了哪些公司将参与到与站点的购买关系中之后，则必须为每个公司创建买方组织。您可拥有所需数量的买方组织。

买方组织在结构上与卖方组织类似。与卖方组织相似，买方组织也可拥有子组织或部门，这些子组织或部门表示该组织的不同购买活动。

现在假定您的买方组织不拥有任何子组织。要设置买方组织，这里是您需要执行步骤的概括:

1. 如您在创建卖方组织时所做的，创建新组织并按需要定义可核准的任务。再次说明，定义可核准的任务仅对于“商家到商家”站点是必需的。
2. 为新买方组织指定角色。因为您现在创建的是买方组织，因此可能指定的典型角色包括买方管理员、买方（购买方）、买方核准员等。
3. 创建用户并为他们指定角色。指定角色时，您将从前一步指定给买方组织的角色的列表中选择角色。
4. 对希望添加到站点的每个买方组织重复整个过程。

再次说明，上面概述的所有步骤都是通过管理控制台中的“访问管理”菜单执行的。

注: 在 WebSphere Commerce 专业版中，所有顾客都属于缺省组织。

理解访问控制

定义完将要参与电子交易站点的组织和用户之后，可通过一组策略（称为*访问控制*的一个过程）来管理其活动。在下一部分中，将探讨访问控制策略及其基本结构。

什么是访问控制策略?

访问控制策略是一个规则，它描述了授权哪组用户在站点上执行特定活动。这些活动的范围可以包括从注册到管理拍卖、到更新产品目录和对订单授权核准，以及运作和维护电子交易站点所需的所有数以百计的其它活动。

策略的作用是授予用户对站点的访问权。除非已通过一个或多个访问控制策略来授权用户执行其责任，否则用户对站点的任何功能都不具有访问权。

访问控制策略如何工作?

访问控制策略由四个部分组成: 访问组、操作组、资源组和可选关系。

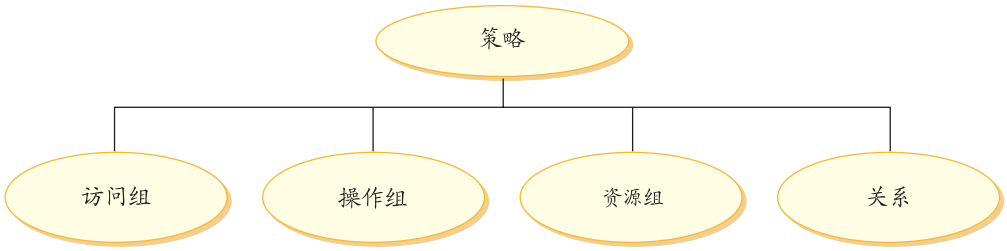
*访问组*是对站点上的一组功能共享公共访问权的一组用户。访问组通常包含共享公共属性（例如同一角色、部门或技能集）的用户。

*操作组*是指可对同一资源执行的一组操作。通常，操作组包含与公共业务区域关联的操作，或站点上相关的一组活动。

*资源组*包含受控于策略的资源。资源组可能包含诸如合同或一组相关命令之类的商业对象。

在某些情况下，只有对某一资源具有关系的用户才能对该资源执行操作。例如，可能只允许创建合同的那些用户修改该合同。

图 1. 访问控制策略的四个部分



这四个部分一起，通过指定以下内容定义了 WebSphere Commerce 中的策略: 用户、他们可执行的操作、所执行操作的商业对象或命令组，以及（可选）用户与资源组的关系。

关于访问组、操作组、资源组和关系的更多详细信息，请参阅第 9 页的第 3 章，『访问控制概念』。

如何着手使用访问控制?

在一些情况下，您什么也不用做！这是因为 WebSphere Commerce 中的缺省策略基于系统中的典型用户以及他们所执行的与他们在组织中角色相关联的活动，提供了访问控制的基本结构。这些策略涵盖了广阔范围的公共业务活动，包括成员资格、订单创建和处理、工作流核准以及贸易（例如拍卖、报价请求和合同）。定义了组织和用户之后，可按所提供的原样使用缺省策略，或者定制它们以符合公司的个别需求。

但是，在能够决定是要使用缺省策略还是定制它们之前，理解它们在 WebSphere Commerce 中的概况是很重要的。关于对缺省策略的详细深入研究，请参阅第 27 页的『详细探讨一个策略』。

第 3 章 访问控制概念

WebSphere Commerce 将访问控制视为验证用户或应用程序是否具有访问资源的足够权限的过程。本部分描述了 WebSphere Commerce 访问控制的若干方面的详细信息。

WebSphere Commerce 中的访问控制是使用访问控制策略实现的。访问控制策略是描述哪组用户可对某组资源执行某组操作的规则。WebSphere Commerce 提供了一组缺省的访问控制策略。这些缺省的访问控制策略以 XML 格式指定，且设计用来致力于电子交易站点需要的许多典型的访问控制要求。为了理解 WebSphere Commerce 的访问控制组件，首先必须理解电子交易站点典型的组织层次结构。

组织层次结构

WebSphere Commerce 成员子系统中的用户和组织实体被组织到层次结构中。此层次结构仿照典型的组织层次结构，以条目表示组织和组织单位，而在叶节点中以条目表示用户。层次结构在顶部包含称为*根组织*的人为组织实体。所有其它组织实体和用户都是此根组织的后代。在根组织下可有一个卖方组织和若干个买方组织；所有这些组织可在其下拥有一个或多个子组织。买方或卖方管理员是组织的领导人，他们负责维护其组织。在卖方组织这一方，每个子组织可在其中拥有一个或多个商店。商店管理员负责维护商店。以下图表显示了“商家到商家”电子交易站点的组织层次结构。

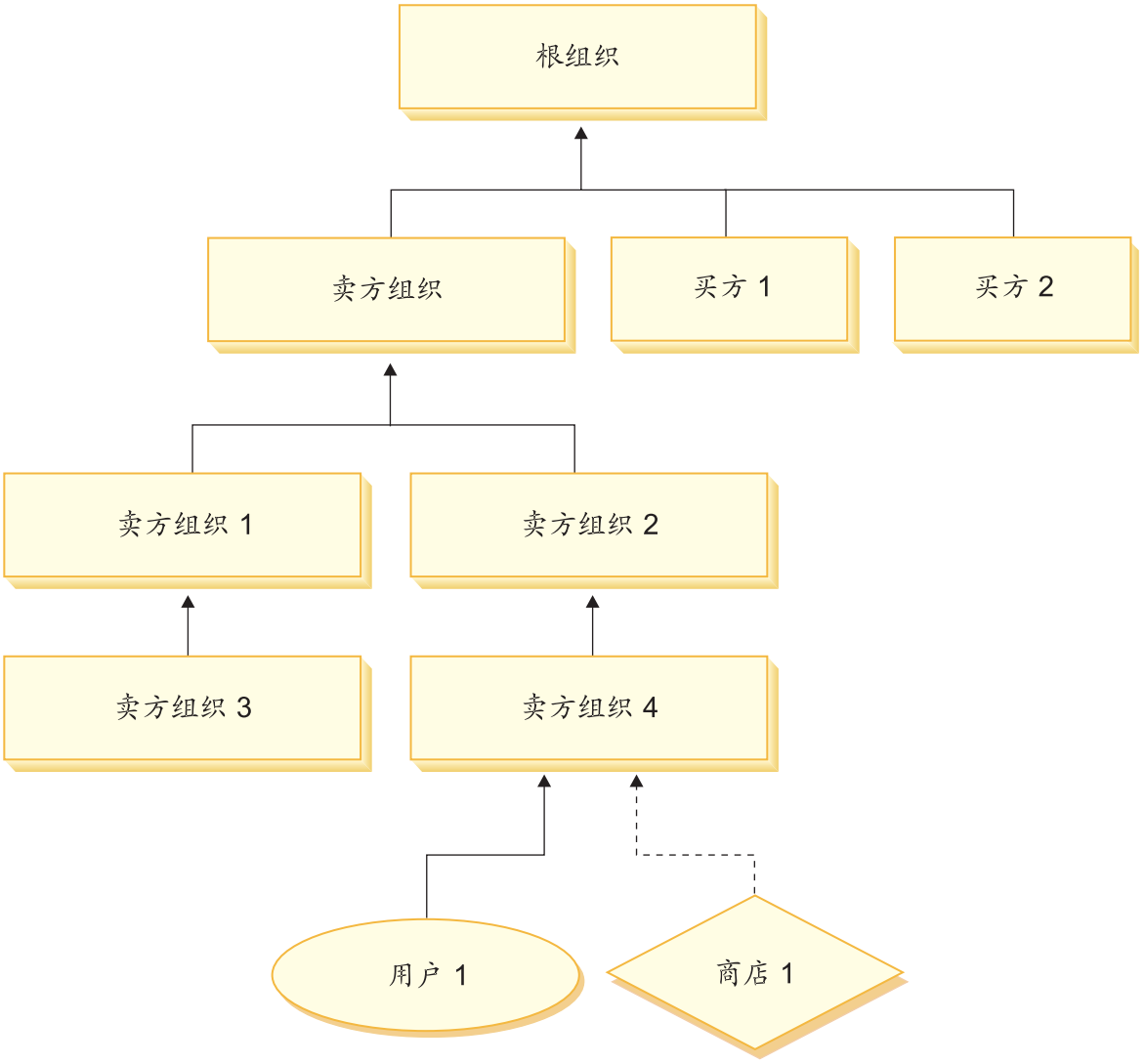


图 2. “商家到商家”站点的组织层次结构

根组织

根组织位于组织层次结构的顶部。站点管理员具有超级用户访问权，可执行 WebSphere Commerce 中的任何操作。站点管理员安装、配置和维护 WebSphere Commerce 及其关联的软件和硬件。此角色通常控制访问和授权（即创建并指定成员给适当的角色）以及管理 Web 站点。站点管理员可将角色指定给用户，并指定用户对其担当该角色的组织。站点管理员必须将密码指定给每个管理员以确保只有经授权方才能访问机密信息。这提供了一种方法来控制关键责任，例如更新产品目录或核准报价请求（RFQ）。

注: 用户可以在其父组织之外的组织中担当角色。

在 WebSphere Commerce 站点中，有一个卖方组织。在“商家到商家”站点中，还有一个或多个买方组织。站点管理员可定义卖方组织（拥有商店）的访问控制策略以及从商店购买的每个组织的访问控制策略。在“商家到消费者”站点中，没有买方组织。将“商家到消费者”的顾客建模为缺省组织的成员。

组织（卖方）

在“商家到商家”和“商家到消费者”站点中，站点管理员创建一个顶级卖方。在此卖方组织下，可创建其它子组织或组织单位。所有这些销售方组织实体都可拥有一个或多个商店。然后站点管理员定义卖方组织的所有特殊的访问控制策略，并指定卖方管理员来管理该组织。卖方管理员根据与该组织相关的访问控制策略，对用户进行注册并将不同的角色指定给他们以满足组织的商务需要。

卖方管理员的责任总结如下:

- 创建可拥有商店的子组织。可选地，定义组织内哪些过程需要核准。仅在“商家到商家”站点中需要该步骤。
- 将角色指定给子组织。
- 创建用户。
- 将角色指定给用户。

组织（买方）

在“商家到商家”站点中，站点管理员根据商务需要创建一个或多个买方组织。然后站点管理员定义买方组织的所有特殊的访问控制策略，并指定买方管理员来管理买方组织。买方管理员根据与该组织相关的访问控制策略，对用户进行注册并将不同的角色指定给他们以满足组织的商务需要。

买方管理员的责任总结如下:

- 创建并管理买方组织内的子组织。可选地，定义组织内哪些过程需要核准。仅在“商家到商家”站点中需要该步骤。
- 将角色指定给子组织。
- 创建用户。
- 将角色指定给用户。

注: 如有必要，站点管理员可修改和管理买方组织的访问控制策略。关于站点管理员任务的更多信息，请参阅第 12 页的『站点管理员』。

角色

如上所述，WebSphere Commerce 提供了一组缺省的角色。站点管理员在将用户指定为特定角色之前，必须将这些特定角色指定给每个组织。组织仅可拥有已指定给其父组织的那些角色。类似地，用户仅可拥有已指定给其父组织的那些角色。

WebSphere Commerce 中的所有角色，其作用范围都限于某个组织。例如，用户担当组织 X 的“产品经理”角色。还必须将“产品经理”角色指定给该用户的父组织本身。这样则可以设置访问控制策略，以使该用户仅可执行组织 X 及其子组织的上下文中的产品管理操作。

注: 将角色指定给用户和组织是在 MBRROLE 表中完成的。

随 WebSphere Commerce 附带的缺省角色可分为以下类别:

- 站点操作
- 站点和内容开发
- 市场营销管理

- 产品管理
- 销售管理
- 后勤和运作管理
- 组织管理

站点操作

WebSphere Commerce 支持以下技术操作角色:

- 站点管理员
- 商店管理员

站点管理员

站点管理员安装、配置和维护 WebSphere Commerce 及关联的软件和硬件。管理员对系统警告、提醒和错误作出响应，并诊断和解决系统问题。此角色通常控制访问和授权（创建并指定成员给适当的角色）、管理 Web 站点、监视性能以及管理负载均衡任务。站点管理员还可能负责为开发的不同阶段（例如测试、登台和生产）建立和维护若干服务器配置。此角色还处理关键系统备份以及解决性能问题。

商店管理员

商店管理员管理商店有用资源，并更新和发布对税款、装运和商店信息的更改。商店管理员还可管理组织的访问控制策略。商店管理员通常是商店开发组的领导，是该组中具有发布商店归档文件权限的唯一角色（站点管理员也可发布商店归档文件）。商店管理员通常了解 Web，且透彻地了解商店商务过程。

站点和内容开发

WebSphere Commerce 支持“商店开发者”站点和内容开发角色。

商店开发者

商店开发者创建 Java™ Server Pages 文件和所有必需的定制代码，并可修改 WebSphere Commerce 包含的所有标准功能。一旦创建了商店归档文件，则商店开发者有权对其作手工更改，或通过使用“商店简要表”笔记本以及“税款”和“装运”笔记本对其进行更改。他们不具有将商店归档文件发布到 WebSphere Commerce Server 的权限。

后勤和运作

WebSphere Commerce 支持以下后勤和操作管理角色:

- 后勤部经理
- 业务经理
- 收货员
- 退货管理员
- 提货装货员

后勤部经理

Business 后勤部经理（有时称为装运经理）管理和协商从递送者至仓库以及至个人顾客的成批货运或装运。此角色负责确保公司以最合理成本使用最佳装运商以满足公司战略。装运是客户服务的重要方面，且可能是网上业务的关键成功因素。

业务经理

B2C 此角色管理订单处理，确保正确实现了订单、接收了支付以及装运了订单。业务经理可搜索顾客订单、查看详细信息、管理订单信息以及创建和编辑退货。

提货装货员

提货装货员从实现中心提出产品，并包装产品以便装运给顾客。提货装货员还管理提货单和装货单，这些单据用于在订单实现期间确认产品的装运。

收货员

收货员在实现中心接收库存，跟踪订购产品的预期库存记录和特别接收，以及接收由于顾客退货而退回的产品。

退货管理员

退货管理员管理对退回产品的处理。

- 列出退货
- 列出退回产品
- 处理退回产品

产品管理

WebSphere Commerce 支持以下产品管理角色:

- 买方（销售方）
- 类别经理
- 产品经理或销售部经理

买方（销售方）

买方购买商品以供销售。买方处理与供应商的关系并进行协商以便以优惠的条款（例如有关交付和支付选项的条款）获取所需的产品。买方可设置价格。库存由买方管理以确定购买数量，并确保正确补充了库存。

类别经理

类别经理通过创建、修改和删除类别来管理类别层次结构。类别层次结构组织商店提供的产品或服务。类别经理还管理产品、预期库存记录、供应商信息、库存和退货原因。

产品经理 / 销售部经理

Business 销售部经理或 B2C 产品经理在网上商店中跟踪顾客购买、建议折扣并确定显示、定价和销售产品的最佳方式

- 执行类别经理的所有任务
- 执行市场部经理的所有任务

销售管理

WebSphere Commerce 支持以下商务关系管理角色:

- 销售经理
- 客户代表
- 客户服务主管

- 客户服务代表

销售经理
销售经理获得和留住顾客、达到销售预测、提供增加顾客业务的刺激、管理合同、设置定价条款、与产品经理协同工作以建立库存预测，以及与市场部经理协同工作以进行促销

客户代表
客户代表处理个人帐户以建立关系，并管理客户服务问题。可以对他们进行授权以更改合同定价、协商合同、制作简要表以及按帐户类别分析赢利能力。

客户服务主管
此角色具有对所有客户服务任务的访问权。客户服务主管管理顾客查询（例如顾客注册、订购、退货和拍卖），且有权完成客户服务代表无法访问的任务，例如核准系统拒绝的退货记录、就支付异常（例如信用卡授权失败）联系顾客。

客户服务代表
无论将在线商务设计得多好以便向顾客提供自助功能，仍将存在一些类型的顾客或是一些情况，即使是最了解 Web 的顾客也将需要个人联系。大多数在线商务提供电子邮件、传真或联系电话以供顾客获取直接服务。客户服务代表负责处理来自顾客的所有查询。

市场营销管理
WebSphere Commerce 支持“市场部经理”的市场营销管理角色。

市场部经理
市场部经理向顾客交流市场营销战略和品牌消息。此角色监视、分析和理解顾客行为。并且，市场部经理为目标销售创建或修改顾客简要表，并创建和管理竞销和促销。竞销事件规划可由商家、市场部经理和销售部经理组成的一个小组来处理。

组织管理
WebSphere Commerce 支持以下组织管理角色:

- 卖方管理员
- 买方管理员
- 买方核准员

卖方管理员
卖方管理员管理销售组织的信息。卖方管理员创建和管理销售组织内的子组织以及销售组织中的各个用户，包括指定适当的商务角色。

买方管理员
买方管理员管理购买组织的信息。他们创建和管理购买组织内的子组织并管理各个用户，包括将用户核准为买方。可能创建和管理其它购买方角色，例如买方核准员和附加的买方组织管理员。

买方核准员
买方核准员是买方组织中的个人，他在提交订单以向卖方购买之前，核准由买方下的订单。

访问控制策略

访问控制策略授予一组用户对 WebSphere Commerce 中的某组资源执行某组操作的权力。除非通过一个或多个访问控制策略经过授权，否则用户将不能访问系统的任何功能。要理解访问控制策略，您需要理解四个主要概念: 用户、操作、资源和关系。用户是使用系统的人。资源是系统中需要保护的对象。操作是用户可对资源执行的活动。关系是存在于用户和资源之间的可选条件。

访问控制策略的元素

访问控制策略由四个元素组成:

访问组 应用策略的一组用户。

操作组 由用户对资源执行的一组操作。

资源组 由策略控制的资源。资源组可包含商务对象（例如“合同”或“订单”）或一组相关命令（例如特定角色的用户可执行的所有命令）。

关系（可选）

每个资源类可具有与其关联的一组关系。每个资源可具有满足每个关系的一组用户。例如，某个策略可指定只有订单的创建者才可修改该订单。在此情况下，关系将是“创建者”，且它存在于用户和订单资源之间。

访问控制策略概念

访问控制策略授予用户对站点的访问权。除非通过一个或多个访问控制策略授权用户执行其职责，否则用户不能访问站点的任何功能。

每个访问控制策略具有以下格式:

```
AccessControlPolicy [AccessGroup,ActionGroup,ResourceGroup,Relationship]
```

访问控制策略中的元素指定: 允许属于特定访问组的用户对属于指定资源组的资源执行指定操作组中的操作，只要用户对资源满足特定关系。仅在需要时指定关系。例如，`[AllUsers,UpdateDoc,doc,creator ]` 指定所有用户都可更新文档，只要他们是文档的创建者。

以下部分描述了与访问控制关联的概念性信息和术语。

成员组

WebSphere Commerce 中的“成员”子系统使您能够创建成员组，成员组是出于各种商务原因而分类的用户组。分组可用于许多目的，例如，访问控制目的、核准目的，以及诸如计算折扣、价格和显示产品的市场营销目的。类型为“访问组”（-2）的成员组用于访问控制目的，而类型为“用户组”（-1）的成员组则用于一般用途。在 MBRGRPUSG 表中，成员组与成员组类型关联。

访问组: 类型为“访问组”（-2）的成员组用于为访问控制目的而对用户进行分组。访问组是访问控制策略的一个元素，定义为特别为访问控制目的而定义的一组用户。访问组中成员资格的条件通常基于角色、用户所属的组织或用户的注册状态。例如，称为“买方管理员”的访问组是其用户担当买方管理员角色的组。

WebSphere Commerce 包含许多缺省角色，且对应于每个角色有一个隐式引用该角色的缺省访问组。角色可用作属性以基于用户在站点中所执行活动的类型将用户添加到访问组中。例如，缺省情况下有一个称为“卖方管理员”的角色和一个称为“卖方管理

员”的对应访问组。站点管理员使用 WebSphere Commerce 管理控制台创建、维护和删除站点的访问组。买方管理员或卖方管理员使用 WebSphere Commerce 组织管理控制台对用户指定角色，或显示地对访问组指定用户。访问组可以是隐式的和／或显式的。

隐式访问组: 隐式访问组由一组条件定义。满足条件的所有人都是组成员。条件通常基于用户的角色、父组织或注册状态。定义成员组中成员资格的隐式条件在 MBRGRP 表的 CONDITIONS 列中。使用指定用户属性的隐式访问组，便于对类似用户授予访问权，而无须对个别用户作显式的指定和取消指定。它还排除了在用户属性更改时更新组成员的必要。访问组的简单准则是：包含指定了特定角色的每个人，而不管该用户在哪个组织中担任角色。复杂一些的准则是：指定只有担当特定组织的一组可能角色之一的用户才属于访问组。

显式访问组: 可以显式地向成员组中添加用户或从成员组中除去用户。可使用 MBRGRPMBR 表来完成这两种显式指定。显式访问组显式地包含指定的用户，这些用户可能共享也可能不共享公共属性。它还让您能够排除虽然满足隐式定义的组中的包含条件、但您还是要将其排除的个人。

用户组: 类型为“用户组”（-1）的成员组是由商家定义的拥有共同兴趣的一组用户。用户组类似于大型商店对其经常光顾的或优先的顾客提供的俱乐部。成为用户组的成员可使顾客拥有购买产品的折扣或其它奖励的权力。例如，如果市场调查显示高级顾客经常购买旅行书和行李包，则可将这些顾客指定为称为“高级顾客的旅行俱乐部”的成员组。类似地，可创建用户组以奖励经常光顾的顾客。

操作

通常，操作是对资源执行的动作。在控制器命令的基于角色的操作中，操作是 Execute，资源是正在执行的命令。在视图的基于角色的操作中，操作是视图的名称，资源是 com.ibm.commerce.commands.ViewCommand。对于资源级别的访问控制，操作通常映射为 WebSphere Commerce 命令，而资源通常是受保护的 EJB（Enterprise Java Bean）的远程接口。例如，控制器命令 com.ibm.commerce.order.commands.OrderCancelCmd 对 com.ibm.commerce.order.objects.Order 资源执行操作。最后，Display 操作用于激活数据 bean 资源。

站点管理员可使用 WebSphere Commerce 管理控制台将现有操作与操作组相关联，而非用于创建新操作。可通过在 XML 文件中定义新操作，然后将它们装入数据库来创建新操作。操作存储在 ACACTION 表中。

操作组

操作组是相关操作的分组。操作组的示例是 AccountManage 组，该组包含以下命令:

- com.ibm.commerce.account.commands.AccountDeleteCmd
- com.ibm.commerce.account.commands.AccountSaveCmd

只有站点管理员才可创建、更新和删除操作组。可从 WebSphere Commerce 管理控制台以及通过 XML 来完成此操作。操作组存储在 ACACTGRP 表中。在 ACACTACTGP 表中，操作与操作组相关联。

资源类别

资源类别是指需要受访问控制保护的一类资源。资源必须实现 Protectable 接口信息。资源类别是 Java 类，例如订单、RFQ 和拍卖。资源是这些类的实例。例如，由拍卖管理员 A 创建的 Auction1 是一个资源；由拍卖管理员 B 创建的 Auction2 是另一资源。这两个资源都属于资源类别：拍卖。

注: 关于 Protectable 接口的更多信息，请参阅《*IBM WebSphere Commerce 程序员指南*》。

在 ACRESCGRY 表中定义了资源类别，且出于简洁，有时也称为资源。站点管理员可使用 WebSphere Commerce 管理控制台将现有资源类别与资源组相关联。可使用 XML 创建新资源类别。

资源

资源是系统中需要保护的任何对象。例如，RFQ、拍卖、用户和订单是 WebSphere Commerce 中需要保护的一些资源。每个资源都具有所有者。资源的所有权用于确定所适用的访问控制策略。访问控制策略也具有所有者，即组织实体。策略仅适用于属于拥有该策略的相同组织实体的资源。上级组织实体所拥有的策略也适用于资源。

控制器命令资源: 对于控制器命令的基于角色的访问控制，策略经过适当构架，使 Execute 操作在控制器命令资源上执行。这些策略意在限制只有具有指定角色的用户才能执行控制器命令。这些策略的访问组通常是具有单一角色的访问组，例如，产品经理（具有产品经理角色）。这样，资源组将是产品经理可以执行的一组控制器命令。

当对控制器命令强制实施基于角色的访问控制时，必须确定命令的所有者。如果已实现了 getOwner() 方法，则通过对命令调用该方法来完成此操作。通常并未实现此方法，因此 WebSphere Commerce 运行时将通过执行以下操作之一来对此进行评估:

- 使用拥有当前处于命令上下文中的商店的组织。
- 如果在命令上下文中没有商店，则使用根组织作为所有者。

数据 bean 资源: 并非所有的数据 bean 都需要保护。在现有的 WebSphere Commerce 应用程序中，需要保护的数据 bean 已实现了必需的访问控制。在您创建新的数据 bean 时，才提出要保护什么的问题。对要保护资源的确定取决于您的应用程序。如果要显示的信息未受到对视图（该视图对应于包含数据 bean 的 JSP，即 Java Server Page）的基于角色的访问控制的充分保护，则应当直接或间接地对数据 bean 进行保护。

如果数据 bean 需要保护且可独立存在，则应当直接保护它。如果数据 bean 的存在取决于另一数据 bean 的存在，则应将它交托给另一数据 bean 保护。应直接保护的数据 bean 的示例是 Order 数据 bean。应间接保护的数据 bean 的示例是 OrderItem 数据 bean，因为没有 Order 数据 bean，它就无法存在。关于如何保护数据 bean 资源的更多信息，请参阅《*WebSphere Commerce 5.4 程序员指南*》。

数据资源: 数据资源是指可操纵的商务对象，例如拍卖、订单、RFQ 和用户。通常在企业 bean 级别对它们进行保护，但是可以保护任何的类，只要该类实现 Protectable 接口。通过使用资源级别的访问控制检查来保护数据资源。完成此操作的常见方式是通过返回控制器命令或任务命令的 getResources() 方法中的数据资源。关于更多信息，请参阅《*WebSphere Commerce 5.4 程序员指南*》。

资源组

资源组标识一组相关资源。资源组可包含商务对象，例如合同或一组相关命令。在访问控制中，资源组指定访问控制策略授权访问的资源。

ACRESGRP 表中定义了资源组。站点管理员可使用 WebSphere Commerce 管理控制台或使用 XML 来管理资源组以及将资源与资源组相关联。

隐式资源组: 隐式资源组定义与某组属性相匹配的资源。这些属性之一必须是 Java 类名。其它属性可包含状态、商店标识、价格等。例如，您可创建包含了处于未决状态（ORDERS.STATUS=P）的所有订单的隐式资源组。当资源共享 Java 类名之外的公共属性时，隐式资源组通常用于对将用在资源级别的策略中的那些资源进行分组。

隐式资源组是使用 ACRESGRP 表的 CONDITIONS 列定义的。可使用 WebSphere Commerce 管理控制台创建简单的隐式资源组。可使用 XML 创建越来越复杂的组。

显式资源组: 显式资源组是通过将一个或多个资源类别与某个资源组相关联而指定的。这种关联是在 ACRESGPRES 表中完成的。通过列出资源类别的 Java 类名而显式地向组添加资源类别，使您能够对可能不一定共享公共属性的个别资源进行分组。

关系

每个资源可能具有与之相关联的某类关系以及满足每个关系的一组成员。例如，所有资源都具有关系*所有者*，资源的所有者满足该关系。其它关系可包含文档的接收方和订单的创建者。这些资源关系在确定谁可对资源的特定实例执行某些操作时是很重要的。例如，文档的创建者可能不能够删除它，但是也许审计人员可以。类似地，复查者可能仅能够读取和核准文档，但是不能转发它或执行其它操作。

关系存储在 ACRELATION 表中，也可以选择在访问控制策略中作出指定，方法是通过使用 ACPOLICY 表的 ACRELATION_ID 列。当评估一个需要实现用户和资源之间关系的策略时，将对该资源调用 fulfills(Long Member, String relationship) 方法来对此作评估。将这些关系与关系组作比较时，有时也将这些关系称为简单关系。

关系组: 访问控制策略可指定用户必须对所访问的资源满足特定关系，或者策略可指定用户必须满足关系组中所指定的条件。大多数情况下，一个关系已足够。然而，如果需要更为复杂的关系，则可使用关系组。关系组允许指定多个关系，以及一个关系链。这两者都是通过使用关系链构造而完成的。关系链是可表达简单关系（直接存在于用户和资源之间）、也可用于表达用户和资源之间的一系列关系的一种构造。例如，为了表达用户必须具有组织中的一个角色，而该组织对资源具有除所有者关系之外的其它关系，则必须使用关系组。在此示例中，用户和组织之间存在角色关系，而组织和资源之间也存在关系。

将关系与关系组作比较: 大多数情况下，关系的使用应当满足应用程序的访问控制要求，因为概念上，大多数关系直接存在于用户和资源之间。例如，策略可声明用户必须是资源的创建者。然而，如果需要指定多个关系，则应当使用关系组。例如，策略可声明用户必须是资源的创建者或提交者。

还需要关系组来表达用户和资源之间的关系链。在关系链中，用户和资源之间不存在直接关系，例如，用户属于由订单所指定的买方组织。在此情况下，用户与组织之间具有子女关系，而该组织与订单之间具有购买关系。

关系链: 每个关系组都由一个或多个 RELATIONSHIP_CHAIN 开放条件组成，这些条件按 andListCondition 或 orListCondition 元素进行分组。关系链是一个或多个关系的序列。关系链的长度取决于其所包含关系的数目。这可以通过检查关系链的 XML 表示法中 <parameter name= "X" value="Y"/> 条目的数目而确定。以下是长度为 1 的关系链的示例。

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

对于长度为 1 的关系链， <parameter name="Relationship" value="something"> 元素指定用户和资源之间的直接关系。值属性是表示用户和资源之间关系的字符串。它还必须对应于 protectable 资源上的 fulfills() 方法的 relationship 参数。

当关系链的长度为 2 时，它是一个由两个关系组成的序列。第一个 <parameter name= "X" value="Y"/> 元素存在于用户和组织实体之间。最后一个 <parmeter name= "X" value="Y"/> 元素存在于组织实体和资源之间。以下是长度为 2 的关系链的示例。

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

aValue1 的可能值包含 HIERARCHY 和 ROLE。HIERARCHY 指定在成员资格层次结构中，用户和组织实体之间存在层次结构关系。ROLE 指定用户在组织实体中担当角色。

如果 aValue1 的值是 HIERARCHY，则可能的值将包含 child，该值返回在成员层次结构中用户系其直接子女的组织实体。如果 aValue1 的值是 ROLE，则可能的值将包含 ROLE 表的 NAME 列中的任何有效条目的值，该值返回当前用户对其担当此角色的所有组织实体。

aValue3 条目是一个字符串，表示从第一个参数的评估中检索到的一个或多个组织实体和资源之间的关系。此值对应于 protectable 资源上的 fulfills() 方法的 relationship 参数。如果对参数 aValue1 进行评估时返回了多个组织实体，且当这些组织实体中的至少一个满足由参数 aValue2 所指定的关系时，则满足这一部分的 RELATIONSHIP_CHAIN。

注: 由带有单个参数元素的单个关系链所组成的关系组在功能上等价于简单关系。在此情况下，在策略中使用关系而不是关系组则更为方便。关于定义关系组的更多信息，请参阅第 80 页的『定义关系组』。

资源和策略所有权

所有策略都属于组织实体。所有访问控制资源也有所有者，通常是一个组织实体；例如，订单由拥有商店（在该商店中下了此订单）的组织所有。用户也可以拥有资源，例如注册用户拥有他自己的用户注册信息。在确定哪些策略适用于某个资源时，资源和访问控制策略的所有权非常重要。对于给定资源，应用属于其所属组织实体及该所有者上级组织实体的策略。

访问控制策略类型

有两种类型的访问控制策略:

- 标准策略
- 模板策略

标准策略

标准策略具有固定的所有者。例如，如果标准策略由卖方组织所有，则它将只适用于卖方组织所拥有的资源和它的下级组织实体（如果存在）所拥有的资源。由于在 WebSphere Commerce 中根组织是所有其它组织的上级组织，因此根组织（成员标识为 -2001）所拥有的任何策略，理论上适用于站点中的所有资源。这样，根组织所拥有的标准策略有时也称为站点级别的策略。

不由根组织所拥有的标准策略称为组织级别的策略，因为它们不适用于整个站点范围，而只适用于策略所有者所拥有的资源，或它的任何下级组织实体所拥有的资源。商店管理员可以管理它自己的组织实体及其下级组织实体的策略。站点管理员可以修改所有策略。

模板策略

模板策略的所有者是动态的。模板策略动态地适用于拥有资源的组织实体及其上级组织实体。例如，设想根组织下有 10 个组织，且每个组织都希望确保商店管理员只能修改对其担当该角色的组织所拥有的资源。则有两种这样设置的方法:

1. 根据所访问的资源，有一个将动态适用于这 10 个组织中任何组织的模板策略。模板策略中的访问组标准也可以是动态的。例如，如果用户试图访问组织 3 所拥有的资源，则模板策略的所有者将动态地更改为组织 3，且访问组也将动态地将其作用范围设为组织 3，即用户必须担当组织 3 的商店管理员角色。
2. 有 10 个策略，每个策略属于这 10 个组织中的一个。组织 1 的访问组将指定用户必须担当组织 1 的商店管理员角色。组织 2 的访问组将指定用户必须担当组织 2 的商店管理员角色，以此类推。

第一种解决方案的优点是，策略只有一个物理副本，而不是 10 个逻辑副本。模板策略可以由站点管理员管理。

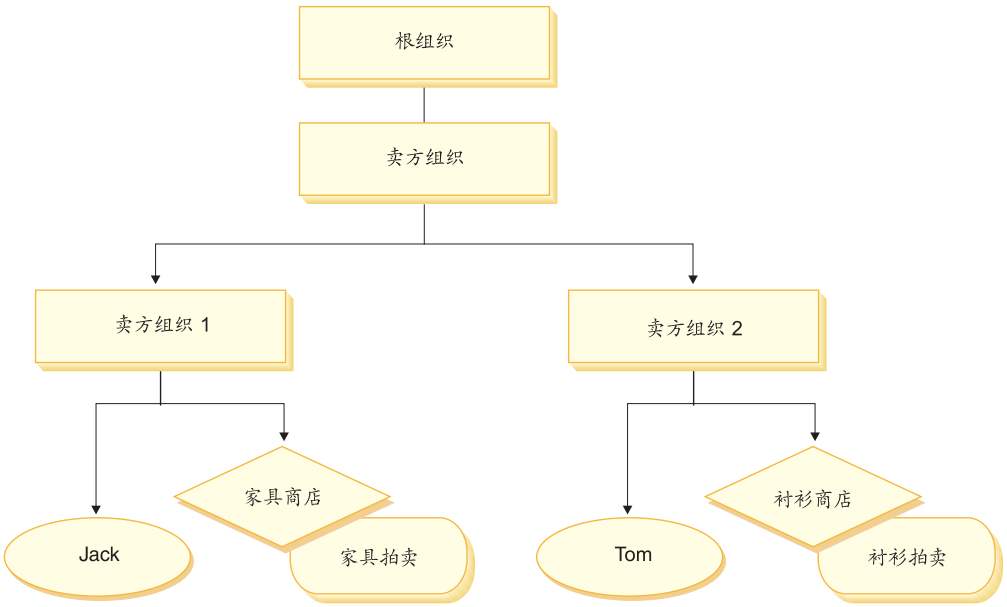
重设模板策略: 模板策略的另一个功能是: 对于指定的组织实体，他们可以重设。回到上面的示例，如果在 WebSphere Commerce 站点中添加了第 11 个组织实体，但这个最新的组织实体不希望上面的模板策略适用于它，则有一种方法可作此指定。必须在 ACORGPOL 表中添加一个条目，指定模板策略的策略标识和第 11 个组织的组织实体标识。这也可以通过 WebSphere Commerce 管理控制台，在商店管理员删除或更新模板策略时，在特定组织的上下文中完成。

当重设根组织的下级组织的模板策略时，该模板策略将仍然适用于根组织级别。如果在下级组织级别以更为严格的策略重设了模板策略，则也应当重设根组织级别的模板策略。重设根组织的模板策略的唯一方式是通过数据库，方式是运行以下 SQL 语句:

```
insert into ACORGPOL (acpolicy_id, member_id) values ( (select acpolicy_id from
ACPOLICY where policyname = 'policyToOverride'), -2001)
```

访问控制级别

WebSphere Commerce 中有两个广泛级别的访问控制: 命令级别（也称为基于角色的）和资源级别（也称为实例级别的）。



命令级别或基于角色的访问控制

命令级别或基于角色的访问控制是粗粒度的访问控制。它确定“谁可执行什么”。使用基于角色的访问控制，可指定特定角色的所有用户可执行某些命令。设想有一个访问控制策略：卖方可执行卖方命令。在此策略中，卖方命令之一是 ModifyAuction 命令。在上图中，Jack 和 Tom 都是卖方，因此两人都可修改拍卖。

基于角色的访问控制用于控制器命令和视图。此类型的访问控制不考虑命令将对其发生作用的数据资源。它仅确定是否允许用户执行特定的控制器命令或视图。

此级别的访问控制是强制的，且由运行时强制。所有的控制器命令都必须受到命令级别访问控制的保护。并且，可以直接调用或可通过来自另一命令的重定向而启动（相对于通过转发给视图而启动）的任何视图，都必须受到命令级访问控制的保护。

控制器命令的命令级别访问控制: 无论何时运行控制器命令，都必须存在一个访问控制策略，它授予用户对命令资源执行 Execute 操作的权限。资源是控制器命令的接口名称。访问组通常针对单个角色。例如，可指定具有“客户代表”角色的用户可执行 AccountRepresentativesCmdResourceGroup 资源组中的任何命令。

视图的命令级别访问控制: 当直接从 URL 调用视图时，或者从命令重定向调用视图时，该视图必须具有访问控制策略。在 ACACTION 表中，此类策略的 viewname 必须指定为操作。然后必须使用 ACACTACTGP 表将此操作与操作组相关联。而此操作组必须在 ACPOLICY 表中受到相应命令级别策略的引用。

实例级别或资源级别的访问控制

实例级别或资源级别的访问控制策略提供了细粒度的访问控制，确定了“谁可对哪些资源执行什么命令”。前面的基于角色的访问控制策略的示例允许卖方修改拍卖，可将它精细调整为资源级别的访问控制：卖方可修改对其担当该角色的组织所拥有的拍卖。在 21 中，Jack 具有卖方组织 1 的卖方角色，Tom 具有卖方组织 2 的卖方角色。Jack 在家具商店创建了家具拍卖。Tom 在衬衫商店创建衬衫拍卖。Jack 可修改家具拍卖，而*不能*修改衬衫拍卖。Tom 可修改衬衫拍卖，而*不能*修改家具拍卖。

总而言之，首先系统执行命令级别访问检查。如果允许用户执行命令，则执行后续的资源级别访问控制策略来确定用户是否可访问正被讨论的资源。

资源级别访问控制适用于命令和数据 bean。

命令的资源级别访问控制: 命令级别访问控制检查完成后，如果授予了访问权，则在以下两种情况之一中完成资源级别检查:

- 命令实现 `getResources()` — 此方法指定需要对当前操作进行检查的资源实例；在这里现在命令是操作。WebSphere Commerce 运行时将强制当前用户具有 `getResources()` 指定的所有资源的访问权限。缺省情况下，`getResources()` 返回 null，即，它不执行任何资源级别的检查。
- 命令调用 `checkIsAllowed(Object Resource, String Action)` — 当运行时调用 getResources() 时，命令编写器不知道需要检查哪些资源的情况下，命令可以按照需要调用此 `checkIsAllowed()` 方法，以确定当前操作和资源对是否得到授权。操作通常是当前命令的接口名称。调用此方法时，如果访问被拒绝，则抛出异常: `ECApplicationException( ECMessage._ERR_USER_AUTHORITY, ..)`

数据 bean 的资源级别访问控制: 如上面所做的说明，视图受到命令级别策略的保护，而这些策略通常是基于角色的。例如，命令级别策略可以指定卖方管理员对特定的视图具有访问权。常常需要进一步确保 JSP 上的数据 bean 都是与用户对其担任卖方管理员角色的组织相关的。这是通过让需要保护（直接或间接）的所有数据库实现 Delegator 接口而完成的。这些数据 bean 交托给主（独立）数据 bean，然后这些主（独立）数据 bean 实现 Protectable 接口。主数据 bean 将交托给它自身，因此实现这两个接口。这样，无论何时使用数据 bean 管理器的 `activate()` 方法调用数据 bean，WebSphere Commerce 运行时都将确保有一个策略授予当前用户对主数据 bean 资源执行 `Display` 操作的权限。

访问控制如何防止未授权的操作

本部分解释了基于策略的访问控制如何工作以确保用户仅可执行已授权的操作。

在执行用户启动的操作之前检查权限

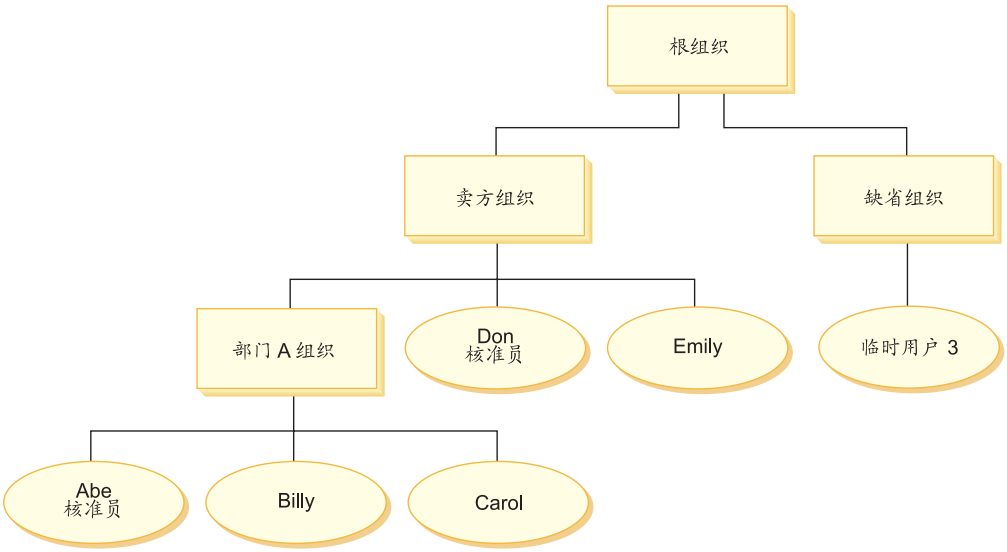
*策略管理器*是确定是否允许当前用户对指定资源执行指定操作的访问控制组件。访问控制策略以 XML 格式指定。实例创建期间，将缺省策略装入适当的数据库表中。当启动 WebSphere Commerce 应用程序服务器时，访问控制信息高速缓存在内存中，因此策略管理器可在被调用执行检查时快速检查用户的权限。如果通过 WebSphere Commerce 管理控制台或通过装入 XML 策略数据，在数据库中更改了访问控制信息，则需要更新访问控制高速缓存。这可通过更新 WebSphere Commerce 管理控制台中的访问控制注册表来完成。重新启动 WebSphere Commerce 也将导致更新高速缓存。

当用户试图执行受访问控制保护的操作时，将执行访问控制检查以确保用户是已授权的。策略管理器查找适用于拥有该资源的组织的所有访问控制策略。然后它检查这些策略以评估是否已授予用户对目标资源执行此操作的权限。如果存在至少一个这样的策略，则策略管理器将授予访问权，否则它将拒绝访问。

评估访问控制策略

本部分可用作评估访问控制策略的指南。在本部分中，将向您展示一个方案，并通过一个如何评估标准访问控制策略和模板访问控制策略的示例对您作指导。每个部分都以对相关策略以及使用每个策略的方案的描述作为开头。关于标准策略和模板策略的更多信息，请参阅第 19 页的『访问控制策略类型』。

下图以图形方式显示了方案:



组织层次结构

从图中可看到站点中有以下四个组织:

- 根组织
- 卖方组织
- 缺省组织
- 部门 A 组织

如您所见，根组织是卖方组织和缺省组织的父组织。卖方组织是部门 A 组织的父组织。

用户

在图中，Don 和 Emily 已注册到卖方组织。Abe、Billy 和 Carol 已注册到部门 A 组织。临时用户 3 未注册，但是出于访问控制目的，隐式地属于缺省组织。

角色

Don 具有卖方组织的核准员角色。Abe 具有部门 A 组织的核准员角色。

访问组

以下访问组用于此方案:

- 注册用户: 此组隐式地包含了已注册的所有用户。
- 卖方核准员: 此组隐式地包含了具有卖方组织核准员角色的所有用户。
- 部门 A 核准员: 此组隐式地包含了具有部门 A 组织核准员角色的所有用户。

文档

文档对象是受保护的资源。文档的所有者定义为在其中创建该文档的组织。

更新文档的访问控制需求

以下是更新文档的访问控制需求:

1. 注册用户可更新他们是其创建者的文档。
2. 部门 A 核准员可更新由部门 A 所拥有的文档，但不能更新由卖方组织所拥有的文档。卖方组织核准员可更新由部门 A 和卖方组织所拥有的文档。

评估标准策略

本部分引导您完成标准策略以及评估这些策略的方案。

与更新文档相关的访问控制策略

以下是与更新文档相关的策略格式和访问控制策略:

策略格式: `[Access Group, Action Group, Resource Group, Relationship]`

策略 1:

```
[Registered Users, Execute Command Action Group,  Update Document
Resource Group, - ]
```

这是由根组织所拥有的基于角色的标准策略。在此策略中，注册用户可执行 `Update Document` 命令。

策略 2:

```
[Registered Users, Update Document Action Group, document, creator ]
```

这是由根组织所拥有的资源级别的标准策略。在此策略中，如果注册用户是文档的创建者，就可更新该文档。

策略 3:

```
[Approvers for Seller, Update Document Action Group, document, - ]
```

这是由卖方组织所拥有的资源级别的标准策略。在此策略中，卖方核准员可更新卖方所拥有的文档。

策略 4:

```
[Approvers for Division A, Update Document Action Group, document, - ]
```

这是由部门 A 组织所拥有的资源级别的标准策略。在此策略中，部门 A 核准员可更新由部门 A 所拥有的文档。

方案

方案 1: Billy 尝试更新他自己的文档: 以下是此方案的访问控制评估:

命令级别的检查:

1. 未指定商店标识，因此命令的所有者将设置为根组织。因此，只有根组织拥有的策略才将用于评估用户是否具有命令级别的访问权: 策略 1 和 2 是根组织所拥有的。

2. 策略 1 授权访问权，因为 Billy 是注册用户访问组的成员，且他正在对 Update Document 命令资源执行 Execute 操作。

资源级别的检查:

1. Update Document 命令指定要保护文档资源。Billy 的文档由部门 A 所拥有。因此，只有由部门 A 及其上级组织所拥有的那些策略才适用: 策略 1、2、3 和 4。
2. 策略 2 授权访问权，因为 Billy 是注册用户访问组的成员，他正在对文档资源执行 Update Document 命令操作，并满足与文档之间的创建者关系。

因为 Billy 同时通过了命令级别和资源级别的访问控制检查，因此他可更新他自己的文档。

方案 2: Don 尝试更新 Carol 的文档: 以下是此方案的访问控制评估:

命令级别的检查:

1. 未指定商店标识，因此命令的所有者将设置为根组织。因此，只有根组织拥有的策略才将用于评估用户是否具有命令级别的访问权: 策略 1 和 2 是根组织所拥有的。
2. 策略 1 授权访问权，因为 Don 是注册用户访问组的成员，且他正在对 Update Document 命令资源执行 Execute 操作。

资源级别的检查:

1. Update Document 命令指定要保护文档资源。Carol 的文档由部门 A 所拥有。因此，只有由部门 A 及其上级组织所拥有的那些策略才适用: 策略 1、2、3 和 4。
2. 策略 4 授权访问权，因为 Don 是卖方核准员访问组的成员，且他正在对文档资源执行 Update Document 命令操作。

因为 Don 同时通过了命令级别和资源级别的访问控制检查，因此他可更新 Carol 的文档。

方案 3: Abe 尝试更新 Emily 的文档: 以下是此方案的访问控制评估:

命令级别的检查:

1. 未指定商店标识，因此命令的所有者将设置为根组织。因此，只有根组织拥有的策略才将用于评估用户是否具有命令级别的访问权: 策略 1 和 2 是根组织所拥有的。
2. 策略 1 授权访问权，因为 Abe 是注册用户访问组的成员，且他正在对 Update Document 命令资源执行 Execute 操作。

资源级别的检查:

1. Update Document 命令指定要保护文档资源。Emily 的文档由卖方组织所拥有。因此，只有由卖方组织及其上级组织所拥有的那些策略才适用: 策略 1、2 和 3。
2. 策略 3 不授予访问权，因为 Abe 不是卖方核准员访问组的成员。

尽管 Abe 通过了命令级别的检查，但是因为他未通过资源级别的访问控制检查，因此他不能更新 Emily 的文档。

方案 4: 临时用户 3 尝试更新他自己的文档: 以下是此方案的访问控制评估:

命令级别的检查:

1. 未指定商店标识，因此命令的所有者将设置为根组织。因此，只有根组织拥有的策略才将用于评估用户是否具有命令级别的访问权: 策略 1 和 2 是根组织所拥有的。

2. 策略 1 不授予访问权，因为临时用户 3 不是“注册用户”访问组的成员。

资源级别的检查:

1. 因为命令级别的检查失败，因此根本不会执行资源级别的检查。

因为临时用户 3 未通过命令级别的检查，因此他不能更新他自己的文档。

评估模板策略

此示例基于前面的方案。

与更新文档相关的访问控制策略

当评估模板策略时，用于评估标准策略的访问控制策略 1 和 2 仍然适用，然而模板策略 5 现在取代了标准策略 3 和 4。关于策略 1 和 2 的更多信息，请参阅第 24 页的『评估标准策略』。

策略 5:

```
[Approvers for Organization, Update Document Action Group, document, - ]
```

此策略是资源级别的模板策略。拥有文档的组织的核准员可更新文档。

还需要将用参数表示的新访问组用于此模板策略。将以下访问组添加到此方案:

- 组织核准员: 此组隐式地包含了具有 ? 组织核准员角色的所有用户。(当在运行时应用模板策略时，? 参数将动态更改为策略所有者。)

方案

以下方案仅使用策略 1、2 和 5。

方案 1: Don 尝试更新 Carol 的文档: 以下是此方案的访问控制评估:

命令级别的检查:

1. 未指定商店标识，因此命令的所有者将设置为根组织。因此，只有根组织拥有的策略才将用于评估用户是否具有命令级别的访问权: 策略 1 和 2 是根组织所拥有的。策略评估期间，模板策略动态地将所有者资格更改为拥有资源的组织，接着再更改为该组织的上级组织，因此策略 5 也将适用。
2. 策略 1 授权访问权，因为 Don 是注册用户访问组的成员，且他正在对 `Update Document` 命令资源执行 `Execute` 操作。

资源级别的检查:

1. `Update Document` 命令指定要保护文档资源。Carol 的文档由部门 A 所拥有。因此，只有由部门 A 及其上级组织所拥有的那些策略才适用: 策略 1 和 2。策略评估期间，模板策略动态地将所有者资格更改为拥有资源的组织，接着再更改为该组织的上级组织，因此策略 5 也将适用。
2. 模板策略 5 首先应用于拥有资源的组织: 部门 A。此时策略 5 本质上与策略 5a 的行为相似:

   ```
   [Approvers for Division A, Update Document Action Group, document, - ] standard
   resource-level policy owned by Division A.
   ```

3. 策略 5a 不授予访问权，因为 Don 不是部门 A 核准员访问组的成员。
4. 模板策略 5 接着将应用于部门 A 的父组织: 卖方组织。此时策略 5 本质上与策略 5b 的行为相似:

```
[Approvers for Seller, Update Document Action Group, document, - ] standard
resource-level policy owned by Seller
```

5. 策略 5b 授权访问权，因为 Don 是卖方核准员访问组的成员，且他正在对文档资源执行 Update Document 命令操作。

因为 Don 同时通过了命令级别和资源级别的访问控制检查，因此他可更新 Carol 的文档。

方案 2: Abe 尝试更新 Emily 的文档: 以下是此方案的访问控制评估:

命令级别的检查:

1. 未指定商店标识，因此命令的所有者将设置为根组织。因此，只有根组织拥有的策略才将用于评估用户是否具有命令级别的访问权: 策略 1 和 2 是根组织所拥有的。策略评估期间，模板策略动态地将所有者资格更改为拥有资源的组织，接着再更改为该组织的上级组织，因此策略 5 也将适用。
2. 策略 1 授权访问权，因为 Abe 是注册用户访问组的成员，且他正在对 Update Document 命令资源执行 Execute 操作。

资源级别的检查:

1. Update Document 命令指定要保护文档资源。Emily 的文档由卖方组织所拥有。因此，只有由卖方及其上级组织所拥有的那些策略才适用: 策略 1 和 2。策略评估期间，模板策略动态地将所有者资格更改为拥有资源的组织，接着再更改为该组织的上级组织，因此策略 5 也将适用。
2. 模板策略 5 首先应用于拥有资源的组织: 卖方组织。此时策略 5 本质上与策略 5a 的行为相似:

   ```
   [Approvers for Seller, Update Document Action Group, document, - ] standard
   resource-level policy owned by Seller
   ```

3. 策略 5a 不授予访问权，因为 Abe 不是卖方核准员访问组的成员。
4. 模板策略 5 接着将应用于卖方组织的父组织: 根组织。此时策略 5 本质上与策略 5b 的行为相似:

   ```
   [Approvers for Root, Update Document Action Group, document, - ] standard
    resource-level policy owned by Root
   ```

5. 策略 5b 不授予访问权，因为 Abe 不是根组织核准员访问组的成员。
6. 根组织不具有父组织，因此已完整地评估了模板策略 5。

尽管 Abe 通过了命令级别的检查，但是因为他未通过资源级别的访问控制检查，因此他不能更新 Emily 的文档。

详细探讨一个策略

既然理解了访问控制策略的基本结构和存在着的策略类型，那么现在让我们用一系列不同的示例来详细探讨一个缺省策略。将要研究的策略如下:

```
AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
```

注: 此策略是资源级别的策略。它的策略类型是模板。

在第一个示例中，将学习如何使用 WebSphere Commerce 管理控制台读取策略、识别其组成部分并理解策略的含义。第二个示例将探讨 XML 格式的策略，以帮助您理解同一信息在代码中呈现的样子。

第三个示例将更进一步地理解一个策略如何与其它策略相关。理解策略之间的从属性对于更改访问控制策略或创建新策略是重要的先决条件。

示例 1: 读取策略

在此示例中，将使用 WebSphere Commerce 管理控制台查找策略并识别定义它的各个组成部分。还将使用这些组成部分来形成对策略的一般描述。

在管理控制台中查找策略

1. 登录到 WebSphere Commerce 管理控制台。从“访问管理”菜单，选择**策略**。
2. 请验证“查看”下拉菜单是否已设置为您的组织。
3. 在“策略”页面上，滚动策略列表并查找以下策略:
   `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`
   请注意可通过使用滚动条以及使用**第一页**、**上一页**、**下一页**和**最后一页**链接，在策略列表中间滚动。

查看策略的各个组成部分

1. 通过单击策略旁的框并单击**显示操作组**来选择策略。
2. 在“操作组”页面上，将看到操作组 AuctionManage。这是与策略关联的操作组。选择 `AuctionManage` 并单击**显示操作**。
3. 在下一页上，将看到包含在 `AuctionManage` 操作组中的以下操作或命令的列表:
   - `com.ibm.commerce.negotiation.commands.CloseBiddingCmd`
   - `com.ibm.commerce.negotiation.commands.DeleteAuctionCmd`
   - `com.ibm.commerce.negotiation.commands.ModifyAuctionCmd`

   这里，`AuctionManage` 包括结束拍卖（`CloseBiddingCmd`）、删除拍卖（`DeleteAuctionCmd`）和修改拍卖（`ModifyAuctionCmd`）。关于命令的更多信息，请参阅联机帮助文档中的参考部分。

   请注意也可从“策略”页面通过单击**显示操作**，访问同一操作列表。
4. 要返回到策略页面，请选择任意操作，并单击**显示策略**。
5. 再次选择策略，但是现在单击**显示成员组**以查看此策略适用的成员（访问组）。
6. 请记下成员（访问）组名称。在此例中，成员（访问）组是 `AuctionAdministratorsForOrg`。
7. 从“访问管理”菜单，选择**访问组**。
8. 查找 `AuctionAdministratorsForOrg`。选择它并单击**更改**。
9. 单击**条件**。在“条件”页面上，在选定的角色和组织下查找。应当看到以下角色:
   - 卖方 — 对于组织
   - 产品经理 — 对于组织
   - 买方（销售方）— 对于组织
   - 类别经理 — 对于组织

指定了拥有拍卖资源的组织的这些角色之一的所有用户都是 AuctionAdministratorsForOrg 访问组的组成部分。

10. 不作任何更改离开“条件”页面。从“访问管理”菜单，再次选择**策略**。查找以下策略:

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

11. 选择该策略并单击**显示资源**。在“资源”页面上，将看到 com.ibm.commerce.negotiation.objects.Auction 资源。这是列在操作组中的那些操作对其实施操作的资源。在此例中，资源是拍卖。请注意可从“策略”页面通过单击**显示资源组**并进而转至个别资源，访问此同一列表。
12. 现在从“访问管理”菜单中选择**策略**，并查找以下策略:

    AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

13. 选择该策略并单击**更改**。在“更改策略”页面上，查看**关系**下的下拉菜单。请注意关系设置为“无”。这意味着策略不具有关系。
14. 在对话框中单击**取消**和**确定**。

理解策略的含义

既然已识别了此策略的单个组成部分，则可着手将它们组合在一起以理解策略的作用。首先已知该策略适用于属于 AuctionAdministratorsForOrg 组的所有用户。通过单击**显示成员组**可以了解到这一点。在该处使用了“访问管理”菜单转至“访问组”页面，并看到访问组包含以下角色: 卖方、产品经理、买方（用于销售方）以及类别经理。总体来说，具有这四个角色之一的用户可称为拍卖管理员。

还已经了解到操作组包含用于修改、撤销和结束拍卖的命令，资源组仅包含受管的拍卖资源。同样，通过从“策略”页面单击**显示操作**和**显示资源**，并进而转至详细信息级别，了解到这一点。最后，可得知策略不包含访问组和资源之间的关系。

将所有已知情况放在一起，可总结如下: 该策略允许拍卖管理员执行与管理对拍卖资源的拍卖相关联的所有活动，例如修改、撤销和结束拍卖，只要管理员对拥有拍卖的组织担当该角色。

可通过查看策略的名称而知道策略的含义。在此示例中，策略以指定用户组的名称 AuctionAdministrator 开头。ForOrg 指示策略适用于组织。AuctionManageCommands 描述操作组，AuctionResource 描述资源组。

示例 2: 读取 XML 格式的策略

缺省访问控制策略存储在 XML 文件中，该文件是在实例创建期间装入数据库的。当在 WebSphere Commerce 管理控制台中查看策略时，是在使用界面来查看和更改存储在数据库中的信息。策略管理器使用数据库中的信息来评估访问控制。如果数据库信息比起 XML 文件更新，则您可使用抽取程序工具将数据库中的访问控制策略信息抽取到 XML 文件中。

大部分时候您都将使用 WebSphere Commerce 管理控制台用户界面来管理策略。然而，如果希望查看 XML 格式的策略，或者是希望进行高级修改，则以下是策略在 XML 文件中呈现的样子:

```
<!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
```

```
-->
<Policy
Name="AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="template">
</Policy>
```

这里，策略是按以下内容定义的:

Name: 策略的名称。

OwnerID: 策略应用的组织。

UserGroup: 访问组。

ActionGroupName: 操作组。

ResourceGroupName: 资源组。

PolicyType: 策略类型，例如站点级别、模板或组织。

包含所有缺省访问控制策略的文件称为 defaultAccessControlPolicies.xml 且位于以下目录:

X:*installation_directory*\xml\policies\xml。

注: 对每个缺省访问控制文件的描述包含在 defaultAccessControlPolicies_*locale*.xml 文件中，可在同一目录中找到该文件。对缺省访问控制文件中的缺省访问控制策略作出更改后，需要在 defaultAccessControlPolicies_zh_CN.xml 中对其相应的描述作更新。强烈建议对 XML 文件的任何更改保留给高级用户使用。

示例 3: 识别与您的策略关联的其它策略

在这最后一个示例中，将探讨访问控制策略与其它策略有何种从属关系。

定义一组用户（访问组）可对资源执行的命令（操作）的策略称为资源级别的策略。例如，上面详细探讨的策略:

AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource 是资源级别的策略的示例。

然而，资源级别的策略所允许的操作还依赖于属于该策略的访问组中每个角色所允许的操作。描述对特定角色允许哪些操作的策略称为基于角色的策略。

要识别与资源级别的策略关联的基于角色的策略，请执行以下操作:

查找与策略关联的角色

1. 登录到 WebSphere Commerce 管理控制台并在“策略”页面中查找资源级别的策略。使用同一示例，已知需要以下策略:

   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource

   .

2. 识别与策略关联的访问组。在此例中，已知访问组是 AuctionAdministratorsForOrg。
3. 查找与访问组关联的角色。对于 AuctionAdministratorsForOrg，从上一示例中已知这些角色是：买方（销售方）、类别经理、产品经理和卖方。

为每个角色查找基于角色的策略

1. 转至本书结尾的附录，并找到节标题『基于角色的策略』。您将使用附录查找与角色关联的每个基于角色的策略。
2. 查找 Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup 策略。此策略与买方（销售方）角色关联。因为策略的前缀是 Buyers(sell-side)，因此可了解到这一点。
3. 使用角色前缀识别正确的策略，来查找与买方（销售方）、类别经理、产品经理和卖方角色关联的其余基于角色的策略。应当得到以下列表:
   - Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
   - Buyers(sell-side)ExecuteBuyers(sell-side)Views
   - CategoryManagersExecuteCategoryManagersCmdResourceGroup
   - CategoryManagersExecuteCategoryManagersViews
   - ProductManagersExecuteProductManagersCmdResourceGroup
   - ProductManagersExecuteProductManagersViews
   - SellersExecuteSellersCmdResourceGroup
   - SellersExecuteSellersViews
4. 每个基于角色的策略允许具有该角色的用户执行特定的控制器命令或视图。要查看哪个操作与基于角色的策略关联，请使用与示例 1 相同的过程，从 WebSphere Commerce 管理控制台的“策略”页面查找策略。

为何识别策略之间的从属性是至关重要的

了解哪些基于角色的策略与资源级别的策略关联通常是定制策略以及创建新策略的先决条件。

在第 41 页的第 5 章，『定制方案』中，将了解有关资源级别和基于角色的策略的更多内容，包括如何识别、理解其差别以及了解它们彼此如何相关。

第 4 章 定制缺省访问控制策略

WebSphere Commerce 提供的缺省访问控制策略致力于满足组织所具有的基本需要，这些基本需要用于控制对组织用户提供的操作和信息。通常，缺省策略对于站点的需要可能已足够。同时，缺省策略是高度可定制的，这样允许按您自己的需求进行定制。

SiteAdministratorsCanDoEverything 策略是一种特殊缺省策略，它将超级用户访问权授予具有站点管理员角色的管理员。在此策略中，站点管理员可对任意资源执行任意操作，即使未定义过这些操作或资源。在将此角色指定给用户时意识到这一点是很重要的。

本章提供了如何对随 WebSphere Commerce 包含的缺省访问控制策略进行基本更改的信息。通过介绍您将需要了解的某些概念和关系作为开始。

注: 如果遇到不熟悉的术语或概念，请参阅第 9 页的第 3 章，『访问控制概念』以获取更多信息。

识别受更改影响的策略

在上一章中，已了解到策略通常与其它策略相关。还了解到如何着手使用资源级别的策略以及识别与其关联的基于角色的策略。在本部分中将更详细地说明策略如何彼此相关，以及为何需要在可修改现有的策略或创建新策略之前，了解它们的关系。在许多情况下，需要更改几个策略以正确地实现更改。

了解基于角色和资源级别的策略之间的关系

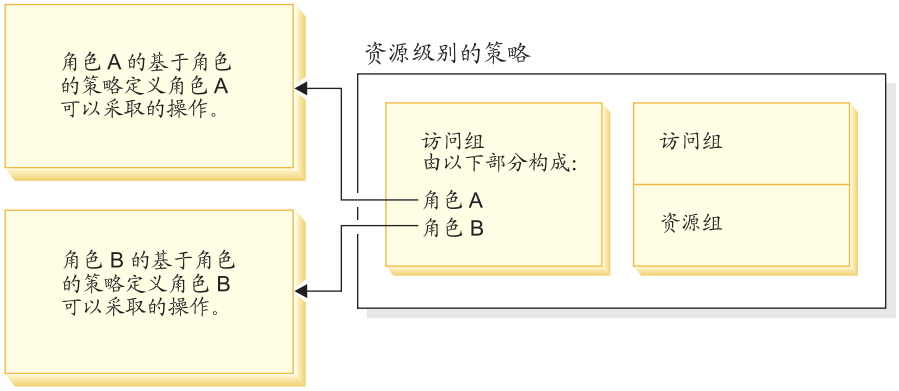
在 WebSphere Commerce 中，如下使用基于角色的策略，将可由用户执行的每个操作指定给一个或多个角色:

- 每个缺省角色都具有对应的访问组。例如，角色“商店管理员”的访问组是 StoreAdministrators。
- 每个“基于角色”的访问组通常具有两个关联的基于角色的策略:
  - 一个策略定义已授权该角色执行的控制器命令。
  - 另一个策略定义已授权该角色执行的视图操作。在 VIEWREG 表中将视图操作映射为视图。例如，StoreListView 显示的 Web 页面带有系统中商店的列表。

一些控制器命令仅有基于角色的策略，而没有资源级别的策略。这发生在命令没有作用于任何受保护资源的情况下。例如，命令 SetCurrencyPreferenceCmd 不需要资源级别的策略，因为它仅可更改正在运行该命令的用户的货币首选项。如果它能够更改另一用户的货币首选项，则必须保护用户对象，并且将需要资源级别的策略。

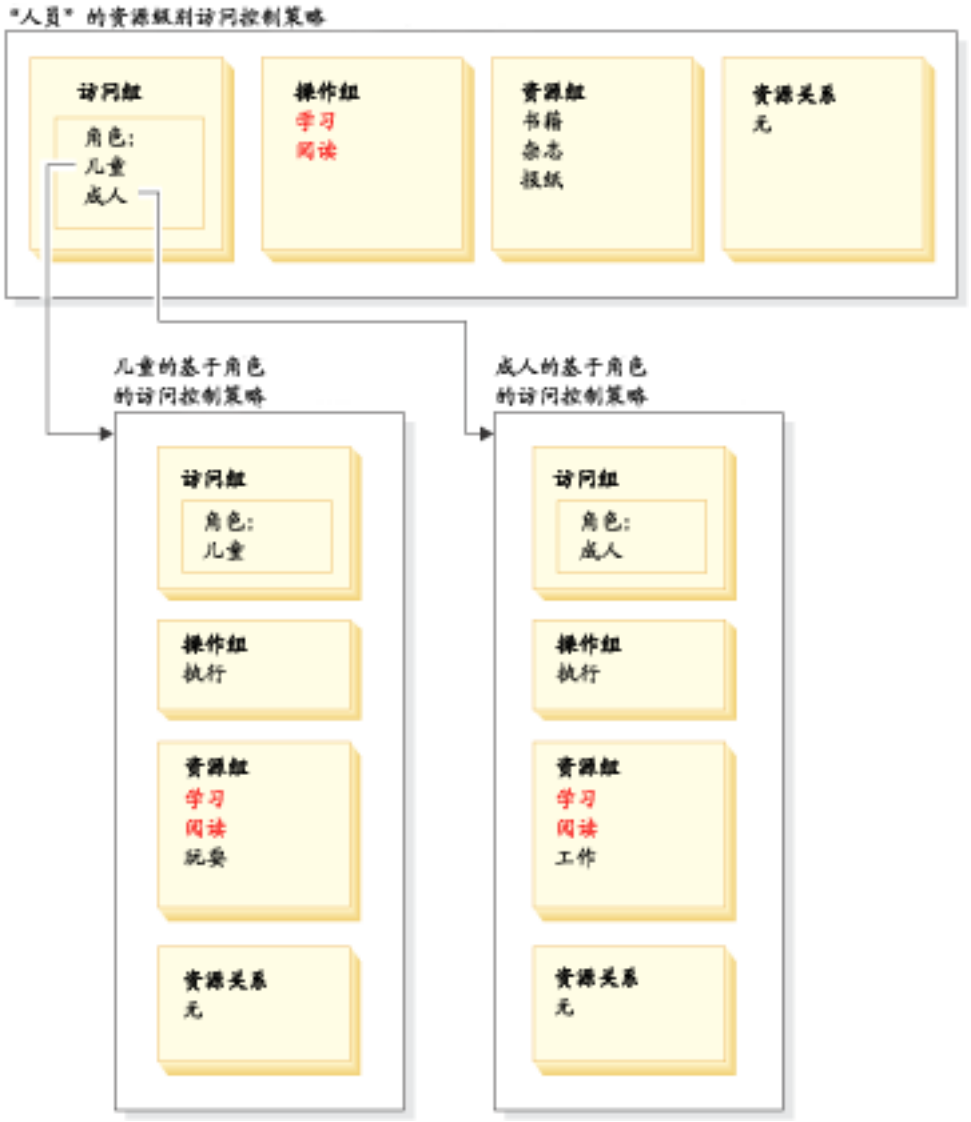
用于控制器命令的资源级别的策略与用于控制器命令的某些基于角色的策略直接相关。在资源级别的策略中，控制器命令是操作组的一部分，但是在基于角色的策略中，控制器命令是资源组的一部分。下图说明了此关系。资源级别的策略在其访问组中包含角色 A 和 B，这将使角色 A 和 B 的基于角色的策略起作用。当资源级别的策略授权具有角色 A 或 B 的用户对一组特定资源执行某些操作时，关联的基于角色的策略通常会对具有角色 A 和 B 的用户提供授权执行这些操作。

图 3. 资源级别的策略及其关联的基于角色的策略之间的关系



下图显示了一个样本资源级别的策略，它授权“人员”访问组中的用户阅读或研究某些资源（即书籍、杂志和报纸）。此策略是正确表达的，因为用于角色“儿童”和“成人”的基于角色的策略也授权他们阅读或研究书籍、杂志和报纸。

图 4. 资源级别的策略以及影响它的基于角色的策略。



请注意在用于控制器命令的基于角色的策略中:

- 操作组仅包含单个操作: 执行。
- 资源组包含可执行的控制器命令。

类似地，在用于视图的基于角色的策略中:

- 操作组包含可执行的视图。
- 资源组包含单个资源: com.ibm.commerce.command.ViewCommand。

另一方面，在资源级别的策略中:

- 操作组包含可对资源组中的资源执行的一组操作。
- 资源组包含可对其实施操作的一系列实际业务资源。

资源级别的策略仅可授权特定角色的用户执行已得到对应的基于角色的策略授权的操作。例如，在上述示例中，角色“儿童”被授权执行以下操作:

- 学习
- 阅读
- 玩耍

假定资源级别的策略现在更改为包含新的名为“工作”的操作。具有角色“成人”的用户将能够执行操作“工作”。但是，具有角色“儿童”的用户则不能。当检查这两个角色的基于角色的策略时会发现原因是显然的。用于“成人”的策略在其资源组中列出了操作“工作”。用于“儿童”的策略则没有。即使“儿童”和“成人”都得到了资源级别的策略的正确授权，但是用于“儿童”的基于角色的策略不授权操作“工作”。

由于资源级别的策略关联到基于角色的策略的方式，因此跟踪受特定更改影响的所有策略的最佳方法是从资源级别的策略逆向工作。第一步是检查资源级别的策略的访问组并确定它是否包含任何角色。可通过从管理控制台选择“访问管理 > 角色”，查看缺省角色的完整列表。

如果资源级别的策略的访问组包含角色，请复查其基于角色的策略以查看是否需要对它们进行更改。如果正在将操作添加到资源级别的策略的操作组，则需要确保相关的基于角色的策略也对新操作作了授权。如果正在从资源级别的策略中删除操作，并且没有其它资源级别的策略引用此操作，则最好从关联的基于角色的策略中除去相应的资源。

理解策略模型

授权策略必须存在，用户才能执行操作。但是如果有**任何**策略提供了所需的授权，则 WebSphere Commerce 允许用户执行操作。因此，如果定义了比缺省策略更具有限制性的新策略，则必须删除或修改更为宽泛的缺省策略，以防止它覆盖新策略。

例如，假定缺省策略 A 授权所有注册用户提交拍卖投标。您希望更改此策略，以便将拍卖投标限制在具有买方角色的用户。如果您仅定义授权买方可创建拍卖投标的新策略，则新策略将不生效。缺省策略 A 将仍然允许所有注册用户投标。要使新策略生效，必须删除更为宽泛的缺省策略。

表 1 总结了在创建、删除或更改资源级别的策略时需要进行的附加更改。

表 1. 更改使用角色的资源级别的策略时需要的附加更改。

当您对资源级别的策略作此更改时:	如果资源级别的访问组使用角色，还必须进行以下更改:
将操作添加到策略的操作组。	确保适用的基于角色的策略在其资源组中包含该操作。
从策略的操作组中除去操作。	无需附加更改。出于一致性，最好从相关的基于角色的策略的相应资源组中除去此操作。仅当没有其它操作组引用此操作时才可这样做。如果其它操作组正在引用此操作，则很可能存在着基于角色的策略仍然需要在其资源组中包含此操作。
使用另一操作组。	确保适用的基于角色的策略在其资源组中包含新操作组的操作。
将角色添加到策略的访问组。	请确保对应于新角色的基于角色的策略所引用的资源组包含了在资源级别的策略中指定的操作。
从策略的访问组除去角色。	无需附加更改。出于一致性，最好修改相应的基于角色的策略，以便它不再在其资源组中引用这些操作。

表 1. 更改使用角色的资源级别的策略时需要的附加更改。 (续)

使用另一访问组。	确保适用的基于角色的策略在其资源组中包含资源级别的策略的操作组中的操作。
创建新策略。	检查是否存在对相同操作作了授权的现有策略。如有必要则删除它。
删除该策略。	要防止有任何用户执行该策略的操作，请删除对相同操作作了授权的所有其它策略。

确定策略是基于角色的还是资源级别的

基于角色的策略也称为命令级别的策略，因为这些策略授权具有特定角色的用户执行一组命令。资源级别的策略授权一组用户对一组特定资源执行一组命令。例如，基于角色的策略可授权儿童吃东西。而资源级别的策略可授权儿童吃米饭。

通常可通过观察其名称，确定策略是基于角色的策略还是资源级别的策略。

基于角色的策略

定义角色可执行的控制器命令的策略遵循命名约定:

<AccessGroupforRoleXYZ> Execute <XYZCmdResourceGroup>

例如: `ProductManagersExecuteProductManagersCmdResourceGroup`。

在用于控制器命令的基于角色的策略中，操作组包含名为 `Execute` 的单个条目，资源组包含具有该角色的用户可执行的一系列 WebSphere Commerce 命令。

定义角色可执行的视图的策略遵循命名约定:

<AccessGroupforRoleXYZ> Execute <XYZViews>

例如: `SalesManagersExecuteSalesManagerViews`。

在用于视图的基于角色的策略中，操作组包含具有该角色的用户可执行的一系列视图。

资源级别的策略

定义谁可对数据资源（可创建或操纵的商业对象）执行操作的策略遵循命名约定:

<AccessGroupXYZ> Execute <XYZCommands> On <XYZResource>

例如: `AllUsersExecuteOrderProcessOnOrderResource`。

在资源级别的策略中，操作组包含 WebSphere Commerce 命令，资源组识别可进行操作的特定业务资源。

一个例外是授权创建实体（例如订单、投标或 RFQ）的策略。这些策略不对实体本身执行操作，因为尚未创建实体。而是对包含它们的实体执行操作。例如，在商店上下文中创建拍卖，在组织上下文中创建用户。大多数资源都是在商店上下文中创建的。因此，这些策略具有如下的名称:

<AccessGroupXYZs> Execute <XYZCommands> On <StoreEntityResource>

例 如 :
AuctionAdministorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource。

定义谁可查看数据 bean 资源（数据 bean 包含有关数据资源的信息，例如投标或订单，通常用于 JSP）的策略遵循命名约定:

<AccessGroupXYZs> Display <XYZDatabeanResourceGroup>

例如: MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup。

更改缺省策略的技巧

更改缺省策略时，请牢记以下内容:

- 大多数访问组是按用户角色定义的，例如买方或产品经理。要更好地理解这些角色以及允许它们执行哪些操作，请参阅第 11 页的『角色』。
- 在将策略更改为使用另一访问组之前，请复查该访问组的定义以确保它符合需要。要完成此操作，请从管理控制台选择**访问管理 > 访问组**。
- 根据对“查看”选择的值，“策略”页面显示站点级别的策略或特定于特定组织的策略:
  - 如果将“查看”字段设置为“根组织”，则显示根组织所拥有的标准策略以及模板策略的主版本。
  - 如果将“查看”字段设置为某个组织的名称，则显示该组织所拥有的标准策略以及该组织可修改的模板策略。
- 重命名更改的所有缺省策略，以便策略名称反映出策略的作用，以及可识别出已更改的缺省策略。请考虑对定制的策略实现命名约定。如果合适，还应当修改策略的描述及其显示名称。

注: WebSphere 管理控制台仅可对访问控制策略定义和访问组定义执行简单的修改。更为强健的解决方案是使用 XML 文件更新数据。以下操作仅可通过 XML 完成:

1. 定义新的操作、资源、属性、关系和关系组。
2. 定义复杂的隐式资源组以及复杂的隐式访问组。

更改策略之后

每次创建或修改访问控制策略时，都必须执行某些测试以验证策略是否正确工作。

一旦完成了对当前处于数据库中的所有新的和已更改的策略的测试，则将该信息抽取到 XML 文件中是一个好方法。这些文件与初始的访问控制策略相关文件的格式相同: defaultAccessControlPolices.xml、defaultAccessControlPolicies_locale.xml 和 ACUserGroup_locale.xml。这一步骤是必需的，因为使用管理控制台所作的更改仅影响存储在数据库中的策略信息。并未自动更新用于在实例创建期间装入缺省访问控制策略及其组成部分的 XML 文件。

应当维持 XML 文件和数据库中的访问控制信息之间的一致性，原因有以下几个:

- 创建 WebSphere Commerce 实例时，策略和访问组定义是从 XML 文件装入的。

- XML 文件提供了直接查看和编辑策略及其组件部分的便捷方式，因此将这些文件保持为最新是至关重要的。

测试策略更改

对于每个策略，确保以下内容:

- 属于策略的访问组的用户能够对指定的资源执行指定的操作。如果除去了对执行某个操作的授权，则还应当进行测试以确保用户不再能够执行该操作。
- 不属于策略的访问组的用户不能对指定的资源执行指定的操作。

例如，假定您实现第 5 章中的拍卖定制方案 1，在此方案中除去拍卖管理员的结束拍卖投标的能力。要测试此更改是否正确工作，请以属于“拍卖管理员”访问组用户的身份登录，并执行以下操作:

- 修改拍卖。
- 删除拍卖。

还应当验证拍卖管理员是否无法结束投标。

然后，以不属于“拍卖管理员”访问组用户的身份登录，并尝试执行同样的操作。如果策略正确工作，则您的尝试应当失败。

将策略更改抽取到 XML 文件中

最终确定并测试了策略更改时，应当更新 XML 文件以保持其与数据库中的策略信息同步。附录描述了与访问控制策略和访问组相关的不同 XML 文件。它还说明了如何将策略更改从数据库抽取到 XML 文件，以及如何将策略信息从 XML 文件装入到数据库中。

第 5 章 定制方案

下面展示的定制方案让您能应用所学到的关于访问控制策略的知识，对缺省策略进行各种基本更改。对于所有这些方案，假定站点管理员正在修改根组织的策略。一旦按步骤完成了其中的一些方案，您就可以遵循同样的方法执行这里没有特别说明的更改。

方案是按业务区域组织的。在每个业务区域中，以渐增的复杂性为顺序展示这些方案。

表 2. 方案目录

业务区域	起始页
拍卖	第 42 页的『拍卖方案 1: 除去拍卖管理员结束拍卖投标的能力』
合同	第 46 页的『合同方案 1: 除去合同管理员添加或删除合同附件的能力』
订单	第 48 页的『订单方案 1: 仅允许买方创建订单』
成员资格	第 53 页的『成员资格方案 1: 除去用户自注册能力』
赠券	第 57 页的『赠券方案 1: 仅允许买方兑换赠券』
采购	第 61 页的『采购方案 1: 允许采购购物车经理为由其组织创建的订单管理采购购物车』
库存	第 63 页的『库存方案 1: 允许实现中心经理更新实现中心但是不能删除它们』
商务智能	第 65 页的『商务智能方案 1: 允许审计员查看商务智能报表』

如果正在查找说明特定种类更改的方案，请参阅下表，它按说明的定制类型交叉引用了这些方案。

表 3. 按定制类型组织的定制方案

定制	请参阅页面
将角色添加到策略的访问组	59
更改策略的操作组	62,63
更改策略的资源关系	50,61
将策略更改为使用另一访问组	44,48,50,54,57,59
创建新访问组并将它用于策略	52,55
创建新操作组并将它用于策略	55,62
创建新的资源级别的策略	47,62
创建新的基于角色的策略	55,65
创建新角色并将它用于资源级别的策略	55,65

表 3. 按定制类型组织的定制方案 (续)

删除策略	43,43,54
从策略的操作组中除去操作	3,46

表 3: 按定制类型组织的定制方案

拍卖方案 1: 除去拍卖管理员结束拍卖投标的能力

缺省情况下，商店的拍卖管理员可修改或删除商店拍卖，并可结束投标。在某些情况下，或者是因为您希望由其他人处理此操作，或者是因为对于您的商店不需要此操作，您可能不希望授予拍卖管理员结束投标的权限。

在此方案中，将除去拍卖管理员结束投标的权限。要完成此更改，将执行以下操作:

1. 使用附录查找定义了拍卖管理员可执行的操作的资源级别的策略。
2. 确定策略的操作组名称。
3. 从策略的操作组中删除结束拍卖投标的操作。

要执行的步骤

识别必须更改其操作组的策略

1. 查看附录的“拍卖”下的内容，识别出要更改的资源级别的策略。策略是:

   `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下策略的操作组的名称 `AuctionManage`。这是需要更改的操作组，以除去结束投标的操作。

从策略的操作组中除去结束投标的操作

1. 单击**访问管理 > 操作组**。
2. 从操作组列表中，选择 **AuctionManage**。
3. 单击**更改**显示“更改资源组”页面。
4. 从“选定的操作”列表中，选择 **com.ibm.commerce.negotiation.commands.CloseBiddingCmd**。
5. 单击**除去**。
6. 单击**确定**。

使用更改更新策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

拍卖方案 2: 除去拍卖管理员撤销投标的能力

缺省情况下，商店的拍卖管理员可撤销对其拍卖所提交的投标。在一些情况下，您可能不希望将此权限授予任何人。要进行此更改，必须查找到定义谁可撤销投标的资源级别的策略并删除它。

在拍卖方案 1 中，“结束投标”操作是包含在策略中的数个操作之一。因此，仅须从策略的操作组中除去该操作。然而在此方案中，整个策略控制着投标撤销。因此，必须删除策略而不仅仅是删除操作。

要删除策略，需要执行以下操作:

- 使用附录查找涉及由拍卖管理员撤销拍卖投标的资源级别的策略。
- 删除该策略。

注: 在删除策略之前，请记下其名称、访问组名称、资源组名称以及操作组名称，以便可以在下一方案中重新创建它。

要执行的步骤

1. 查看附录的“拍卖”下的内容，识别出要更改的资源级别的策略。策略是:

   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表中，选择以下策略:

   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource
5. 单击**删除**。

使用更改更新策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

拍卖方案 3: 除去拍卖管理员在某个组织中撤销投标的能力。

缺省情况下，商店的拍卖管理员可撤销对其拍卖所提交的投标。在一些情况下，作为站点管理员，您可能希望对特定组织更改此策略。要进行此更改，必须删除对此组织授权该操作的模板策略。

注: 在 WebSphere Commerce 专业版中，仅有三个组织: 根组织、缺省组织和卖方组织。

删除策略之后，该组织的拍卖管理员将不再能够撤销投标。其它组织的拍卖管理员不会受此更改的影响。

要删除策略，需要执行以下操作:

- 使用附录查找对撤销拍卖投标作了授权的资源级别的策略。
- 在该组织的策略列表中查找该策略。
- 删除该策略。

要执行的步骤

删除策略

1. 查看附录的“拍卖”下的内容，识别出要更改的资源级别的策略。策略是:
   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择希望删除其策略的组织。选择了特定组织（而不是根组织）时，您的策略更改仅应用于该组织（而不是站点上的所有组织）。
4. 从策略列表中，选择以下策略:
   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource
5. 单击**删除**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

拍卖方案 4: 将拍卖投标限制为买方

缺省情况下，允许所有注册用户对商店中拍卖的产品投标，无论这些用户在其组织中的位置如何。在一些情况下，您可能希望将投标限制到一组受限用户，例如 WebSphere Commerce 中指定为“买方”角色的那些用户。

在此方案中，将更改资源级别的策略及其关联的基于角色的策略。要将投标限制到具有“买方”角色的买方组织的成员，需要执行以下操作:

- 使用附录查找指定谁可创建拍卖投标的资源级别的策略。
- 将策略的访问组从所有注册用户更改为具有“买方”角色的那些用户。
- 重命名策略、描述和显示名称。
- 识别用于创建投标的命令。
- 使用附录查找用于买方（购买方）的基于角色的策略。此策略定义了具有买方（购买方）角色的用户可执行的命令。必须更新此策略的资源组以允许买方执行创建投标的命令。
- 更新此基于角色的策略的资源组使其包含创建投标的命令。

要执行的步骤

识别资源级别的策略

1. 查看附录的“拍卖”下的内容，识别出要更改的资源级别的策略。策略是:
   `RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource`。
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表中，选择
   RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource。

5. 记下策略的操作组名称 BidCreate。这是需要查看的操作组，以查找用于创建投标的命令名称。

更改策略的访问组

1. 单击**更改**显示“更改策略”页面。
2. 对于“用户组”，单击**查找**并选择**买方（购买方）**。
3. 单击**确定**。
4. 通过编辑其文本，重命名策略、显示名称和策略描述。
5. 单击**确定**。

识别用于创建投标的命令

1. 单击**访问管理 > 操作组**。
2. 从操作组列表中，选择 **BidCreate**。
3. 单击**更改**显示“更改操作组”页面。记下用于创建投标的命令名称：com.ibm.commerce.negotiation.commands.BidSubmitCmd。必须将此命令添加到包含买方可执行命令列表的资源组中。

识别买方（购买方）角色的基于角色的策略和资源组

1. 查看附录的“基于角色的策略”下的内容，查找出用于买方（购买方）的基于角色的策略。策略是:

   Buyers(buy-side)ExecuteBuyers(buyside)CommandsResourceGroup.
2. 单击**访问管理** > **策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 记下资源组的名称: Buyers(buy-side)CommandsResourceGroup。现在有了需要更新的资源组的名称。

更新基于角色的策略中的资源组使其包含用于创建投标的命令

1. 单击**访问管理 > 资源组**。
2. 选择 **Buyers(buy-side)CommandsResourceGroup**。
3. 单击**更改**显示“更改资源组”页面。
4. 单击**下一步**显示“详细信息”页面。
5. 从“可用的资源”列表，选择 **com.ibm.commerce.negotiation.commands.BidSubmitCmd**。这是用于创建投标的命令。
6. 单击**添加**将命令添加到资源组。
7. 单击**完成**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

合同方案 1: 除去合同管理员添加或删除合同附件的能力

缺省情况下，商店的合同管理员可添加或删除他们管理的合同的附件。在一些情况下，您可能不希望将此权限授予合同管理员。

在此方案中，将更改定义合同管理员可执行操作的资源级别的策略。要除去合同管理员添加或删除合同附件的权限，需要执行以下操作:

- 使用附录查找定义了合同管理员可执行的操作的资源级别的策略。
- 确定策略的操作组名称。
- 从策略操作组的操作列表中删除添加附件和删除附件的操作。

要执行的步骤

识别资源级别的策略和操作组

1. 查看附录的“合同”下的内容，识别出要更改的资源级别的策略。策略是:

   ContractAdministratorsForOrgExecuteContractManageCommandsOnContractResource
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下策略的操作组的名称 ContractManage。这是需要更改的操作组，以除去添加和删除附件的操作。

从策略的操作组中除去添加和删除附件的操作

1. 单击**访问管理 > 操作组**。
2. 从操作组列表中，选择 **ContractManage**。
3. 单击**更改**显示“更改资源组”页面。
4. 从“选定的操作”列表中，选择以下操作:
   com.ibm.commerce.contract.commands.ContractAttachmentAddCmd
   com.ibm.commerce.contract.commands.ContractAttachmentDeleteCmd。
5. 单击**除去**。
6. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

合同方案 2: 允许合同操作员和合同管理员部署合同

缺省情况下，商店的合同操作员可部署合同。在一些情况下，您可能希望也将此权限授予合同管理员。

访问控制策略的灵活设计提供了实现此更改的若干方法:

- 可创建包含合同操作员和合同管理员的新访问组，并将定义谁可部署合同的策略指定给此新访问组。

- 可将“部署合同”操作添加到该策略，该策略指定合同管理员可执行的操作。
- 可创建新策略，该策略允许合同管理员部署合同。

此方案说明第三种方法。它显示了如何创建授权合同管理员部署合同的新的资源级别的策略。

要创建此策略，需要执行以下操作:

- 使用附录查找授权合同操作员部署合同的资源级别的策略。
- 记下此策略的操作组名称。
- 记下此策略的资源组名称。
- 对“合同管理员”访问组定义新策略，指定来自授权合同操作员部署合同的策略的操作组和资源组。

要执行的步骤

识别要用于新策略的操作组和资源组

1. 查看附录的“合同”下的内容，以查找授权合同操作员部署合同的资源级别的策略。该策略是:
   `ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource`。
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下策略的操作组名称 `ContractDeploy`。这是需要用于定义新策略的操作组。
6. 记下资源组名称 `ContractDataResourceGroup`，这是需要用于定义新策略的资源组。

定义新策略

1. 单击**新建**显示“新建策略”页面。
2. 对于“名称”，指定:
   `ContractAdministratorsForOrgExecuteContractDeployCommandsOnContractResource`
3. 对于“显示名称”，用本地语言环境指定策略的简短描述。
4. 对于“描述”，用本地语言环境指定关于策略作用的更详细描述。
5. 对于“用户组”，单击**查找**并选择 **ContractAdministratorForOrg**。
6. 单击**确定**。
7. 对于“资源组”，选择 **ContractDataResourceGroup**。
8. 对于“操作组”，选择 **ContractDeploy**。
9. 对于“策略类型”，选择**模板策略**将策略指定为模板策略。
10. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

订单方案 1: 仅允许买方创建订单

缺省情况下，允许所有用户对产品创建订单，无论用户在其组织中的位置如何。在一些情况下，您可能希望将创建订单的能力限制在一组受限用户，例如买方组织的雇员。通常，对这些雇员指定了买方组织的买方（购买方）角色。

要将订单创建限制到具有“买方”角色的买方组织成员，需要执行以下操作:

- 使用附录查找指定谁可创建订单的资源级别的策略。
- 将策略的访问组从所有用户更改为具有“买方”角色的那些用户。
- 更新策略的名称、显示名称和描述。
- 识别用于创建订单的命令。
- 使用附录查找用于买方（购买方）的基于角色的策略。此策略定义了具有买方（购买方）角色的用户可执行的命令。必须更新此策略的资源组以允许买方执行创建订单的命令。
- 更新此基于角色的策略的资源组使其包含创建订单的命令。

注: 此资源级别的策略是模板策略。在此方案中，已在根组织级别更改了此模板的主副本。如果希望仅对除根组织以外的特定组织更改它，则必须在更改策略之前将“查看”更改为其它组织。这导致仅对该组织覆盖模板策略。然后为该组织创建新的标准策略，该策略拥有更具限定性的买方（购买方）用户访问组。因为限定性较弱的模板策略仍然在根组织级别适用，因此还必须在该级别覆盖该模板策略。当前，完成此操作的唯一方式是通过手工更新数据库中的 ACORGPOL 表，并运行以下 SQL 语句:

```
insert into ACORGPOL (acpolicy_id, member_id) values ( (select acpolicy_id
 from ACPOLICY where policyname = ' AllUsersExecuteOrderCreateCommands
OnStoreResource'), -2001)
```

要执行的步骤

识别资源级别的策略

1. 查看附录的“订单”下的内容，识别出要更改的资源级别的策略。策略是: AllUsersExecuteOrderCreateCommandsOnStoreResource。
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表，选择 **AllUsersExecuteOrderCreateCommandsOnStoreResource**。记下策略的操作组名称 OrderCreateCommands。这是需要查看的操作组，以查找用于创建订单的命令名称。

更改访问组

1. 单击**更改**显示“更改策略”页面。
2. 对于“用户组”，单击**查找**并选择**买方（购买方）**。
3. 单击**确定**。
4. 更新策略的名称、显示名称和描述以反映对访问组的更改。
5. 单击**确定**。

识别用于创建订单的命令

1. 单击**访问管理 > 操作组**。
2. 从操作组列表中，选择 **OrderCreateCommands**。
3. 单击**更改**显示“更改操作组”页面。记下用于创建订单的命令名称:

   ```
   com.ibm.commerce.order.commands.OrderCopyCmd
    com.ibm.commerce.order.commands.OrderScheduleCmd
    com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
    com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
    com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
   ```

   必须将这些命令添加到包含买方可执行命令列表的资源组中。

   注: 不需要 com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd 命令。

识别买方（购买方）的基于角色的策略

1. 查看附录的“基于角色的策略”下的内容，查找出用于买方（购买方）的基于角色的策略。策略是:
   Buyers(buyside)ExecuteBuyers(buyside)CommandsResourceGroup。
2. 单击**访问管理** > **策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下资源组的名称 Buyers(buyside)CommandsResourceGroup。 这是需要更新的资源组。

更新基于角色的策略中的资源组使其包含用于创建订单的命令

1. 单击**访问管理 > 资源组**。
2. 从资源组列表，选择 **Buyers(buyside)CommandsResourceGroup**。
3. 单击**更改**显示“更改资源组”页面。
4. 单击**下一步**显示“详细信息”页面。
5. 从“可用的资源”列表，选择用于创建订单的以下命令:

   ```
   com.ibm.commerce.order.commands.OrderCopyCmd

   com.ibm.commerce.order.commands.OrderScheduleCmd
    com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
    com.ibm.commerce.orderitems.commands.OrderItemUpdateCmd
    com.ibm.commerce.requisitionlist.commands.RequisitionListSubmitCmd
   ```

6. 单击**添加**。
7. 单击**完成**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

订单方案 2: 仅允许买方管理员修改订单

注: 此方案不适用于 WebSphere Commerce 专业版。

缺省情况下，允许所有用户修改其所创建的订单，无论用户在其组织中的位置如何。在一些情况下，您可能希望只有组织的买方管理员具有修改订单的权限。

在此方案中，将更改资源级别的策略，以及基于角色的策略。要仅允许买方管理员修改属于买方组织成员的订单，需要执行以下操作:

- 使用附录查找指定谁可修改订单的资源级别的策略。
- 将策略的访问组从所有用户更改为具有“买方管理员”角色的那些用户。
- 除去对资源关系的指定以允许买方管理员修改属于其它用户的订单。
- 更新策略的名称、显示名称和描述。
- 识别用于修改订单的命令。
- 使用附录查找用于买方管理员的基于角色的策略。此策略定义了具有买方管理员角色的用户可执行的命令。必须更新此策略的资源组以允许买方管理员执行修改订单的命令。
- 更新此基于角色的策略的资源组使其包含修改订单的命令。

要执行的步骤

识别资源级别的策略

1. 查看附录的“订单”下的内容，识别出要更改的资源级别的策略。策略是: `AllUsersExecuteOrderWriteCommandsOnOrderResource`。
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表中，选择 **AllUsersExecuteOrderWriteCommandsOnOrderResource**。
5. 记下策略的操作组名称 `OrderWriteCommands`。需要查看此操作组以查找用于创建订单的命令名称。

更改访问组

1. 单击**更改**显示“更改策略”页面。
2. 对于“用户组”，单击**查找**并选择**买方管理员**。
3. 单击**确定**。
4. 更新策略的名称、显示名称和描述以反映对访问组的更改。
5. 单击**确定**。

识别用于修改订单的命令

1. 单击**访问管理 > 操作组**。
2. 从操作组列表中，选择 **OrderWriteCommands**。
3. 单击**更改**显示“更改操作组”页面。请记下用于修改订单的命令的名称:

```
com.ibm.commerce.order.commands.OrderCancelCmd
 com.ibm.commerce.order.commands.OrderCopyCmd-Write
 com.ibm.commerce.order.commands.OrderUnlockCmd
```

```
com.ibm.commerce.orderitems.commands.OrderItemAddCmd
com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
```

必须将这些命令添加到包含买方可执行命令列表的资源组中。

注:

a. 不需要 com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd 命令。

b. 将命令 com.ibm.commerce.order.commands.OrderCopyCmd-Write 添加到资源组时，它在“可用的资源”下显示为 com.ibm.commerce.order.commands.OrderCopyCmd。

识别买方管理员角色的基于角色的策略

1. 查看附录的“基于角色的策略”下的内容，查找出用于买方管理员的基于角色的策略。策略是: BuyerAdministratorsExecuteBuyersAdministratorsCommands。
2. 单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 请记下资源组的名称 BuyersAdministratorsCommmandsResourceGroup。

   这是需要更新的资源组的名称。

更新基于角色的策略中的资源组使其包含用于修改订单的命令

1. 单击**访问管理 > 资源组**。
2. 选择 **BuyersAdministratorsCommandsResourceGroup**。
3. 单击**更改**显示“更改资源组”页面。
4. 单击**下一步**显示“详细信息”页面。
5. 从“可用的资源”列表中，选择用于修改订单的命令:

```
com.ibm.commerce.order.commands.OrderCancelCmd
 com.ibm.commerce.order.commands.OrderCopyCmd
 com.ibm.commerce.order.commands.OrderUnlockCmd
 com.ibm.commerce.orderitems.commands.OrderItemAddCmd
 com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
 com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
 com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
```

6. 单击**添加**将命令添加到资源组。
7. 单击**完成**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

订单方案 3: 允许 RMA 核准员核准所有 RMA

缺省情况下，仅允许商店的退货商品授权（RMA）核准员核准他们自己商店的 RMA。在一些情况下，您可能希望允许 RMA 核准员核准任意商店的 RMA。在同一组织拥有数个商店或者同一个人处理多个商店的 RMA 核准时，可能希望这样做。

在此方案中，将创建新的访问组并将它用于新的资源级别的策略。要允许 RMA 核准员对任意商店核准 RMA，需要执行以下操作:

- 使用附录查找允许组织的 RMA 核准员核准其组织的 RMA 的资源级别的策略。
- 记下策略中使用的资源组和操作组的名称。
- 查看策略的访问组 RMAApproversForOrg 并记下它包含的角色。访问组是通过同时将组织和角色用作选择条件定义的。要给予用户跨多个组织执行操作的权限，必须不带组织条件定义访问组。
- 创建新访问组 RMAApprovers，该访问组使用同一些角色，但是不包含组织条件。
- 创建使用下列组成部分的新策略:
  - 新访问组 RMAApprovers
  - 来自现有策略的操作组
  - 来自现有策略的资源组

要执行的步骤

识别要用于定义新策略的操作组和资源组

1. 查看附录的“订单”下的内容，查找出授权 RMAApproversForOrg 核准其商店的 RMA 的资源级别的策略。策略是: RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下策略的操作组名称 RMAApproveCommands。这是将用于定义新策略的操作组。
6. 记下资源组名称 RMADataResourceGroup，这是将用于定义新策略的资源组。
7. 记下访问组名称 RMAApproversForOrg。查看此访问组以查看要包含在新访问组中的角色。

识别要用于新访问组的角色

1. 单击**访问管理 > 访问组**。
2. 从访问组列表中，选择 **RMAApproversForOrg**。
3. 单击**更改**。
4. 选择**条件**显示“条件”页面。
5. 在“选定的角色和组织”下，记下访问组中使用的角色:
   - 客户服务主管
   - 卖方
   - 销售经理
   - 业务经理

6. 单击**取消**返回访问组列表。

定义新访问组

1. 单击**新建**显示新访问组的“详细信息”页面。
2. 对于“名称”，指定 RMAApprovers。
3. 对于“描述”，指定访问组的描述。
4. 对于“父组织”，选择“根组织”。
5. 单击**下一步**显示新访问组的“条件”页面。
6. 单击**基于组织和角色的条件**。
7. 从角色列表中，选择以下角色:
   - **客户服务主管**
   - **卖方**
   - **销售经理**
   - **业务经理**
8. 单击**完成**。

定义新策略

1. 单击**访问管理 > 策略**。
2. 单击**新建**显示“新建策略”页面。
3. 对于“名称”，指定: RMAApproversExecuteRMAApproveCommandsOnRMAResource
4. 对于“显示名称”，用本地语言环境指定策略的简短描述。
5. 对于“描述”，用本地语言环境指定关于策略作用的更详细描述。
6. 对于“用户组”，单击**查找**并选择 **RMAApprovers**。
7. 单击**确定**。
8. 对于“资源组”，选择 **RMADataResourceGroup**。
9. 对于“操作组”，选择 **RMAApproveCommands**。
10. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

成员资格方案 1: 除去用户自注册能力

缺省情况下，如果用户隶属已注册的组织，则允许这些用户自注册。还授权成员资格管理员注册隶属其组织的用户。对于需要严格控制访问的站点，则可能有必要除去自注册能力并要求由成员资格管理员对用户进行注册。

注: 在 WebSphere Commerce 专业版中，仅有三个组织: 根组织、缺省组织和卖方组织。

在此方案中，将除去允许用户自注册的资源级别的策略，但是保留一个策略，该策略允许成员资格管理员注册其组织中的用户。

要删除允许用户自注册的资源级别的策略，请执行以下操作:

- 使用附录查找允许用户自注册的资源级别的策略。
- 删除该策略。

要执行的步骤

删除策略

1. 查看附录的“成员资格”下的内容，查找出允许用户自注册的资源级别的策略。策略是: GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource。
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表中，选择 **GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource**。
5. 单击**删除**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

成员资格方案 2: 仅允许已注册的和已核准的用户更改其地址信息

缺省情况下，如果已核准了用户注册或用户注册是正在审批的核准，则用户可修改其地址信息。在一些情况下，您可能希望只有已注册和已核准的用户可管理其地址。

在此方案中，将如下更改授权用户管理其地址信息的资源级别的策略的访问组:

- 使用附录查找允许用户管理其地址信息的资源级别的策略。
- 更改策略的访问组。

  因为访问组 RegisteredApprovedUsers 不包含任何角色，因此无需为此更改更新基于角色的策略。

要执行的步骤

更改资源级别的策略的访问组

1. 查看附录的“成员资格”下的内容，以查找允许用户管理其地址信息的资源级别的策略。策略是 NonRejectedUsersExecuteAddressManageCommandsOnUserResource。

   注: 非拒绝用户是其注册未被拒绝的用户。其注册已经核准，或者正在审批核准。
2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表中，选择 **NonRejectedUsersExecuteAddressManageCommandsOnUserResource**。
5. 单击**更改**显示“更改策略”页面。
6. 对于“用户组”，单击**查找**并选择 **RegisteredApprovedUsers**。

7. 单击**确定**。
8. 更新策略的名称、显示名称和描述以反映对访问组的更改。
9. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

成员资格方案 3: 允许成员注册员对用户进行注册

缺省情况下，授权组织的成员资格管理员注册其组织的成员。访问组 MemberAdministratorsForOrg 包含若干角色（例如买方管理员和卖方管理员），已授权这些角色执行一系列管理任务。在一些情况下，您可能希望创建单独的一个角色，仅授权该角色注册组织成员:

这里是所涉及步骤的概述:

- 创建新角色，并为其创建新访问组、新资源组和新的基于角色的策略。
- 修改现有的资源级别的策略以使用此新角色。

在此方案中，将执行以下操作:

- 定义名为“成员注册员”的新角色。
- 定义名为 MemberRegistrars 的新访问组，该访问组包含成员注册员角色。
- 使用附录查找允许成员资格管理员注册成员的资源级别的策略。
- 记下其操作组中的操作名称。必须创建具有此操作的新资源组，并将它用于新角色的基于角色的策略。请牢记，在基于角色的策略中，对于操作，操作组仅包含单一操作“执行”。资源组包含可执行的操作（命令）。
- 定义名为 MemberRegistrationCommands 的新资源组，该资源组包含用于注册成员的命令。将在成员注册员角色的基于角色的策略中使用此资源组。
- 为成员注册员定义新的基于角色的策略，该策略使用 MemberRegistrars 访问组和 MemberRegistrationCommands 资源组。
- 修改定义谁可注册成员的资源级别的策略，并将其访问组从 MembershipAdministrators 更改为 MemberRegistrars。

要执行的步骤

定义新角色

1. 从管理控制台，单击**访问管理 > 角色**。
2. 在“角色”页面上，单击**新建**。
3. 对于“名称”，指定“成员注册员”。
4. 对于“描述”，用本地语言环境指定成员注册员角色的描述。
5. 单击**确定**。

定义包含成员注册员角色的新访问组

1. 单击**访问管理 > 访问组**。
2. 在“访问组”页面上，单击**新建**显示新访问组的“详细信息”页面。
3. 对于“名称”，指定：MemberRegistrars。
4. 对于“父组织”，选择“根组织”。
5. 对于“描述”，用本地语言环境指定访问组的描述。
6. 单击**下一步**显示新访问组的“条件”页面。
7. 单击**基于组织和角色**。
8. 从“角色”列表中，选择**成员注册员**。
9. 单击**对于组织**指定该角色必须处于用户自己的组织之内。
10. 单击**完成**。

识别要用于成员注册员的基于角色的策略的资源组的操作

1. 查看附录的“成员资格”下的内容，查找出允许成员资格管理员注册用户的策略。策略是:

   ```
   MembershipAdministratorsForOrgExecuteUserAdminRegistration
   CommandsOnOrganizationResource
   ```

2. 单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下策略的操作组名称 UserAdminRegistration。这是需要查看的操作组以识别用于注册成员的操作。
6. 单击**访问管理 > 操作组**。
7. 从操作组列表中，选择 **UserAdminRegistration**。
8. 单击**更改**显示“更改操作组”页面。
9. 记下用于注册成员的命令名称:
   com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd。

定义要用于成员注册员的基于角色的策略的新资源组

1. 单击**访问管理 > 资源组**显示“资源组”页面。
2. 单击**新建**显示新资源组的“常规”页面。
3. 对于“名称”，指定 UserAdminRegistrationCommands。
4. 对于“显示名称”，用本地语言环境指定资源组的描述。
5. 对于“描述”，用本地语言环境指定资源组的更详细描述。
6. 对于“类型”，选择**显式资源组**。
7. 单击**下一步**。
8. 单击**下一步**显示新资源组的“详细信息”页面。
9. 从“可用的资源”列表中，选择以下资源:

   com.ibm.commerce.usermanagement.commands.
   UserRegistrationAdminAddCmd

10. 单击**添加**。
11. 单击**完成**。

定义成员注册员角色的基于角色的策略

1. 单击**访问管理 > 策略**。
2. 在“策略”页面上，单击**新建**。
3. 对于“名称”，指定 **MemberRegistrarsExecuteUserAdminRegistrationCommands**。
4. 对于“显示名称”，用本地语言环境指定策略的描述。
5. 对于“描述”，用本地语言环境指定关于策略作用的更详细描述。
6. 对于“用户组”，单击**查找**并选择 **MemberRegistrars**。
7. 单击**确定**。
8. 对于“资源组”，选择 **UserAdminRegistrationCommands**。
9. 对于“操作组”，选择 **ExecuteCommandActionGroup**。
10. 单击**确定**。

修改资源级别的策略以使用新访问组

1. 从策略列表中，选择以下策略:

   MembershipAdministratorsForOrgExecuteUserAdminRegistration CommandsOnOrganizationResource

   .
2. 单击**更改**显示“更改策略”页面。
3. 更新策略的名称、显示名称和描述以反映对访问组的更改。
4. 对于“用户组”，单击**查找**并选择 **MemberRegistrars**。
5. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

赠券方案 1: 仅允许买方兑换赠券

缺省情况下，允许所有注册用户兑换赠券。在一些情况下，您可能希望将赠券兑换限制到 WebSphere Commerce 中具有“买方”角色的用户。

在此方案中，将更改资源级别的策略及其关联的基于角色的策略。要将赠券兑换限制到具有“买方”角色的用户，需要执行以下操作:

- 使用附录查找指定谁可兑换赠券的资源级别的策略。
- 将策略的访问组从所有注册用户更改为具有“买方”角色的那些用户。
- 识别用于兑换赠券的命令。
- 使用附录查找用于买方（购买方）的基于角色的策略。此策略定义了具有买方（购买方）角色的用户可执行的命令。必须更新此策略的资源组以允许买方执行兑换赠券的命令。
- 更新此基于角色的策略的资源组使其包含兑换赠券的命令。

要执行的步骤

识别资源级别的策略及其操作组

1. 查看附录的“赠券”下的内容，识别出要更改的资源级别的策略。策略是:

   RegisteredApprovedUsersExecuteCouponRedemptionCommandsOnCouponWalletResource

2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表中，选择以下策略:

   RegisteredApprovedUsersExecuteCouponRedemption CommandsOnCouponWalletResource

5. 记下策略的操作组名称 CouponRedemption。这是必须查看的操作组以查找兑换赠券的命令名称。

更改访问组

1. 单击**更改**显示“更改策略”页面。
2. 对于“用户组”，单击**查找**并选择**买方（购买方）**。
3. 单击**确定**。
4. 更新策略的名称、显示名称和描述以反映对访问组的更改。
5. 单击**确定**。

识别用于兑换赠券的命令

1. 单击**访问管理 > 操作组**。
2. 从操作组列表中，选择 **CouponRedemption**。
3. 单击**更改**显示“更改操作组”页面。记下用于创建投标的命令名称:

   com.ibm.commerce.couponredemption.commands.CouponDSSCmd
   com.ibm.commerce.couponredemption.commands.UseCouponIdCmd

   必须将这些命令添加到包含买方可执行命令列表的资源组中。

识别买方（购买方）的基于角色的策略

1. 查看附录的“基于角色的策略”下的内容，查找出用于买方（购买方）的基于角色的策略。策略是:

   Buyers(buy-side)ExecuteBuyers(buyside)CommandsResourceGroup

2. 单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下资源组名称: Buyers(buyside)CommandsResourceGroup。 这是需要更新的资源组的名称。

更新基于角色的策略中的资源组使其包含用于创建投标的命令

1. 单击**访问管理 > 资源组**。
2. 选择 **Buyers(buy-side)CommandsResourceGroup**。
3. 单击**更改**显示“更改资源组”页面。
4. 单击**下一步**显示“详细信息”页面。

5. 从“可用的资源”列表，选择 **com.ibm.commerce.couponredemption.commands.CouponDSSCmd** **com.ibm.commerce.couponredemption.commands.UseCouponIdCmd**. 这些是用于兑换赠券的命令。
6. 单击**添加**将命令添加到资源组。
7. 单击**完成**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

赠券方案 2: 允许赠券管理员和商店管理员创建电子赠券促销

缺省情况下，商店的赠券管理员可为其商店创建电子赠券促销。在一些情况下，您可能希望也授予商店管理员此权限。

访问控制策略的灵活设计提供了实现此更改的若干方法:

- 可将商店管理员角色添加到指定了谁可创建电子赠券促销的策略的访问组。
- 可创建新策略，该策略允许商店管理员创建电子赠券促销。

此方案说明了第一种方法。它显示了如何将商店管理员角色添加到授权赠券管理员创建赠券的资源级别的策略。

要进行此更改，需要执行以下操作:

- 使用附录查找指定谁可创建电子赠券促销的资源级别的策略。
- 更改策略的访问组以包含具有“商店管理员”角色的用户。
- 查看资源级别的策略的操作组以识别用于创建电子赠券促销的命令。
- 使用附录查找用于“商店管理员”的基于角色的策略。此策略定义了具有“商店管理员”角色的用户可执行的命令。必须更新此策略的资源组以允许商店管理员执行创建电子赠券促销的命令。
- 更新此基于角色的策略的资源组使其包含创建电子赠券促销的命令。

要执行的步骤

识别资源级别的策略的操作组和访问组

1. 查看附录的“拍卖”下的内容，识别出要更改的资源级别的策略。策略是:

   CouponAdministratorsForOrgExecuteCouponPromotionCreateCommands OnStoreEntityResource

2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下策略的操作组的名称 CouponPromotionCreate。这是必须查看的操作组以查找用于创建电子赠券促销的命令名称。

6. 记下策略的访问组名称 CouponAdministratorsForOrg。这是必须更新的访问组以包含商店管理员角色。

更改访问组

1. 单击**访问管理 > 访问组**。
2. 从访问组列表，选择 **CouponAdministratorsForOrg**
3. 单击**更改**显示“详细信息”页面。
4. 单击**条件**显示“条件”页面。
5. 从“角色”列表，选择**商店管理员**。
6. 单击**对于组织**指定该角色必须处于用户自己的组织之内。
7. 单击**添加**。
8. 单击**确定**。

识别用于创建电子赠券促销的命令

1. 单击**访问管理 > 操作组**。
2. 从操作组列表中，选择 **CouponPromotionCreate**。
3. 单击**更改**显示“更改操作组”页面。记下用于创建电子赠券促销的命令名称 com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd。 必须将此命令添加到包含商店管理员可执行命令列表的资源组中。

识别商店管理员的基于角色的策略

1. 查看附录的“基于角色的策略”下的内容，查找出用于商店管理员的基于角色的策略。 策略是：StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup。
2. 单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下其资源组的名称 StoreAdministratorsCmdResourceGroup。 这是需要更新的资源组的名称。

更新基于角色的策略中的资源组使其包含用于创建电子赠券促销的命令

1. 单击**访问管理 > 资源组**。
2. 选择 **StoreAdministratorsCmdResourceGroup**。
3. 单击**更改**显示“更改资源组”页面。
4. 单击**下一步**显示“详细信息”页面。
5. 从“可用的资源”列表中，选择 com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd。这是用于创建电子赠券促销的命令。
6. 单击**添加**。
7. 单击**完成**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

采购方案 1: 允许采购购物车经理为由其组织创建的订单管理采购购物车

注: 此方案不适用于 WebSphere Commerce 专业版。

缺省情况下，授权采购购物车经理在创建了订单时管理采购购物车。在一些情况下，您可能希望扩展采购购物车经理的权限以便让他们为由其组织的任何成员创建的订单管理采购购物车。

要进行此更改，需要执行以下操作:

- 使用附录查找授权采购购物车管理员管理采购购物车的资源级别的策略。
- 将此策略的资源关系从“创建者”更改为“与创建者相同的组织实体”。

要执行的步骤

更改资源级别的策略的资源关系

1. 查看附录的“采购”下的内容，查找出授权采购购物车经理为订单管理采购购物车的资源级别的策略。策略是:

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   CartManageOnOrderResource
   ```

2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 从策略列表中，选择以下策略:

   ProcurementShoppingCartManagersExecuteProcurementShopping CartManageOnOrderResource

5. 单击**更改**显示“更改策略”页面。
6. 对于“关系”，选择 **sameOrganizationalEntityAsCreator**。
7. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

采购方案 2: 允许采购买方管理员为由其组织创建的订单提交采购购物车

注: 此方案不适用于 WebSphere Commerce 专业版。

缺省情况下，采购购物车经理在其创建了订单时可保存或提交采购购物车。在一些情况下，您可能希望对这些任务划分职责。您可以允许采购购物车经理保存包含其已创建订单的采购购物车，但是给予与订单创建者处于同一组织中的采购买方管理员提交采购购物车的权限。如果希望采购买方管理员在提交计划的购买之前对其进行复查，则这可能是有益的。

要进行此更改，需要执行以下操作:

- 使用附录查找将采购购物车经理授权为中心经理以管理实现中心的资源级别的策略。
- 从策略的操作组中除去用于提交采购购物车的操作。
- 定义新的操作组，该操作组包含用于提交采购购物车的命令。将使用此操作组定义新的资源级别的策略，该策略授权采购买方管理员在与订单创建者处于同一组织的情况下可提交采购购物车。
- 创建新的资源级别的策略，该策略授权采购买方管理员在与订单创建者处于同一组织的情况下可提交采购购物车。

要执行的步骤

识别资源级别的策略的操作组和资源组

1. 查看附录的“采购”下的内容，查找出授权采购购物车经理为订单管理采购购物车的资源级别的策略。策略是:

   ```
   ProcurementShoppingCartManagersExecuteProcurement
   ShoppingCartManageOnOrderResource
   ```

2. 从管理控制台，单击**访问管理 > 策略**。
3. 在策略列表中查找策略。
4. 记下其操作组的名称 ProcurementShoppingCartManage。将更新此操作组以除去用于提交采购购物车的操作。
5. 记下其资源组的名称 OrderDataResourceGroup。将使用此资源组定义新的资源级别的策略。

更新资源级别的策略的操作组

1. 单击**访问管理 > 操作组**。
2. 从操作组列表，选择 **ProcurementShoppingCartManage**。
3. 单击**更改**显示“更改操作组”页面。
4. 从“选定的操作”列表，选择 **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**。 将创建具有此操作的新操作组，并将该操作组用于新的资源级别的策略。
5. 单击**除去**。
6. 单击**确定**。

定义新操作组

1. 单击**访问管理 > 操作组**。
2. 单击**新建**显示“新建操作组”页面。
3. 对于“名称”，指定 ProcurementShoppingCartSubmit。
4. 对于“显示名称”，用本地语言环境指定操作组的简短描述。

5. 对于“描述”，用本地语言环境指定关于操作组作用的更详细描述。
6. 从“可用的操作”列表，选择 **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**。
7. 单击**添加**。
8. 单击**确定**。

定义新策略

1. 单击**访问管理 > 策略**。
2. 对于“查看”，单击**根组织**以显示站点级别的策略。
3. 单击**新建**显示“新建策略”页面。
4. 对于“名称”，指定:

   ```
   ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmitCommands
   OnOrderResource
   ```

5. 对于“显示名称”，用本地语言环境指定策略的简短描述。
6. 对于“描述”，用本地语言环境指定关于策略作用的更详细描述。
7. 对于“用户组”，单击**查找**并选择 **ProcurementBuyerAdministrators**。
8. 单击**确定**。
9. 对于“资源组”，选择 **OrderDataResourceGroup**。
10. 对于“操作组”，选择 **ProcurementShoppingCartSubmit**。
11. 对于“关系”，选择 **sameOrganizationalEntityAsCreator**。
12. 对于“策略类型”，选择**模板策略**将策略指定为模板策略。
13. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

库存方案 1: 允许实现中心经理更新实现中心但是不能删除它们

缺省情况下，授权实现中心经理更新或删除与其商店关联的实现中心。在一些情况下，您可能希望允许实现中心经理更新实现中心，但是不能删除它们。

要进行此更改，需要执行以下操作:

- 使用附录查找授权实现中心经理管理实现中心的资源级别的策略。
- 从策略的操作组中除去用于删除实现中心的操作。

要执行的步骤

除去用于删除实现中心的操作

1. 查看附录的“采购”下的内容，查找出授权采购购物车经理为订单管理采购购物车的资源级别的策略。策略是:

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenter
   ManageCommandsOnFulfillmentResource
   ```

2. 从管理控制台，单击**访问管理 > 策略**。
3. 在策略列表中查找策略。
4. 记下其操作组的名称 FulfillmentCenterManage。需要更新此操作组以除去用于删除实现中心的操作。
5. 单击**访问管理 > 操作组**。
6. 从操作组列表中，选择 **FulfillmentCenterManage**。
7. 单击**更改**显示“更改操作组”页面。
8. 从“选定的操作”列表中，选择 **com.ibm.commerce.inventory.commands.FulfillmentCenterDeleteCmd**。
9. 单击**除去**。
10. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

库存方案 2: 仅允许后勤部经理和业务经理创建、更新或删除实现中心

缺省情况下，授权实现中心经理创建、更新或删除与其商店关联的实现中心。实现中心访问组包含以下角色：卖方、后勤部经理和业务经理。在一些情况下，您可能不希望将卖方授权为实现中心经理。

要进行此更改，需要执行以下操作:

- 使用附录查找授权实现中心经理管理实现中心的资源级别的策略。
- 从“实现中心经理”访问组定义中除去卖方角色。

要执行的步骤

从访问组除去卖方角色

1. 查看附录的“采购”下的内容，查找出授权采购购物车经理为订单管理采购购物车的资源级别的策略。策略是:

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage
   CommandsOnFulfillmentResource
   ```

2. 从管理控制台，单击**访问管理 > 访问组**。
3. 从访问组列表，选择 **FulfillmentCenterManagersForOrg**。
4. 单击**更改**显示“更改访问组”页面。
5. 单击**访问管理 > 访问组**。
6. 单击**更改**显示“详细信息”页面。
7. 单击**条件**显示“条件”页面。
8. 从“角色”列表，选择**卖方**。
9. 单击**除去**。
10. 单击**确定**。

使用更改更新访问控制策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. 单击**更新**。

商务智能方案 1: 允许审计员查看商务智能报表

缺省情况下，允许智能报表查看员查看其商店的商务智能报表。在一些情况下，您也可能希望创建名为“审计员”的新角色，并授权具有此角色的用户查看商店的商务智能报表。

这里是所涉及步骤的概述:

- 创建新角色，并为其创建新访问组、新资源组和新的基于角色的策略。
- 将新角色添加到资源级别的策略的访问组。
- 定义名为“审计员”的新角色。
- 定义名为 Auditors 的新访问组，该访问组包含审计员角色。
- 将审计员角色添加到资源级别的策略的访问组，该策略定义谁可查看其商店的商务智能报表。

在此方案中，将执行以下操作:

- 使用附录查找允许商务智能报表查看员查看商务智能报表的资源级别的策略。
- 记下其操作组中的操作名称。必须创建具有此操作的新资源组，并将它用于新角色的基于角色的策略。请牢记，在基于角色的策略中，对于操作，操作组仅包含单一操作“执行”。资源组包含可执行的操作（命令）。
- 定义名为 AuditorCommands 的新资源组，该资源组包含用于查看商务智能报表的命令。将在审计员角色的基于角色的策略中使用此资源组。
- 为审计员定义新的基于角色的策略，该策略使用 Auditors 访问组和 AuditorCommands 资源组。
- 将审计员角色添加到资源级别的策略的访问组，该策略定义谁可查看其商店的商务智能报表。

要执行的步骤

定义新审计员角色

1. 从管理控制台，单击**访问管理 > 角色**。
2. 在“角色”页面上，单击**新建**。
3. 对于“名称”，指定“审计员”。
4. 对于“描述”，用本地语言环境指定对审计员角色的描述。
5. 单击**确定**。

为审计员角色定义新访问组

1. 单击**访问管理 > 访问组**。
2. 在“访问组”页面上，单击**新建**显示新访问组的“详细信息”页面。
3. 对于“名称”，指定 Auditors。

4. 对于“描述”，用本地语言环境指定访问组的描述。
5. 对于“父组织”，选择“根组织”。
6. 单击**下一步**显示新访问组的“条件”页面。
7. 单击**基于组织和角色**。
8. 从“角色”列表，选择**审计员**。
9. 单击**添加**。
10. 单击**完成**。

识别要用于审计员角色的基于角色的策略的资源组的操作

1. 在附录的“商务智能”下查看，以查找授权智能报表查看员查看商务智能报表的策略。策略是:

   ```
   IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport
   CommandsOnStoreEntityResource
   ```

2. 从管理控制台，单击**访问管理 > 策略**。
3. 对于“查看”，选择**根组织**以显示站点级别的策略。
4. 在列表中查找策略。
5. 记下策略的操作组名称 `ViewBusinessIntelligenceReport`。这是必须查看的操作组以识别用于注册成员的操作。
6. 单击**访问管理 > 操作组**。
7. 从操作组列表，选择 **ViewBusinessIntelligenceReport**。
8. 单击**更改**显示“更改操作组”页面。
9. 记下用于查看商务智能报表的命令名称 `com.ibm.commerce.bi.commands.BIShowReportCmd`。

定义要用于审计员角色的基于角色的策略的新资源组

1. 单击**访问管理 > 资源组**显示“资源组”页面。
2. 单击**新建**显示新资源组的“常规”页面。
3. 对于“名称”，指定 AuditorCommands。
4. 对于“显示名称”，用本地语言环境指定资源组的描述。
5. 对于“描述”，用本地语言环境指定资源组的更详细描述。
6. 单击**下一步**。
7. 对于“类型”，选择**显式资源组**。
8. 单击**下一步**显示新资源组的“详细信息”页面。
9. 从“可用的资源”列表，选择 **com.ibm.commerce.bi.commands.BIShowReportCmd**。
10. 单击**添加**。
11. 单击**完成**。

为审计员角色定义基于角色的策略

1. 单击**访问管理 > 策略**。
2. 在“策略”页面上，单击**新建**。
3. 对于“名称”，指定 **AuditorsExecuteAuditorCommands**。

4. 对于“显示名称”，用本地语言环境指定策略的描述。
5. 对于“描述”，用本地语言环境指定关于策略作用的更详细描述。
6. 对于“用户组”，单击**查找**并选择 **Auditors**。
7. 单击**确定**。
8. 对于“资源组”，选择 **AuditorCommands**。
9. 对于“操作组”，选择 **ExecuteCommandActionGroup**。
10. 单击**确定**。

将审计员角色添加到资源级别的策略的访问组

1. 单击**访问管理 > 访问组**。
2. 从访问组列表，选择 **IntelligenceReportViewersForOrg**。
3. 单击**更改**显示“更改访问组”页面。
4. 单击**条件**显示访问组的“条件”页面。
5. 从“角色”列表，选择**审计员**。
6. 单击**对于组织**指定该角色必须处于用户自己的组织之内。
7. 单击**添加**。
8. 单击**确定**。

使用更改更新策略注册表

1. 单击**配置 > 注册表**。
2. 从注册表列表中，选择**访问控制策略**。
3. **单击“更新”。**

第 6 章 使用 XML 文件定制访问控制策略

WebSphere Commerce 管理控制台允许对访问控制策略及其组成部分作简单的更改。要作更为复杂的更改，则需要直接编辑 XML 文件。

在开始对用于访问控制的 XML 文件作更改之前，应当阅读《*IBM WebSphere Commerce 程序员指南*》中关于访问控制的一章。该章提供了对访问控制的技术性概述，并说明了如何创建可受访问控制策略保护的已定制命令、实体 bean 和 JSP 模板。

一旦遵循《*IBM WebSphere Commerce 程序员指南*》中所提供的指南完成了代码定制，则可编辑用于访问控制的 XML 文件以建立所需的保护。

仅可通过编辑和装入 XML 文件作出的更改

以下更改仅可通过编辑然后装入相应的 XML 文件作出:

- 保护新命令或视图
- 创建或修改关系
- 创建或修改关系组
- 保护新资源
- 创建或修改属性
- 创建或修改使用复杂条件的访问组
- 使用复杂条件创建或修改资源组

关于访问控制的 XML 文件

下表显示了 WebSphere Commerce XML 文件、DTD 文件以及用于 XML 转换程序的 XSL 文件的名称和描述。

表 4. 用于访问控制的 WebSphere Commerce XML 文件

文件名	描述
ACUserGroups_de_DE.xmll ACUserGroups_en_US.xml ACUserGroups_es_ES.xml ACUserGroups_fr_FR.xml ACUserGroups_it_IT.xml ACUserGroups_ja_JP.xml ACUserGroups_ko_KR.xml ACUserGroups_pt_BR.xml ACUserGroups_zh_CN.xml ACUserGroups_zh_TW.xml	以每种支持语言表述的访问组定义和描述。
defaultAccessControlPolicies.xml	包含缺省访问控制策略、操作组、资源组、关系、关系组、操作、资源类别以及属性的定义的主文件。
defaultAccessControlPolicies_de_DE.xml defaultAccessControlPolicies_en_US.xml defaultAccessControlPolicies_es_ES.xml defaultAccessControlPolicies_fr_FR.xml defaultAccessControlPolicies_it_IT.xml defaultAccessControlPolicies_ja_JP.xml defaultAccessControlPolicies_ko_KR.xml defaultAccessControlPolicies_pt_BR.xml defaultAccessControlPolicies_zh_CN.xml defaultAccessControlPolicies_zh_TW.xml	包含以每种支持语言表述的缺省访问控制策略、操作组、操作、资源组、资源类别、关系以及属性的显示名称和描述的文件。
ACPoliciesfilter.xml	用于从数据库抽取已更改的访问控制信息的过滤文件。
accesscontrolpolicies.dtd	访问控制策略 XML 文件必须符合此 DTD。
accesscontrolpoliciesnls.dtd	访问控制策略 NLS（特定于本地语言）XML 文件（仅显示名称和描述）必须符合此 DTD。
ACUserGroups_en_US.dtd	访问控制用户组 XML 文件必须符合此 DTD。
accesscontrol.xsl	用于访问控制策略 XML 文件的 XSL 转换规则文件。

表 4. 用于访问控制的 WebSphere Commerce XML 文件 (续)

accesscontrolnls.xsl	用于访问控制策略 NLS XML 文件（仅显示名称和描述）的 XSL 转换规则文件。
ACUserGroup.xsl	用于访问组 XML 文件的 XSL 转换规则文件。
wcstoacpolicies.xsl	用于抽取之后的 ExtractedACPolicies.xml 文件以创建访问控制策略 XML 文件的 XSL 转换规则文件。
wcstoacpoliciesnls.xsl	用于抽取之后的 ExtractedACPolicies.xml 以创建访问控制策略 NLS XML 文件的 XSL 转换规则文件。
wcstoacusergroup.xsl	用于抽取之后的 ExtractedACPolicies.xml 文件以创建访问组 XML 文件的 XSL 转换规则文件。

定制 XML 文件

保护视图

直接从 URL 调用或者作为来自另一命令的重定向而启动的所有视图，都需要基于角色的访问控制策略以便得到显示。以下示例显示用于视图的基于角色的策略:

```
<Policy Name="ProductManagersExecuteProductManagersViews"
OwnerID="RootOrganization"
UserGroup="ProductMangers"
ActionGroupName="ProductMangersViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

ResourceGroup 名称 ViewCommandResourceGroup 指示这是用于视图的基于角色的策略。策略声明 ProductManagers 用户组中的用户可显示 ProductMangersViews 操作组中的视图。

以下是 ProductMangersViews 操作组的示例:

```
<ActionGroup Name="ProductManagersViews"
OwnerID="RootOrganization">

<ActionGroupAction Name="ProductImageView"/>
<ActionGroupAction Name="ProductManufacturerView"/>
<ActionGroupAction Name="ProductSalesTaxView"/>

 </ActionGoup>
```

上面示例列出在 ProductManagerViews 操作组中的可执行的三个操作: ProductImageView、ProductManufacturerView 和 ProductSalesTaxView。

以下是 ProductImageView 操作定义的示例:

```
<Action Name="ProductImageView"
CommandName="ProductImageView">
</Action>
```

Name 属性 ProductImageView 用作在 XML 的其它位置（例如将该操作与操作组关联时）引用该操作的标记。

注: 存储在 VIEWREG 表的 VIEWNAME 列中的视图名称必须与操作定义中的 CommandName 匹配。CommandName 的值存储在 ACACTION 表的 ACTION 列。Name 和 CommandName 属性无需是相同的。

添加使用现有策略的新视图

要添加可由具有现有的基于角色的“视图”策略的角色来访问的新视图，请执行以下操作:

1. 在具有视图名称 MyNewView 的 XML 文件中创建新操作定义。

   ```
   <Action Name="MyNewView"
   CommandName="MyNewView">
   </Action>
   ```

2. 确定哪些角色应当具有对此视图的访问权，并在 XML 文件中将新操作与对应的操作组关联:

   ```
   <ActionGroup Name="ProductManagersViews"
   OwnerID="RootOrganization">

   <ActionGroupAction Name="ProductImageView"/>
   <ActionGroupAction Name="ProductManufacturerView"/>
   <ActionGroupAction Name="ProductSalesTaxView"/>
   <ActionGroupAction Name="MyNewView"/>

   </ActionGroup>
   ```

3. 将 XML 更改装入数据库。关于装入 XML 更改的更多信息，请参阅第 91 页的『将更改装入数据库』。
4. 在管理控制台中更新访问控制策略注册表。

因为已有基于角色的策略包含了此操作组，因此现在可以使用该视图。

添加使用新策略的新视图

要添加可由不具有现有的基于角色的策略的新角色来访问的新视图，请执行以下操作:

1. 在具有视图名称 MyNewView 的 XML 文件中创建新操作定义。

   ```
   <Action Name="MyNewView
   CommandName="MyNewView">
   </Action>
   ```

2. 创建要与新角色关联的新操作组:

   ```
   <ActionGroupName="XYZViews"
   OwnerID="RootOrganization">
   </ActionGroup>
   ```

3. 将新操作与新操作组关联:

   ```
   <ActionGroupName="XYZViews"
   OwnerID="RootOrganization">

   <ActionGroupAction Name="MyNewView"/>

   </ActionGroup>
   ```

4. 创建引用新操作组的策略:

```
<Policy Name="XYZExecuteXYZViews"
OwnerID="RootOrganization"
UserGroup="XYZ"
ActionGroupName="XYZViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

5. 将 XML 更改装入数据库。关于装入 XML 更改的更多信息，请参阅第 91 页的『将更改装入数据库』。
6. 在管理控制台中更新访问控制策略注册表。

现在可使用该视图。

保护控制器命令

所有的控制器命令都需要基于角色的访问控制策略以便得到执行。如果控制器命令或任务命令正在执行资源级别的检查，则该命令还需要资源级别的策略。关于更多信息，请参阅第 75 页的『实现资源级别的访问控制』。以下示例显示了用于控制器命令的基于角色的策略:

```
<Policy Name="SellersExecuteSellersCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="Sellers"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="SellersCmdResourceGroup">
</Policy>
```

ActionGroupName ExecuteCommandActionGroup 指示这是用于控制器命令的基于角色的策略。策略声明 Sellers 访问组中的用户可执行 SellersCmdResourceGroup 资源组中的命令。

以下是 SellersCmdResourceGroup 资源组定义的示例:

```
<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CancelCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CloseCmdResourceCategory"/>
<ResourceGroupResource Name="com.ibm.contract.commands.Contract
CreateCmdResourceCategory"/>
</ResourceGroup>
```

上面示例显示了资源组中的以下三个资源（每个资源都与一个控制器命令相对应）:

- com.ibm.contract.commands.ContractCancelCmdResourceCategory
- com.ibm.contract.commands.ContractCloseCmdResourceCategory
- com.ibm.contract.commands.ContractCreateCmdResourceCategory

以下是资源的样本定义:

```
<ResourceCategory Name="com.ibm.commerce.contract.commands.Contract
CloseCmdResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.commands.ContractCloseCmd">

<ResourceAction Name="ExecuteCommand"/>

</ResourceCategory>
```

Name 属性 com.ibm.commerce.contract.commands.ContractCloseCmdResourceCategory 在 XML 文件中用作引用资源的标记。ResourceAction 名称 ExecuteCommand 用于指定

可对资源实施的操作。当使用访问控制策略填充与特定资源对应的“操作”选择框时，在管理控制台中要使用此信息。在此例中，指定了操作 Execute。在以下语句中定义了 Execute 操作:

```
<Action Name="ExcecuteCommand
CommandName="Execute">
</Action>
```

注: 控制器命令的接口名称必须与资源定义中的 ResourceBeanClass 匹配。ResourceBeanClass 的值存储在 ACRESCGRY 表的 RESCLASSNAME 列中。这些命令可用作资源，因为它们扩展 ControllerCommand 接口，该接口扩展 AccCommand 接口，后者再扩展 Protectable 接口。关于这些接口的更多信息，请参阅《*IBM WebSphere Commerce 程序员指南*》。

添加使用现有策略的新控制器命令

要添加可由具有现有的基于角色的控制器命令策略的角色访问的新控制器命令，请执行以下操作:

1. 在与控制器命令的接口名称对应的 XML 文件中，创建新的资源定义。

   ```
   <ResourceCategory  Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
   ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">
   <ResourceAction Name="ExecuteCommand"/>
   </ResourceCategory>
   ```

2. 确定哪些角色应当具有对命令的访问权，并在 XML 文件中将新资源与对应的资源组关联:

   ```
    <ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
   <ResourceGroupResource Name="com.ibm.commerce.contract.
   commands.ContractCancelCmdResourceCategory"/>
   <ResourceGroupResource Name="com.ibm.commerce.contract.
   commands.ContractCloseCmdResourceCategory"/>
   <ResourceGroupResource Name="com.ibm.commerce.contract.
   commands.ContractCreateCmdResourceCategory"/>

   <ResourceGroupResource Name="com.xyz.commands.
   MyNewControllerCmdResourceCategory"/>

   </ResourceGroup>
   ```

3. 将 XML 更改装入数据库。关于装入 XML 更改的更多信息，请参阅第 91 页的『将更改装入数据库』。
4. 在管理控制台中更新访问控制策略注册表。

因为已有基于角色的策略包含了此资源组，因此现在可以使用新控制器命令（如果它未在执行任何资源级别的检查）。

添加使用新策略的新控制器命令

要添加可由新角色访问且不具有现有的基于角色的策略的新控制器命令，请执行以下操作:

1. 在与控制器命令的接口名称对应的 XML 文件中，创建新的资源定义。请参阅『添加使用现有策略的新控制器命令』步骤 1 以获取示例。
2. 创建要与新角色关联的新资源组:

   ```
   <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
   </ResourceGroup>
   ```

3. 将新资源与新资源组关联:

```
<ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.xyz.commands.MyNewControllerResourceCategory"/>
</ResourceGroup>
```

4. 创建引用新资源组的策略:

```
<Policy Name="XYZExecuteXYZsCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="XYZ"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="XYZCmdResourceGroup">
</Policy>
```

5. 将 XML 更改装入数据库。关于装入 XML 更改的更多信息，请参阅第 91 页的『将更改装入数据库』。
6. 在管理控制台中更新访问控制策略注册表。

现在可以使用该控制器命令（如果它未在执行任何资源级别的检查）。

实现资源级别的访问控制

可将资源级别访问控制添加到控制器或任务命令。资源级别的检查是在 WebSphere Commerce 运行时基于命令的 getResources() 方法返回的数据完成的。资源级别的检查也可在命令的 performExcecute() 部分期间完成，方法是使用 void checkIsAllowed(Object resource, String action) throws ECException 方法直接调用访问控制策略管理器。此方法在不允许当前用户对指定资源执行指定操作的情况下将抛出 ECApplicationException。

注: 缺省情况下，getResources() 方法返回空值，且不执行资源级别的检查。

在以下实例中，需要为新命令创建资源级别的策略:

- 新命令从执行资源级别的检查的另一命令扩展而来。
- 新命令本身执行资源级别的访问控制检查。

以下是资源级别的策略的示例:

```
<Policy Name="ContractMangersForOrgExecuteContractManageCommandsOnContractResource"
OwnerID="RootOrganization"
UserGroup="ContractManagersForOrg"
ActionGroupName="ContractManage"
ResourceGroupName="ContractDataResourceGroup"
PolicyType="template">
</Policy>
```

其中:

Name: 策略的名称。

PolicyType: 策略类型。这是模板策略，且将动态应用于拥有资源的组织实体及其上级组织。

OwnerID: 拥有策略的成员。这是模板策略，且将动态更改为资源所拥有的组织实体及其上级，因为该策略是由访问控制策略管理器应用的。

UserGroup: 策略适用于该组的用户。用于以下访问组的命名约定是将 ForOrg 附加到组名上: 在这些访问组中角色的作用域动态地更改为资源组织实体及其上级组织。

ActionGroupName: 包含了要对资源执行的操作的操作组的名称。

ResourceGroupName: 包含了要对其实施操作的资源的资源组的名称。

在上面示例中，操作组 ContractManage 是包含了将对 ContractDataResourceGroup 实施的一组命令的操作组。以下是用于上述资源级别的策略的操作组的示例:

```
<ActionGroupName="ContractManage" OwnerID="RootOrganization">
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
<ActionGroupActionName="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
</ActionGroup>
```

先前对于基于角色的策略定义为资源的命令现在定义为操作。以下是系上述 ContractManage 组一部分的一个操作的样本定义:

```
<Action Name="com.ibm.commerce.contract.commands.ContractCloseCmd"
CommandName="com.ibm.commerce.contract.commands.ContractCloseCmd">
</Action>
```

注: CommandName 的值应当对应于执行资源级别的检查的命令的接口名称。

大多数命令使用企业 bean。这些 bean 通常是受资源级别的策略保护的资源。以下是用于上述资源策略的资源组的样本定义:

```
<ResourceGroup Name="ContractDataResourceGroup" OwnerId="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.contract.
objects.ContractResourceCategory"/>
</ResourceGroup>
```

在此示例中定义了 ContractDataResourceGroup，且它由一个资源组成。资源定义如下:

```
<ResourceCategory Name="com.ibm.commerce.contract.objects.ContractResourceCategory"
ResourceBeanClass="com.ibm.commerce.contract.objects.Contract"
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractCancelCmd"/>
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractCloseCmd"/>
<ResourceAction Name="com.ibm.commerce.contract.commands.ContractDeleteCmd"/>
 </ResourceCategory>
```

其中:

Name: 用于在 XML 文件的其它位置引用此资源的标记。

ResourceBeanClass: 表示要保护资源的类。此类必须实现 Protectable 接口。如果资源是企业 bean，则其远程接口应当扩展 Protectable 接口。

ResourceAction: 指定将对此资源执行的操作。管理控制台在确定哪些操作对特定资源有效时使用此信息。

注: 关于 Protectable 接口的更多信息，请参阅《*WebSphere Commerce 程序员指南*》。

保护数据 bean

数据 bean 包含关于商务对象的信息且用于在 Web 页面上显示对象信息。动态 Web 页面通常映射为 WebSphere Commerce 中的视图，这些视图受基于角色的策略的保护。有时有必要通过保护 Web 页面的数据 bean（如果存在），来进一步保护 Web 页面的内容。

当使用 DataBeanManager.activate(..) 方法填充数据 bean 时，数据 bean 管理器强制实施对这些数据 bean 的访问控制。可使用 Delegator 接口对数据 bean 实施直接或

间接的保护。受直接保护的数据 bean 还实现 Protectable 接口。如果受间接保护的数据 bean 未实现 Delegator 接口，或者对 getDelegate() 方法返回空值，则它并不受保护且任何人都可以显示它。

注: 关于 Protectable 接口的更多信息，请参阅《*WebSphere Commerce 程序员指南*》。

以下是用于数据 bean 的资源级别的策略的示例:

```
<Policy Name="AllUsersDisplayOrderDataBeanResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="DisplayDataBeanActionGroup"
ResourceGroupName="OrderDataBeanResourceGroup"
RelationName="creator">
```

ActionGroupName DisplayDataBeanActionGroup 指示此策略是用于数据 bean 的策略。此操作组包含一个 Display 操作。

其中:

Name: 该策略的名称。

UserGroup: 包含了策略所适用用户的访问组。在此例中，它包含所有用户。

ActionGroupName: DisplayDataBeanActionGroup 的值指示它是用于数据 bean 的资源级别的策略。

ResourceGroupName: 包含了要保护的数据 bean 的资源组的名称。

RelationName: 用户和资源之间必须满足的关系。在此例中，用户必须是商务 Order 资源的创建者。

OrderDataBeanResourceGroup 定义如下:

```
<ResourceGroup Name="OrderDataBeanResourceGroup" OwnerID="RootOrganization">
<ResourceGroupResource Name="com.ibm.commerce.order.beans.
OrderListDataBeanResourceCategory"/>
<ResourceGroupResource Name="com.ibm.commerce.order.beans
.OrderDataBeanResourceCategory"/>
</ResourceGroup>
```

OrderDataBeanResourceGroup 由两个资源构成。以下是用于数据 bean 的样本资源定义:

```
<ResourceCategory Name="com.ibm.commerce.order.beans.OrderDataBeanResourceCategory"
ResourceBeanClass="com.ibm.commerce.order.beans.OrderDataBean">
<ResourceAction Name="DisplayDataBean"/>
</ResourceCategory>
```

其中:

Name: 用于在 XML 文件中引用此资源的标记。

ResourceBeanClass: 受直接保护的数据 bean 的类名。此类必须实现 Protectable 接口。

ResourceAction: 在管理控制台中编辑策略所需的元素。在此例中，此元素指示 Display 是要对此资源执行的有效操作。

按属性将资源分组

资源组完全可通过使用 ACRESGRP 表的 CONDITIONS 列来定义。CONDITIONS 列存储了 XML 文档，该文档包含用于将资源分组的“约束 – 属性”值对。此类型的资源组称为隐式资源组，且通常用于资源类名不充分的场合。例如，如果访问控制策略适用于状态等于 P（未决）或 E（由客户服务代表编辑）的 Order 资源，则可定义此类型的资源组。

注：为了按类名之外的其它属性将资源分组，资源必须实现 Groupable 接口。关于 Groupable 接口的更多信息，请参阅《*IBM WebSphere Commerce 程序员指南*》。

以下是 Order 资源组的示例：

```
<ResourceGroup  Name="OrderResourceGroupwithPEStatus"
OwnerID="RootOrganization">
<ResourceCondition>
 <![CDATA[
  <profile>
   <andListCondition>
<orListCondition>
      <simpleCondition>
       <variable name="Status"/>
       <operator name="="/>
       <value data="P"/>
      </simpleCondition>
      <simpleCondition>
       <variable name="Status"/>
       <operator name="="/>
       <value data="E"/>
      </simpleCondition>
 </orListCondition>
      <simpleCondition>
       <variable name="classname"/>
       <operator name="="/>
       <value data="com.ibm.commerce.order.objects.Order"/>
      </simpleCondition>
    </andListCondition>
   </profile>
 ]]>
</ResourceCondition>
</ResourceGroup>
```

其中：

Name：存储在 ACRESGRP 表 GRPNAME 列的资源组的名称。

OwnerID：资源组的所有者。它必须是根组织。

<ResourceCondition>：指定将装入 ACRESGRP 表 CONDITIONS 列以定义资源组的数据。

<![CDATA[...]]>：指示恰按输入原样使用的字符数据部分。

<profile>：所有资源条件的必需参数。

资源组定义的一个必要组成部分是 name="classname" 的 <simpleCondition> 元素。此元素标识了该组所适用的资源的 Java 类。在以下示例中可见到 Java 类 com.ibm.commerce.order.objects.Order：

```
<simpleCondition>
   <variable name="classname"/>
   <operator name="="/>
   <value data="com.ibm.commerce.order.objects.Order"/>
   </simpleCondition>
```

以下示例指定 com.ibm.commerce.objects.order.objects.Order 资源上的条件，即状态应当等于 P。

```
<simpleCondition>
<variable name="Status"/>
       <operator name="="/>
       <value data="P"/>
   </simpleCondition>
```

在上面示例中，<variable name="*value*"/> 表示由 getGroupingAttributeValue (String attributeName, GroupContext context)() 方法对资源识别出的属性名称。此方法是 Groupable 接口的一部分。出于 WebSphere Commerce 管理控制台中隐式资源组管理的目的，还应当在 ACATTR 表中定义该属性，且将该属性与 ACRESATREL 表中的资源相关联。当到了查找给定资源及操作的适用策略的时候，将通过调用 getGroupingAttributeValue(..) 方法检查此条件，此例中该方法在 Status 中作为 attributeName 参数传递。

<orListCondition> 指定应当使用布尔值 OR 来应用此块中的条件。在此例中，状态是 P 或 E。<andListConditon> 指定应当使用布尔值 AND 来应用此块中的条件。在此例中，(Classname = com.ibm.commerce.order.objects.Order) AND (Status = P OR Status=E)。

以下显示了用于填充 ACATTR 表的样本属性定义:

```
<Attribute Name="Status" Type="String">
</Attribute>
```

Name 元素是用于标识属性的术语，Type 元素标识属性的数据类型。属性的可能值为:

- String
- Integer
- Double
- Currency
- Decimal
- URL
- Image
- Date

在资源定义中指定了属性与资源的关联。例如，以下示例中 Status 属性与 OrderResourceCategory 关联:

```
<ResourceCategory Name="com.ibm.commerce.order.objects.OrderResourceCategory"
ResourceBeanClass="com.ibm.commerce.order.objects.Order" >

<ResourceAttributes Name="Status"
AttributeTableName="ORDERS"
AttributeColumnName="STATUS"
ResourceKeyColumnName="ORDERS_ID"/>
</ResourceCategory>
```

其中:

<ResourceAttributes>: 将属性与资源关联的代码块。

AttributeTableName: 资源的数据库表名称。

AttributeColumnName: 存储该属性的资源表列名。

ResourceKeyColumnName: 存储主键的资源表列名。

定义关系

访问控制策略具有可选的关系元素。仅可通过装入 XML 策略文件创建此关系，该策略文件具有如下所示的关系定义:

```
<Relation Name="value">
 </Relation>
```

Name 条目是任意策略中所使用关系的名称，并将它添加到 ACRELATION 表。Name 对应于 protectable 资源上 fulfills() 方法的 relationship 参数。

以下示例显示名为 creator 的关系的定义。

```
<Relation Name="creator">
</Relation>
```

定义关系组

关系组包含开放条件，它们是隶属于关系组的条件。如果需要定义关系组，必须通过在 XML 文件中定义关系组信息来实现，或者通过修改 defaultAccessControlPolicies.xml 文件，如下所示:

```
<RelationGroup
Name="aValue"
OwnerID="aValue">
<RelationCondition><![CDATA[
<profile>
Relationship Chain Open Condition XML
</profile>
]]></RelationCondition>
</RelationGroup>
```

关系链

每个关系组都由一个或多个 RELATIONSHIP_CHAIN 开放条件组成，这些条件按 andListCondition 或 orListCondition 元素进行分组。关系链是一个或多个关系的序列。关系链的长度取决于其所包含关系的数目。这可以通过检查关系链的 XML 表示法中 <parmeter name= "X" value="Y"> 条目的数目而确定。以下是长度为 1 的关系链的示例。

```
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP"
value="aValue"/>
</openCondition>
```

其中:

<parameter name="Relationshiop" value="something">: 表示用户和资源之间关系的字符串。

name: protectable 资源上 fulfills() 方法的 relationship 参数。

当关系链的长度为 2 或更大值时，它是一个由两个关系组成的序列。第一个 <parmeter name= "X" value="Y"> 条目表示存在于用户和组织实体之间的关系。最后一个 <parmeter name= "X" value="Y"> 条目表示存在于组织实体和资源之间的关系。链中间部分的那些 <parmeter name= "X" value="Y"> 条目表示存在于组织之间的关系。以下是长度为 2 的关系链的示例。

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="aValue1" value="aValue2"/>
<parameter name="RELATIONSHIP" value="aValue3"/>
</openCondition>
```

其中:

aValue1: 可能的值包括 HIERARCHY 和 ROLE。HIERARCHY 指定在成员资格层次结构中，用户和组织实体之间存在层次结构关系。ROLE 指定用户在组织实体中担当角色。如果 aValue1 的值是 HIERARCHY，则可能的值将包括 child，该值返回在成员层次结构中用户系其直接子女的组织实体。如果 aValue1 的值是 ROLE，则可能的值将包含 ROLE 表的 NAME 列中的任何有效条目的值，该值返回当前用户对其担当此角色的所有组织实体。

aValue3: 是一个字符串，表示从第一个参数的评估中检索到的一个或多个组织实体和资源之间的关系。此值对应于 protectable 资源上的 fulfills() 方法的 relationship 参数。如果对参数 aValue1 进行评估时返回了多个组织实体，且当这些组织实体中的至少一个满足由参数 aValue2 所指定的关系时，则满足这一部分的 RELATIONSHIP_CHAIN。

注: 关于定义关系组的更多信息，请参阅第 80 页的『定义关系组』

定义单链关系组

如果作为访问控制策略的一部分，您需要强制用户必须属于某个组织实体（例如资源的 BuyingOrganizationalEntity），则必须创建由一个关系链构成的关系组，该关系链的长度为 2。如以下示例所示:

```
<RelationGroup Name="MemberOf->BuyerOrganizationEntity"
OwnerID="RootOrganization
<RelationCondition><![CDATA[
<profile>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="HIERARCHY" value="child"/>
<parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
</profile>
]]><RelationCondition>
<RelationGroup>
```

关系链的长度为 2，因为它由两个独立的关系构成。第一个关系是在用户和其父组织实体之间。在该关系中用户是 child。对于第二个关系，访问控制策略管理器检查父组织实体是否对资源满足 BuyingOrganizationalEntity 关系。换言之，在它是资源的买方组织实体的情况下返回 true。

注: 关于 openCondition 标记的信息，请参阅《*WebSphere 贸易加速器定制指南*》。

另一示例将是: 是否必须强制用户对组织实体（该组织实体是资源的买方组织实体）具有客户代表角色。这又使用了由长度为 2 的一个关系链组成的关系组。链的第一部分

查找用户对其具有客户代表角色的所有组织实体。然后对于组织实体的集合，访问控制策略管理器检查它们中是否至少有一个对资源满足 BuyingOrganizationalEntity 关系。如果是，则返回值 true。

以下示例显示了如何定义此类型的关系组:

```
<RelationGroup Name="AccountRep->BuyerOrganizationalEntity"
OwnerID="RootOrganization">
<RelationCondition><![CDATA[
<profile>
 <openCondition name="RELATIONSHIP_CHAIN">
 <parameter name="ROLE" value="Account Representative"/>
 <parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
 </profile>
]]><RelationCondition>
<RelationGroup>
```

定义多链关系组

如果需要编写的关系组包含多链关系，则必须指定用户是必须满足所有关系链（即 AND 方案），还是用户必须满足关系链中的至少一个（即 OR 方案）。

在以下示例中，用户必须是资源的创建者，且必须属于资源中所指定的 BuyingOrganizationalEntity。指定用户必须是资源的创建者的第一个链长度为 1。指定用户必须属于资源中指定的 BuyingOrganizationalEntity 的第二个链长度为 2。

```
<RelationshipGroup Name="Creator_And_MemberOf->BuyerOrganizationalEntity"
OwnerID="RootOrganization">
<RelationCondition><![CDATA[
<profile>
<andListCondition>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="RELATIONSHIP" value="creator" />
</openCondition>
<openCondition name="RELATIONSHIP_CHAIN">
<parameter name="HIERARCHY" value="child"/>
<parameter name="RELATIONSHIP" value="BuyingOrganizationalEntity"/>
</openCondition>
</andListCondition>
</profile>
]]></RelationCondition>
</RelationGroup>
```

注: 如果需要用户满足两个关系链中的任何一个，则应将 <andListConditon> 标记更改为 <orListConditon> 标记。

访问组

系 WebSphere Commerce 一部分的缺省访问组可在特定于语言的 XML 文件中找到，例如 *wc_install_directory*/xml/policies/xml/ACUserGroups_locale.xml。此文件遵循由 *wc_install_directory*/xml/policies/dtd/ACUserGroups_en_US.dtd 指定的 DTD。

以下是访问组元素的格式:

```
<UserGroup Name="value"
OwnerID="value"
Description="value"
<UserCondition>
<![CDATA[
<profile>
Condition XML
```

```
</profile>
]]>
</UserCondition>
</UserGroup>
```

其中:

Name: 存储在 MBRGRP 表 MBRGRPNAME 列中的访问组的名称。

OwnerID: 拥有该访问组的“成员标识”。Name 和 OwnerID 的组合必须是唯一的。可使用的特殊值包括: RootOrganization (-2001) 或 DefaultOrganization (-2000)。

Description（可选）: 用于描述访问组的可选属性。

UserCondition（可选）: 用于指定此访问组中成员资格隐式条件的可选元素。此条件存储在 MBRGRPCOND 表的 CONDITIONS 列中。

Condition XML: 使用条件框架, orListCondition、andListCondition、simpleCondition 和 trueConditionCondition 元素的任意有效组合。

对于 UserCondition 元素, 支持以下 SimpleCondition 名称:

表 5. 支持的简单条件名称

变量名	描述	支持的运算符	支持的值	限定符	限定符值
role	指定用户必须在 MBRROLE 表中具有此角色。	= !=	ROLE 表 NAME 列的任意值。	org（如果未指定, 则用户必须对 MBRROLE 表中的任意组织具有该角色。）	• OrgEntityID: 用户必须在此组织实体中具有该角色。 • ?: 它何时用于模板策略。
registration status	指定用户必须具有此注册状态。	= !=	USERS 表 REGISTER-TYPE 列的任意值, 例如 G 表示临时用户, R 表示注册用户。	无	n/a
status	指定用户必须具有此成员状态。这通常用于注册核准的状态。	= !=	MEMBER 表 STATE 列的任意值, 例如 0 表示正在审批的注册核准, 1 表示注册已核准, 2 表示注册已被拒绝。	无	n/a
org	指定用户必须注册到此父组织。它存储在 MBRREL 表中。	= !=	• ORGENTITY 表 ORGENTITY_ID 列的任意值。 • ? — 如果它是模板策略。	无	n/a

注: 当在运行时应用模板策略时，? 将动态更改为拥有资源的组织实体，并随后更改为其上级组织。仅以 ? 定义的访问组使用模板策略。

用于访问组的 simpleCondition 的示例

角色:

不带限定符的角色: 以下示例显示不带限定符的 role simpleCondition，最常用于基于角色的策略。在此示例中用户必须对任何组织实体具有卖方管理角色。

```
<UserConditon>
<![CDATA[
<profile>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller Administrator"/>
</simpleCondition>
</profile>
]]>
</UserCondition>
```

带限定符的角色: 以下示例显示带限定符的 role simpleCondition，最常用于组织级别的策略。在此示例中，用户必须对组织实体 100 具有卖方角色。

```
<UserCondition>
<!CDATA[
<profile>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller"/>
<qualifier name="org" data="100"/>
<simpleCondition>
</profile>
]]>
</UserCondition>
```

带限定符和参数的角色: 以下示例显示带限定符和参数的 role simpleCondition。它仅在模板策略中起作用。在此示例中，用户必须在拥有资源的组织实体中具有销售经理、财务经理或卖方角色，此资源是在模板策略中指定的。

```
<UserCondition><!CDATA[
<profile>
<orListCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Sales Manager"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Account Representative"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleCondition>
<variable name="role"/>
<operator name="="/>
<value data="Seller"/>
<qualifier name="org" data="?"/>
```

```
</simpleCondition>
</orListCondition>
</profile/>
]]></UserCondition>
```

registrationStatus: 以下示例显示 registrationStatus simpleCondition。在此示例中，用户必须已注册（USERS.REGISTERTYPE = R）。

```
<UserCondition><!CDATA[
<profile>
<simpleCondition>
<variable name="registrationStatus"/>
<operator name="="/>
<value data="R"/>
</simpleCondition>
</profile>
]]></UserCondition>
```

status: 以下示例显示 status simpleCondition。在此示例中，必须已核准了用户注册。（MEMBER.STATUS = 1）

```
<UserCondition><![CDATA[
<profile>
<simpleCondition>
<variable name="status"/>
<operator name="="/>
<value data="1"/>
</simpleCondition>
</profile>
]]></UserCondition>
```

org: 以下示例显示 org simpleCondition。在此示例中，用户必须已在组织实体 100 中注册。在 MBRREL 表中，用户必须具有以下值：ANCESTOR_ID = 100，且 SEQUENCE = 1。

```
<UserCondition><![CDATA[
<profile>
<simpleCondition>
<variable name="org"/>
<operator name="="/>
<value data="100"/>
</simpleCondition>
</profile>
]]>
</UserCondition>
```

策略

wc_install_directory/xml/policies/xml/defaultAccessControlPolicies.xml 文件定义直接提供的缺省访问控制策略。它遵循由 *wc_install_directory*/xml/policies/dtd/accesscontrolpolicies.dtd 指定的 DTD。

以下是策略元素的模板：

```
<Policy Name="value"
OwnerId="value"
UserGroup="value"
UserGroupOwner="value"
ActionGroupName="value"
ResourceGroupName="value"
PolicyType="value"
```

```
RelationName="value"
RelationGroupName="value"
RelationGroupOwner="value"
</Policy>
```

其中:

Name: 策略的名称。它装入到 ACPOLICY 表 POLICYNAME 列。Name 和 OwnerID 的组合必须是唯一的。

OwnerID: 拥有策略的组织实体的成员标识。它将装入到 ACPOLICY 表的 member_id 列。OwnerID 和 Name 的组合必须是唯一的。有两个由转换程序工具识别的特殊值，它们是 RootOrganization: -2001 和 DefaultOrganization: -2000

UserGroup: 在 MBRGRP 表 MBRGRPNAME 列中指定的访问组名称。它装入到 ACPOLICY 表的 mbrgrp_id 列。在 wc_install_directory/xml/policies/xml/ACUserGroups_language.xml 文件中定义了缺省访问组。

UserGroupOwner: 拥有访问组的成员的成员标识。当访问组由策略所有者之外的其它成员所拥有时，需要此信息。如果未指定，则假定访问组由 OwnerID 属性所指定的成员所拥有。

ActionGroupName: ACACTGRP 表 GROUPNAME 列中所指定的操作组的名称。它用于获取将存储在 ACPOLICY 表中的相应的操作组标识（ACACTGRP_ID）。用于控制器命令的基于角色的策略将 ActionGroupName 设置为 ExecuteCommandActionGroup。用于数据 bean 的策略将 ActionGroupName 设置为 DisplayDatabeanActionGroup。

ResourceGroupName: 在 ACRESGRP 表 GRPNAME 列中所指定的资源组名称。它用于获取存储在 ACPOLICY 表中的相应的资源组标识（ACRESGRP_ID）。用于视图的基于角色的策略将 ResoureGroupName 设置为 ViewCommandResourceGroup。

PolicyType: 策略类型。有效值为 template（在 ACPOLICY 表中 POLICYTYPE 将设置为 1）。如果未指定此属性，则策略类型值将保持不变。（缺省情况下此列的值为空。1 除外的任意值都暗指非模板的策略类型。）关于策略类型的更多信息，请参阅第 9 页的第 3 章，『访问控制概念』。

RelationName（可选）：在 ACRELATION 表 RELATIONNAME 列中所指定的关系名称。如果指定，则它用于获取存储在 ACPOLICY 表中的相应的关系标识（ACRELATION_ID）。

RelationGroupName（可选）：在 ACRELGRP 表 GRPNAME 列中所指定的关系组名称。如果指定了此属性，则不应指定 RelationName，因为关系组的优先级更高。

RelationGroupOwner: 拥有关系组的成员标识。仅当指定了 RelationGroupName 属性以及当 OwnerID 属性的值不是 RootOrganization 的情况下，此属性是必需的；在此例中，必须将 RelationGroupOwner 指定为 RootOrganization (-2001)。

策略示例

基于角色的策略:

对于控制器命令: 在此示例中，属于 AllUsers 访问组的用户可执行以下控制器命令，这些控制器命令是 AllUserCmdResourceGroup 资源组的一部分。

```
<Policy Name="AllUsersExceuteAllUserCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="AllUserCmdResourceGroup">
</Policy>
```

对于视图: 在此示例中，属于 MarketingManagers 访问组的用户可执行属于 MarketingManagersViews 操作组的视图。

```
<Policy Name="MarketingManagersExecuteMarketingManagersViews"
OwnerID="RootOrganization"
UserGroup="MarketingManagers"
ActionGroupName="MarketingManagersViews"
ResourceGroupName="ViewCommandResourceGroup">
</Policy>
```

资源级别的策略:

对于命令: 在此示例中，属于 RegisteredApprovedUsers 访问组的用户可对由 CouponWalletResourceGroup 指定的资源执行由 CouponRedemption 操作组指定的操作，只要用户对资源满足 creator 关系。

```
<Policy Name="RegisteredApprovedUsersExecuteCouponRedemptionCommandsOn
WalletResource"
OwnerID="RootOrganization"
UserGroup="RegisteredApprovedUsers"
ActionGroupName="CouponRedemption"
ResourceGroupName="CouponWalletResourceGroup"
RelationName="creator">
</Policy>
```

对于数据 bean: 在此示例中，属于 AllUsers 访问组的用户可显示由 UserDatabeanResourceGroup 资源组指定的数据 bean，只要用户对资源满足 owner 关系。

```
<Policy Name="AllUsersDisplayUserDatabeanResourceGroup"
OwnerID="RootOrganization"
UserGroup="AllUsers"
ActionGroupName="DisplayDatabeanActionGroup"
ResourceGroupName="UserDatabeanResourceGroup"
RelationName="owner">
</Policy>
```

模板策略: 在此示例中，属于 MembershipAdministratorsForOrg 访问组的用户可对由 OrganizationDataResourceGroup 指定的资源执行由 ApproveGroupUpdate 操作组指定的操作。

```
<Policy Name=MembershipAdministratorsForOrgExecuteApproveGroupUpdateCommands
OnOrganizationResource"
OwnerID="RootOrganization"
UserGroup="MembershipAdministratorsForOrg"
ActionGroupName="ApproveGroupUpdate"
ResourceGroupName="OrganizationDataResourceGroup"
PolicyType="template">
</Policy>
```

当应用此模板策略时，策略所有者将动态地从 RootOrganization 更改为拥有资源的组织实体，随后再更改为其上级组织实体，直至根组织且包含根组织。检查 MembershipAdministratorsForOrg 访问组的定义将揭示以下成员资格条件:

```
<UserCondition><![CDATA[
<profile>
<orListCondition>
<simple condition>
<variable name="role"/>
<operator name="="/>
<value data="Buyer Administrator"/>
<qualifier name="org" data="?"/>
</simpleCondition>
<simpleConditon>
<variable name="role"/>
<operator name="="/>
<value data="Seller Administrator"/>
<qualifier name="org" data="?"/>
</simpleConditon>
</orListCondtion>
</profile>
]]></UserCondition>
```

注: org = **?** 限定了 role 的 simpleCondition。如上所释，此 **?** 随着策略所有者的更改而被动态地替换。此动态行为仅可用于模板策略。因此在此示例中，对拥有资源的组织实体具有“买方管理员”或“卖方管理员”角色的用户，满足此访问组中的成员资格条件。

可翻译的策略数据

以下是可翻译的访问控制元素的模板，至少必须在 defaultAccessControlPolicies_*locale*.xml 文件中定义这些元素。

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!--The following TRANSLATABLE access control elements should
 be defined in this file:
<Attribute_nls>
<Action_nls>
<Relation_nls>
<ResourceCategory_nls>
<ActionGroup_nls>
<ResourceGroup_nls>
<Policy_nls>-->
<!DOCTYPE PoliciesNLS SYSTEM "../dtd/accesscontrolpoliciesnls.dtd">

<PoliciesNLS LanguageID="value">


 <!--Insert access control element definitions here -->
 </PoliciesNLS>
```

LanguageID 属性是一个字符串，它与特定于语言环境的数据的语言相对应。LanguageID 的有效值为:

- en_US
- fr_FR
- de_DE
- it_IT
- es_ES
- pt_BR
- zh_CN
- zh_TW

- ko_KR
- ja_JP

不可翻译的策略数据

以下是包含了不可翻译数据的定制策略文件的模板:

```
  <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>

<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<!--The following NON-TRANSLATABLE access control elements
 should be defined in this file:

<Attribute>
<Action>
<ResourceCategory>
<Relation>
<RelationGroup>
<ActionGroup>
<ResourceGroup>
<Policy-->
<Policies>

 <!--Insert access control element definitions here-->
 </Policies>
```

特定于语言环境的数据

可以装入以下可选的特定于语言环境的数据，以对在不可翻译的 XML 文件中已作定义的访问控制元素提供附加描述。缺省的特定于语言环境的数据可在以下地址找到:

wc_install_directory\xml\policies\xml\
defaultAccessControlPolicies_*locale*.xml

例如: defaultAccessControlPolicies_en_US.xml。

属性: 以下示例定义附加的属性元素信息:

```
<Atrribute_nls AttributeName="Status"
DisplayName_nls="Status attribute"
Description_nls="Resource status attribute"
/>
```

其中:

AttributeName: 属性名称。此值存储在 ACATTR 表 ATTRNAME 列中。

DisplayName_nls: 属性的显示名称。此值存储在 ACATTRDESC 表 DISPLAYNAME 列中。

Description_nls: 属性的可选描述。此值存储在 ACATTRDESC 表 DESCRIPTION 列中。

操作: 以下示例定义了附加的操作元素信息:

```
<Action_nls ActionName="OrderAdjustmentButton"
DisplayName_nls="Order Adjustment Button View"
Description_nls="The view for loading buttons in the order adjustment page
 when placing an order from Commerce Acclerator"
/>
```

其中:

ActionName: 操作名称。此值存储在 ACACTION 表 ACTION 列中。

DisplayName_nls: 操作的显示名称。此值存储在 ACACTDESC 表 DISPLAYNAME 列中。

Description_nls: 操作的可选描述。此值存储在 ACACTDESC 表 DESCRIPTION 列中。

关系: 以下示例定义附加的关系元素信息:

```
<Relation_nls RelationName="creator"
DisplayName_nls="creator"
Description_nls="creator"
/>
```

其中:

RelationName: 关系名称。此值存储在 ACRELATION 表 RELATIONNAME 列中。

DisplayName_nls: 关系的显示名称。此值存储在 ACRELDESC 表 DISPLAYNAME 列中。

Description_nls: 关系的可选描述。此值存储在 ACRELDESC 表 DESCRIPTION 列中。

资源类别: 以下示例定义了附加的资源类别信息:

```
<ResourceCategory_nls ResourceCategoryName="com.ibm.commerce.
catalog.objects."InterestItemList"
DisplayName_nls="Interest Item List"
Description_nls="Interest Item List command"
/>
```

其中:

ResourceCategoryName: 资源类别名称。此值存储在 ACRESCGRY 表 RESCLASSNAME 列中。

DisplayName_nls: 资源类别的显示名称。此值存储在 ACRSCGDES 表 DISPLAYNAME 列中。

Description_nls: 资源类别的可选描述。此值存储在 ACRSCGDES 表 DESCRIPTION 列中。

操作组: 以下示例定义了附加的操作组信息:

```
<ActionGroup_nls ActionGroupName="DoEverything"
DisplayName_nls="Do Everything"
Description_nls="Permits access to all Actions"
/>
```

其中:

ActionGroupName: 操作组名称。此值存储在 ACACTGRP 表 GROUPNAME 列中。

DisplayName_nls: 操作组的显示名称。此值存储在 ACACGPDESC 表 DISPLAYNAME 列中。

Description_nls: 操作组的可选描述。此值存储在 ACACGPDESC 表 DESCRIPTION 列中。

资源组: 以下示例定义了附加的资源组信息:

```
<ResourceGroup_nls ResourceGroupName="AllResourceGroup"
DisplayName_nls="All Resources Group"
Description_nls="All Resources"
/>
```

其中:

ResourceGroupName: 资源组名称。此值存储在 ACRESGRP 表 GRPNAME 列中。

DisplayName_nls: 资源组的显示名称。此值存储在 ACRESGPDES 表 DISPLAYNAME 列中。

Description_nls: 资源组的可选描述。此值存储在 ACRESGPDES 表 DESCRIPTION 列中。

策略: 以下示例定义了附加的策略信息:

```
<Policy_nls PolicyName="SiteAdministratorsCanDoEverything"
OnwerID="RootOrganization"
DisplayName_nls="Site Administrators Can Do Everything"
Description_nls="Policy that allows Site Administrators to do everything"
/>
```

其中:

PolicyName: 访问控制策略的名称。此值存储在 ACPOLICY 表 POLICYNAME 列中。

OwnerID: 拥有此策略的组织实体的成员标识。

DisplayName_nls: 策略的显示名称。此值存储在 ACPOLDESC 表 DISPLAYNAME 列中。

Description_nls: 策略的可选描述。此值存储在 ACPOLDESC 表 DESCRIPTION 列中。

更改 XML 文件之后

测试更改

关于测试更改的信息，请参阅第 38 页的『更改策略之后』。

将更改装入数据库

如果通过直接处理 XML 文件进行策略更改，则必须将已更改的 XML 文件装回数据库中。维持 XML 文件和数据库中的访问控制信息之间的一致性是很重要的，原因有以下几个:

- 创建 WebSphere Commerce 实例时，策略和访问组定义是从 XML 文件装入的。
- 如果希望在 WebSphere Commerce 的另一实例中实现相同的访问控制策略，则可通过在创建另一实例之前将 XML 文件复制到适当的目录来实现该操作。

- XML 文件提供了直接查看和编辑策略及其组成部分的便捷方式，因此将这些文件保持为最新是至关重要的。

将 XML 更改装入数据库

装入过程读取包含访问控制策略信息和访问组定义的 XML 文件，并将它们装入适当的数据库。包含在 XML 文件中的策略和访问组信息是在安装时装入的，但是，如果对它们作了更改，则必须重新装入这些 XML 文件。

注: 如果创建已定制的 XML 文件，则需要将它们复制到 *<wc_install_directory>*/xml/policies/xml 目录中，以将它们装入数据库。

对于 400：如果创建已定制的 XML 文件，则必须在文件中使用 DTD 的完整路径。访问控制策略 DTD 位于 /QIBM/ProdData/WebCommerce/xml/policies/dtd 中。

要装入访问组和访问控制策略，请运行以下命令。

对于 NT 2000

1. 从目录 *<wc_install_directory>*\bin，按需要以此处列出的顺序运行以下命令文件:
   - 要装入用户（访问）组定义，请运行 **acugload** 命令文件。**语法**: acugload.cmd *<database name> <database user> <database user password> <UserGroups xml file>* **例如**: acugload mall dbuser dbusrpwd ACUserGroups_zh_CN.xml
   - 要装入主访问控制策略文件，请运行 **acpload** 命令文件。 **语法**: acpload.cmd *<database name> <database user> <database user password> <Policies xml file>* **例如**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml
   - 要装入显示名称和描述文件，请运行 **acpnlsload** 命令文件。 **语法**: acpnlsload.cmd *<database name> <database user> <database user password> <NLS Policies xml file>* **例如**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_zh_CN.xml
2. 检查 *<wc_install_directory>*\logs 中的日志文件 **acugload.log**、**acpload.log** 和 **acpnlsload.log** 是否存在任何错误。

对于 AIX Solaris Linux

数据库用户标识必须对目录 *<wc_install_directory>*/xml/policies、*<wc_install_directory>*/bin 和 *<wc_install_directory>*/properties/utilities 及其子目录和文件具有读 / 写 / 执行权限。

1. 使用该数据库用户标识登录。
2. 从目录 *<wc_install_directory>*/bin，按需要以此处列出的顺序运行以下外壳程序脚本:

1. 要装入用户（访问）组定义，请运行 **acugload** 外壳程序脚本。**语法**: acugload.sh *<database name> <database user> <database* user *password> <UserGroups xml filename>* **例如**: acugload mall dbuser dbusrpwd ACUserGroups_zh_CN.xml
2. 要装入主访问控制策略文件，请运行 **acpload** 外壳程序脚本。 **语法**: acpload.sh *<database name> <database user> <database user password> <Policies xml filename>* **例如**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml

3. 要装入显示名称和描述文件，请运行 acpnlsload 外壳程序脚本。**语法**: acpnlsload.sh <*database name*> <*database user*> <*database user password*> <*NLS Policies xml filename*> **例如**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_zh_CN.xml

检查 <*wc_install_directory*>/logs 中的日志文件 acugload.log、acpload.log 和 acpnlsload.log 是否存在任何错误。

注: 执行这些脚本之后，必须检查日志文件，因为当运行这些脚本时可能发生的任何错误将不会出现在命令行中。

对于 400

从命令行，按需要以指定的顺序运行以下命令:

- 要装入用户（访问）组定义，请运行 LODWCSUG 命令。 **语法**: LODWCSUG DATABASE(<*database name*>) SCHEMA(<*schema_name*>) PASSWD(<*instance_password*>) INSTROOT(<*instance_root*>) INFILE(<*full path for XML file*>)
- 要装入主访问控制策略文件，请运行 LODWCSAC 命令。 **语法**: LODWCSAC DATABASE (<database name>) SCHEMA (<schema_name>) PASSWD (<instance_password>) INSTROOT (<instance_root>) INFILE (<*full path for XML file*>)
- 要装入显示名称和描述文件，请运行 LODWCSACD 命令。 **语法**: LODWCSACD DATABASE(<*database name*>) SCHEMA(<*schema_name*>) PASSWD (<*instance_password*>) INSTROOT(<*instance_root*>) INFILE(<*full path to XML file*>)

将数据库中的策略和访问组定义抽取到 XML 文件中

抽取过程读取访问控制数据库中的策略和访问组信息，并生成捕获 XML 格式信息的文件。

对于 NT 2000

1. 从 <*wc_install_directory*>\bin 目录中，运行以下 acpextract 命令:

   ```
   acpextract.cmd <database name> <database user> <database user password>
   ACPoliciesfilter.xml
   ```

   例如:

   ```
   acpextract.cmd mall dbuser dbusrpwd ACPoliciesfilter.xml
   ```

   创建以下文件:

   - ExtractedACPolicies.xml: 此文件包含由 Extract 命令根据给定的过滤条件所抽取的数据。
   - ExtractedACPolicies.dtd: 用于 ExtractedACPolicies.xml 文件的 DTD。
   - AccessControlUserGroups.xml: 包含访问组定义的文件。
   - AccessControlPolicies.xml: 包含独立于语言的访问控制策略信息的文件。
   - AccessControlPolicies_LOCALE.xml: 依赖于语言的访问控制策略文件，该文件包含显示名称和描述。
2. 请检查日志文件 <*wc_install_directory*>\logs\acpextract.log 是否存在任何可能已发生的处理错误。

对于 AIX Solaris Linux

1. 使用该数据库用户标识登录。
2. 从 *<wc_install_directory>*\bin 目录，运行以下 acpextract 外壳程序脚本:

   ```
   acpextract.sh <database name> <database user>
   <database user password> ACPoliciesfilter.xml
   ```

   例如:

   ```
   acpextract.sh mall dbuser dbusrpwd ACPoliciesfilter.xml
   ```

   创建以下文件:

   - ExtractedACPolicies.xml: 此文件包含由 Extract 命令根据给定的过滤条件所抽取的数据。
   - ExtractedACPolicies.dtd: 用于 ExtractedACPolicies.xml 文件的 DTD。
   - AccessControlUserGroups.xml: 包含访问组定义的文件。
   - AccessControlPolicies.xml: 包含独立于语言的访问控制策略信息的文件。
   - AccessControlPolicies_LOCALE.xml: 依赖于语言的访问控制策略文件，该文件包含显示名称和描述。
3. 请检查日志文件 *<wc_install_directory>*\logs\acpextract.log 是否存在任何可能已发生的处理错误。

对于 400

1. 从命令行，运行以下 EXTWCSAC 命令:

   ```
   EXTWCSAC DATABASE (<database name>)
    SCHEMA (<schema_name>) PASSWD (<database user>)
   INSTROOT (<instance_root>) FILTER (<input filter XML file>) OUTDIR
    (<output directory
    for new files>)
   ```

   在使用 OUTDIR 参数指定的目录中创建以下文件:

   - ExtractedACPolicies.xml: 此文件包含由 Extract 命令根据给定的过滤条件所抽取的数据。
   - ExtractedACPolicies.dtd: 用于 ExtractedACPolicies.xml 文件的 DTD。
   - AccessControlUserGroups.xml: 包含访问组定义的文件。
   - AccessControlPolicies.xml: 包含独立于语言的访问控制策略信息的文件。
   - AccessControlPolicies_LOCALE.xml: 依赖于语言的访问控制策略文件，该文件包含显示名称和描述。

附录. 缺省访问控制策略

附录列出了随 WebSphere Commerce 提供的缺省策略。它们分组为以下类别:

- **基于角色的策略**: 对每个缺省角色的基于角色的策略。这些策略也称为命令级别的策略，因为它们定义了谁可执行每个命令。
- **资源级别的策略**: 不同业务区域的资源级别的策略。这些策略定义了一组用户可对特定资源执行的操作。在每个业务区域下，策略是按其所控制的资源的类型来组织的:
  - **数据资源** — 可操纵的商业对象，例如订单或投标。
  - **数据 bean 资源** — 包含关于商业对象的信息。数据 bean 用于在 Web 页面上显示对象信息。

表 6.

策略	起始页
基于角色的策略	第 96 页的『基于角色的策略』
不同业务区域的资源级别的策略:	第 97 页的『不同业务区域的资源级别的策略』
订单	第 97 页的『订单』
贸易（合同）	第 98 页的『贸易（合同）』
核准	第 98 页的『核准』
拍卖	第 99 页的『拍卖』
商务智能	第 99 页的『商务智能』
成员资格	第 99 页的『成员资格』
买方管理控制台	第 100 页的『买方管理控制台』
竞销	第 100 页的『竞销』
产品目录	第 101 页的『产品目录』
连接性和通知	第 101 页的『连接性和通知』
采购	第 102 页的『采购』
赠券	第 102 页的『赠券』
顾客简要表	第 102 页的『顾客简要表』
折扣	第 102 页的『折扣』
库存	第 103 页的『库存管理』
已调度库存	第 103 页的『已调度库存』
库存管理	第 103 页的『库存管理』
订单管理	第 104 页的『订单管理』
支付	第 104 页的『支付』
用于编辑策略、访问组、资源组和操作组的管理控制台页面	第 105 页的『用于编辑策略、访问组、资源组和操作组的管理控制台页面』
产品顾问	第 105 页的『产品顾问』
RFQ	第 105 页的『RFQ』
规则	第 106 页的『规则』

表 6. (续)

调度程序	第 106 页的『调度程序』

基于角色的策略

表 7.

AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
AccountRepresentativesExecuteAccountRepresentativesViews
AllUsersExecuteAllUserCmdResourceGroup
AllUsersExecuteAllUsersViews
BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
BuyerAdministratorsExecuteBuyerAdminstratorsViews
BuyerAdministratorsExecuteBuyerAdminstratorsCommands
BuyerApproversExecuteBuyerApproversCmdResourceGroup
BuyerApproversExecuteBuyerApproversViews
Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
Buyers(buy-side)ExecuteBuyers(buy-side)Views
Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
Buyers(sell-side)ExecuteBuyers(sell-side)Views
CategoryManagersExecuteCategoryManagersCmdResourceGroup
CategoryManagersExecuteCategoryManagersView
CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeView
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
CustomersExecuteCustomersViews
GuestsExecuteGuestUsersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
LogisticsManagersExecuteLogisticsManagersViews
MarketingManagersExecuteMarketingManagerCmdResourceGroup
MarketingManagersExecuteMarketingManagersViews
OperationsManagersExecuteOperationsManagersCmdResourceGroup
OperationsManagersExecuteOperationsManagersView
PickPackersExecutePickPackersCmdResourceGroup
PickPackersExecutePickPackersViews
ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup
ProductManagersExecuteProductManagersCmdResourceGroup
ProductManagersExecuteProductManagersViews
ReceiversExecuteReceiversCmdResourceGroup
ReceiversExecuteReceiversViews
ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup

表 7. (续)

ReturnsAdministratorsExecuteReturnsAdministratorsViews
SalesManagersExecuteSalesManagersCmdResourceGroup
SalesManagersExecuteSalesManagersViews
SellerAdministratorsExecuteSellerAdministratorsCommands
SellerAdministratorsExecuteSellerAdministratorsViews
SellersExecuteSellersCmdResourceGroup
SellersExecuteSellersView
SiteAdministratorsCanDoEverything
StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup
StoreAdministratorsExecuteStoreAdministratorViews

不同业务区域的资源级别的策略

订单

表 8.

数据资源	
订单	AllUsersExecuteOrderCreateCommandsOnStoreResource
	AllUsersExecuteOrderPrepareCommandsOnOrderResource
	AllUsersExecuteOrderProcessOnOrderResource
	AllUsersExecuteOrderReadCommandsOnOrderResource
	AllUsersExecuteOrderWriteCommandsOnOrderResource
	AllUsersExecuteReturnAgainstOrderOnOrderResource
	AllUsersExecuteScheduledOrderCancelOnOrderResource
	OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
需求列表	AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
	AllUsersExecuteRequisitionListExclusiveProcessCommands OnPrivateRequisitionListResource
	AllUsersExecuteRequisitionListExclusiveReadCommandsOn PrivateRequisitionListResource
	AllUsersExecuteRequisitionListSharedProcessCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListSharedReadCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListWriteCommandsOn RequisitionListResource
兴趣商品	AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
	AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource
RMA（退货商品授权）	AllUsersExecuteRMACreateCommandsOnStoreResource
	AllUsersExecuteRMAProcessCommandsOnRMAResource

表 8. (续)

	AllUsersExecuteRMAReadCommandsOnRMAResource
	AllUsersExecuteRMAWriteCommandsOnRMAResource
	RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
	RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
	RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
	RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
	StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource
数据 bean	
订单	AllUsersDisplayApprovalsOrderDataBeansResourceGroup
	AllUsersDisplayOrderDatabeanResourceGroup
需求列表	AllUsersDisplaySharedRequisitionListDataBeansIfSame OrganizationalEntityAsCreator
兴趣商品	AllUsersDisplayInterestItemDatabeanResourceGroup
RMA	AllUsersDisplayRMADatabeanResourceGroup

贸易（合同）

表 9.

数据资源	
合同	ContractAdministratorsForOrgExecuteContractCreateCommandsOn MemberResource
	ContractAdministratorsForOrgExecuteContractManageCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractDeployCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractSubmitCommandsOn ContractResource
	ContractViewersExecuteContractDisplayCommandsOnContractResource
业务策略	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy CreateCommandsOnStoreResoure
	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy ManageCommandsOnBusinessPolicyResourcee
数据 bean	AccountHandlersDisplayTradingDatabeanResourceGroup

核准

表 10.

数据资源	
	AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
	AllUsersExecuteApproveCommandsOnApprovalResource
	AllUsersExecuteCancelApproveCommandsOnApprovalResource

拍卖

表 11.

数据资源	
拍卖	AuctionAdministratorsForOrgExecuteAdminRetractBidCommands OnAuctionResource
	AuctionAdministratorsForOrgExecuteAuctionCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionManageCommands OnAuctionResource
拍卖样式	AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionStyleManageCommands OnAuctionStyleResource
投标控制规则	AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteBidControlRuleManageCommands OnBidControlRuleResource
投标	RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
	RegisteredApprovedUsersExecuteBidManageCommands OnBidResourcesTheyOwn
自动投标代理	RegisteredApprovedUsersExecuteAutoBidCreateCommands OnAuctionResource
	RegisteredApprovedUsersExecuteAutoBidManageCommands OnAutoBidResourcesTheyOwn
数据 bean	AuctionDatabeanOwnersDisplayAuctionDatabeans

商务智能

表 12.

数据资源	
	BusinessAnalystsForOrgExecuteViewContext ListCommandsOnStoreEntityResource
	IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport CommandsOnStoreEntityResource

成员资格

表 13.

数据资源	
用户	GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteUserAdminRegistration CommandsOnOrganizationResource
	MembershipAdministratorsForOrg ExecuteUserAdminUpdateCommandsOnUserResource

表 13. (续)

	NonRejectedUsersExecuteUserSelfRegistration ContinuationCommandsOnUserResource
组织	MembershipAdministratorsForOrgExecute OrgEntityRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteOrg EntityUpdateCommandsOnOrganizationResource
地址	MembershipAdministratorsForOrg ExecuteAddressManageCommandsOnMemberResource
	NonRejectedUsersExecuteAddressManageCommandsOn UserResource
角色	MembershipAdministratorsForOrgExecute RoleManageCommandsOnUserResource
	OrganizationRoleAdministratorsExecute RoleManageCommandsOnOrganizationResource
成员组	MemberGroupAdministratorsForOrgExecute MemberGroupCreateCommandsOnMemberResource
	MemberGroupManagersForOrgExecute MemberGroupManageCommandsOnMemberGroupResource
数据 bean	MembershipAdministratorsForOrgDisplay OrganizationDatabeanResourceGroup
	MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup

买方管理控制台

表 14.

数据资源	
核准组	MembershipAdministratorsForOrgExecute ApproveGroupUpdateCommandsOnOrganizationResource
成员组	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnMemberGroupResource
	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnUserResource

竞销

表 15.

数据资源	
	CampaignManagersForOrgExecute CampaignRelatedCreateCommandsOnStoreEntityResource
	CampaignManagersForOrgExecute CampaignUpdateCommandsOnCampaignResource
	CampaignManagersForOrgExecute CollateralUpdateCommandsOnCollateralResource

表 15. (续)

	CampaignManagersForOrgExecute EMarketingSpotUpdateCommandsOnEMarketingSpotResource
	CampaignManagersForOrgExecute InitiativeUpdateCommandsOnInitiativeResource
数据 bean	CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

产品目录

表 16.

数据资源	
	CatalogEntryManagersForOrgExecute CatalogEntryManageCommandsOnCatalogEntryResource
	CatalogEntryManagersForOrgExecute CatalogEntryRelationManageCommandsOnCatalogResource
	CatalogEntryManagersForOrgExecute StoreCatalogEntryManageCommandsOnStoreEntityResource
	CatalogGroupManagersForOrgExecute CatalogGroupManageCommandsOnCatalogGroupResource
	CatalogGroupManagersForOrgExecute ProductSetAddCommandsOnCatalogResource
	CatalogGroupManagersForOrgExecute ProductSetManageCommandsOnProductSetResource
	CatalogManagersForOrgExecute CatalogManageCommandsOnCatalogResource
	CatalogManagersForOrgExecute StoreCategoryManageCommandsOnCatalogResource
数据 bean	CatalogGroupManagersForOrgDisplay CatalogGroupDataBeansResourceGroup
	ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup

连接性和通知

表 17.

数据资源	
	BackendOrderAdministratorsForOrgExecute BackendOrderStatusCreateCommandsOnOrderDataResource
	BackendPickPackersForOrgExecute BackendPickPackListCommandsOnFulfillmentCenterDataResource
	StoreAdministratorsForOrgExecute MessagingAdminCommandsOnStoreEntityResource
数据 bean	StoreAdministratorsForOrgDisplayMessagingDataBeans

采购

表 18.

数据资源	
	ProcurementAdministratorsForOrgExecute ProcurementAuthenticationAndRegistrationOnOrderDataResource
	ProcurementShoppingCartManagersExecute ProcurementShoppingCartManageOnOrderResource

赠券

表 19.

数据资源	
	CouponAdministratorsForOrgExecute CouponPromotionCreateCommandsOnStoreEntityResource
	CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommands OnCouponPromotionResource
	RegisteredApprovedUsersExecute CouponDeleteCommandsOnCouponWalletResource
	RegisteredApprovedUsersExecute CouponRedemptionCommandsOnCouponWalletResource
	StoreAdministratorsForOrgExecute ScheduledCouponCmdsOnStoreResource
数据 bean	CouponAdministratorsForOrgDisplayECouponPromotionListBeans

顾客简要表

表 20.

数据资源	
	CustomerProfileEditorsForOrgExecute SegmentManageCommandsOnStoreEntityResource
数据 bean	CustomerProfileEditorsForOrgDisplay SegmentationDatabeansResourceGroup

折扣

表 21.

数据资源	
	DiscountAdministratorsForOrgExecute DiscountAssociateCommandsOnCalculationCodeResource
	DiscountAdministratorsForOrgExecute DiscountCreateCommandsOnStoreEntityResource
	DiscountAdministratorsForOrgExecute DiscountDeployCommandsOnCalculationCodeResource
数据 bean	DiscountViewersForOrgDisplayDiscountDatabeans

库存管理

表 22.

数据资源	
	ExpectedInventoryManagersForOrgExecute InventoryManageCommandsOnStoreEntityResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterCreateCommandsOnOrganizationResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterManageCommandsOnFulfillmentResource
	InventoryAdjustersForOrgExecute InventoryAdjustCommandsOnStoreEntityResource
	PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommands OnFulfillmentCenterResource
	PickPackGeneratorsForOrgExecute PickPackGenerateCommandsOnFulfillmentCenterResource
	ReturnReasonsManagersForOrgExecute ReturnReasonsCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorCreateCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorManageCommandsOnVendorResource
数据 bean	StoreAdministratorsForOrgDisplay OrderFulfillmentStatusDataBeansResourceGroup

已调度库存

表 23.

数据资源	
	StoreAdministratorsForOrgExecute InventoryScheduledCommandsOnStoreEntityResource

库存管理

表 24.

数据 bean	
	ExpectedInventoryManagersForOrgDisplay ExpectedInventoryDataBeansResourceGroup
	FulfillmentCenterManagersForOrgDisplay FulfillmentCenterDataBeansResourceGroup
	PickBatchInventoryManagersForOrgDisplay PickBatchInventoryDataBeansResourceGroup
	ProductFindInventoryManagersForOrgDisplay ProductFindInventoryDataBeansResourceGroup

表 24. (续)

	ReceiverOrderManagersForOrgDisplay ReceiverOrderManagementDataBeansResourceGroup
	ReturnReasonsManagersForOrgDisplay ReturnReasonsOrderManagementDataBeansResourceGroup
	ReturnsAdminOrderManagersForOrgDisplay ReturnsAdminOrderManagementDataBeansResource
	SuperUserOrderManagersForOrgDisplay SuperUserOrderManagementDataBeansResourceGroup
	VendorInventoryManagersForOrgDisplay VendorInventoryDataBeansResourceGroup

订单管理

表 25.

数据资源	
	CustomerOrderManagersExecute CustomerServiceCustomerWriteCommandsOnUserResource
	CustomerOrderManagersForDefaultOrgExecute CustomerServiceCustomerWriteCommandsOnUse
	CustomerOrderManagersForOrgExecute CustomerServiceOrderCreateCommandsOnStoreEntityResource
	CustomerOrderManagersForOrgExecute CustomerServiceOrderWriteCommandsOnOrderResource
	CustomerOrderManagersForOrgExecute CustomerServiceReturnCreateCommandsOnStoreEntity
	CustomerOrderManagersForOrgExecute CustomerServiceReturnWriteCommandsOnRMAResource
数据 bean	CustomerOrderManagersDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForDefaultOrgDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForOrgDisplay CustomerOrderManagementDatabeans
	LogisticsManagersForOrgDisplay OrdersAndReturnsListsDatabeans
	ReturnsManagersForOrgDisplayReturnsListsDatabean
	UserOrderManagersDisplayUserDatabeans
	UserOrderManagersForDefaultOrgDisplayUserDatabeans

支付

表 26.

数据资源	

表 26. (续)

	AccountAdministratorsForOrgExecute AccountManageCommandsOnAccountResource
	AccountManagersForOrgExecute AccountCreateCommandsOnOrganizationResource
	AccountViewersForOrgExecute PaymentSummaryGenerateCommandsOnAccountResource
	AccountViewersForOrgExecute StorePaymentAdminCommandsOnStoreEntityResource
	AllUsersExecutePaymentOrderWrite CommandsOnOrderResource

用于编辑策略、访问组、资源组和操作组的管理控制台页面

表 27.

数据资源	
	DescendantStoreAdministratorsExecute ACViewPoliciesForOrgActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyCreateCommandsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyEditCommandsOnACPolicyResource
	StoreAdministratorsForOrgExecute ACViewApplicablePoliciesActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACViewPoliciesForUpdateActionsOnOrganizationResource
数据 bean	StoreAdministratorsForOrgExecute UserGroupSearchViews

产品顾问

表 28.

数据 bean	
	ProductAdvisorStatisticiansForOrgDisplay ProductAdvisorStatisticsDatabeans
	SalesAssistantStatisticiansForOrgDisplay SalesAssistantStatisticsDatabeans

RFQ

表 29.

数据资源	
	RFQAdministratorsAdministerRFQs
	RFQAdministratorsManageRFQResponses

表 29. (续)

	RFQBuyersEvaluateRFQResponsesForRFQsTheyOwn
	RFQBuyersForOrgExecuteRFQCreate CommandsOnStoreEntityDataResourceGroup
	RFQBuyersManageRFQResourcesTheyOwn
	RFQBuyersManageRFQResponsesForRFQsTheyOwn
	RFQSalesManagersExecuteRFQResponse ManageCommandsOnRFQResponseResource
	RFQSalesManagersForOrgCreateRFQResponse
数据 bean	RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
	RFQBuyersDisplayRFQResponseDataBeans ViewabletoRFQOwnerResourceGroup
	RFQSalesViewersDisplayRFQDataBeanResourceGroup
	RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup

规则

表 30.

数据资源	
	StoreAdministratorsForOrgExecutePersonalization RuleServiceAdministrationCommandsOnStoreEntityResource
数据 bean	StoreAdministratorsForOrgDisplay PersonalizationRuleServiceAdministrationDataBeanResource

调度程序

表 31.

数据资源	
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnStoreEntityResource
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnUserResource
数据 bean	StoreAdministratorsForOrgDisplay SchedulerDataBeansResourceGroup

声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其它国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代理咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可证。您可以用书面方式将许可证查询寄往:

IBM Director of Licensing IBM Corporation North Castle Drive Armonk, NY 10504-1785 U.S.A.

有关双字节（DBCS）信息的许可证查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

有关双字节（DBCS）信息的许可证查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

本条款不适用联合王国或任何这样的条款与当地法律不一致的国家或地区:

国际商业机器公司以“按现状”的基础提供本出版物，不附有任何形式的（无论是明示的，还是默示的）保证，包括（但不限于）对非侵权性、适销性和适用于某特定用途的默示保证。某些国家或地区在某些交易中不允许免除明示或默示的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本出版物中描述的产品和／或程序进行改进和／或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。该 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: （i）允许在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及（ii）允许对已经交换的信息进行相互使用，请与下列地址联系:

Manager, e-Commerce Product Development IBM 17 Skyline Drive Hawthorne, NY 10532 U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可证协议或任何同等协议中的条款提供。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其它可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其它关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

本信息包含日常商业运作中所使用的数据和报告示例。为了尽可能完整地说明它们，这些示例包含了个人、公司、品牌和产品的名称。所有这些名称都是虚构的，如与实际公司企业中使用的名称和地址雷同，纯属巧合。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

版权许可证

本信息包含源语言格式的样本应用程序，它说明了各种操作平台上的编程技术。如果您的目的是开发、使用、销售或分发应用程序，而这些应用程序符合操作平台（样本程序就是为该操作平台而写）的应用程序编程接口，则您可以使用任何形式复制、修改和分发这些样本程序，而无需向 IBM 付费。这些示例并未在所有情况下进行完整测试。因此 IBM 无法保证或默示这些程序的可靠性、可服务性或功能。如果您的目的是开发、使用、销售或分发应用程序，而这些应用程序符合 IBM 的应用程序编程接口，则您可以使用任何形式复制、修改和分发这些样本程序，而无需向 IBM 付费。

商标

以下术语是国际商业机器公司在美国和／或其它国家或地区的商标:

DB2 DB2 Universal Database

IBM WebSphere

Lotus®、Domino™ 和 Go Webserver 是 Lotus Development Corporation 在美国和／或其它国家或地区的商标。

Microsoft™®、Windows™ 和 Windows NT™ 是 Microsoft Corporation 在美国和／或其它国家或地区的注册商标。

Pentium™® 是 Intel Corporation 在美国和／或其它国家或地区的商标。

Solaris Operating Environment、JDBC、Java™ 和所有基于 Java 的标记是 Sun Microsystems, Inc. 在美国和其它国家或地区的商标或注册商标。

Blaze Advisor、Blaze Expert、Blaze Presenter、Blaze Accessor、Blaze Enterprise、OOScript 和 Smartlets 是 Blaze Software, Inc. 在美国和／或其它国家或地区的商标。

其它公司、产品和服务名称可能是其它公司的商标或服务标记。

本产品中提供的信用卡图像、商标和贸易名称应当仅由已经过信用卡标记的所有者授权可通过该信用卡接受支付的商家使用。

中国印刷