IBM WebSphere Commerce

安全性指南

版本 5.5

IBM WebSphere Commerce

安全性指南

版本 5.5

注意:

在使用本资料及其支持的产品之前，请务必阅读第 201 页的『声明』中的信息。

第一版（2003 年 6 月）

本版本适用于 IBM WebSphere Commerce V5.5（产品号 5724-A18）以及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。

IBM 欢迎您提出宝贵意见。您可以通过使用在线的 IBM WebSphere Commerce 文档反馈表发送您的意见，该表可在以下 URL 得到:

http://www.ibm.com/software/commerce/rcf.html

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。

目录

关于本书

本文档描述了 WebSphere Commerce 的安全性功能以及如何配置这些功能。

它详细描述了 WebSphere Commerce 的安全性问题和功能，例如认证、授权和访问控制策略。本文档的目的是为负责站点安全性的人员（可能包括系统管理员或 WebSphere Commerce 站点管理员）提供全面的文档以使他们能够可靠地保护 WebSphere Commerce 生产站点。

本文档面向的读者为 WebSphere Commerce 站点的首席安全性官员或安全性管理员。

重要信息

本文档仅涉及与部署电子交易站点相关的 WebSphere Commerce 安全性问题。未涉及与操作系统的薄弱环节相关的问题。应当咨询操作系统供应商来确定为保护操作系统应采取的适当措施。

更改摘要

本安全性指南以及本安全性指南的任何更新版本将在 WebSphere® Commerce 技术库 Web 页面中提供（http://www.ibm.com/software/commerce/library/）。关于您的 WebSphere Commerce 版本的附加信息，请参阅概述页面:

- Business Edition（`http://www.ibm.com/software/webservers/commerce/wc_be/`）
- Professional Edition（`http://www.ibm.com/software/commerce/wscom/support/wc_pe/`）

关于附加支持信息，请参阅 WebSphere Commerce 支持页面（`http://www.ibm.com/software/commerce/support/`）。

要了解对产品的最后更改，请参阅更新的产品自述文件，该文件也可从上面的 Web 站点得到。

本部分将总结对本书的所有更新。

浏览本书

本文档分为以下部分:

- 第 1 页的第 1 部分，『WebSphere Commerce 安全性概念』讨论了 WebSphere Commerce 安全性模型并提供了对 WebSphere Commerce 安全性的概念性概述。任何想要了解对 WebSphere Commerce 安全性的总体概述的人员或规划 WebSphere Commerce 站点安全性的人员将对该部分内容感兴趣。
- 第 41 页的第 2 部分，『管理安全性认证』讨论了关于站点安全性的 WebSphere Commerce 管理任务。任何执行关于站点安全性的管理任务的人员将对该部分内容感兴趣。

- 第 75 页的第 3 部分，『管理安全性授权』讨论了关于访问控制的 WebSphere Commerce 授权任务。任何执行关于 WebSphere Commerce 上的访问控制的系统授权任务的人员将对该部分内容感兴趣。
- 第 153 页的第 4 部分，『支付安全性』讨论了关于 WebSphere Commerce 支付安全性的 WebSphere Commerce 管理任务。任何管理 WebSphere Commerce 支付的人员将对该部分内容感兴趣。
- 第 159 页的第 5 部分，『各种安全性主题』讨论了诸如增强 WebSphere Application Server 安全性的各种 WebSphere Commerce 系统管理任务。负责安全性的系统管理员将对该部分内容感兴趣。

本书中使用的约定

本书使用以下突出显示的约定:

黑体字	表示命令或者诸如字段名、图标或菜单选项之类的图形用户界面（GUI）控件。
等宽字	表示完全按显示原样输入的文本示例、文件名以及目录路径和名称。
斜体字	用于强调词语。斜体还表示必须用相应系统值替代的名称。
host_name	WebSphere Commerce 服务器的全限定主机名（例如 `server.mydomain.ibm.com` 是全限定的）。
instance_name	正在处理的 WebSphere Commerce 实例的名称。
Windows *drive*	表示用于安装正在讨论的产品或组件的驱动器号（例如，`C:`）。

此图标用于标记一个技巧 — 可帮助您完成任务的附加信息。

重要信息

这些部分突出显示特别重要的信息。

注意事项

这些部分突出显示了用于保护数据的信息。

Business 表示特定于 WebSphere Commerce Business Edition 的信息。

Professional 表示特定于 WebSphere Commerce Professional Edition 的信息。

AIX 表示特定于 WebSphere Commerce for AIX® 的信息。

400 表示特定于 WebSphere Commerce for IBM® @server iSeries™ 400®（以前称为 AS/400®）的信息。

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

Solaris 表示特定于 WebSphere Commerce Solaris Operating Environment 软件的信息

Windows 表示特定于 WebSphere Commerce for Windows® 2000 的信息。

路径变量

本指南使用以下变量代表目录路径:

DB2_installdir

此变量代表机器上 DB2 通用数据库的实际安装目录。以下是 DB2 通用数据库在各种操作系统上的缺省安装目录:

AIX `/usr/lpp/db2_08_01`

400 不适用（作为操作系统的一部分安装）

Linux `/opt/IBM/db2/V8.1`

Solaris `/opt/IBM/db2/V8.1`

Windows `C:\Program Files\WebSphere\sqllib`

HTTPServer_installdir

此变量代表机器上 IBM HTTP Server 的实际安装目录。以下是 IBM HTTP Server 在各种操作系统上的缺省安装目录:

AIX `/usr/IBMHttpServer`

400 不适用（作为操作系统的一部分安装）

Linux `/opt/IBMHttpServer`

Solaris `/opt/IBMHttpServer`

Windows `C:\Program Files\WebSphere\IBMHTTPServer`

Oracle_installdir

此变量代表机器上 Oracle 的实际安装目录。以下是 Oracle 在各种操作系统上的缺省安装目录:

AIX `/oracle/u01/app/oracle/product/9.2.0`

400 不适用于 OS/400®。

Linux 对 Linux 不适用

Solaris `/opt/oracle/u01/app/oracle/product/9.2.0`

Windows `C:\oracle\ora91`

WAS_installdir

此变量代表机器上 WebSphere Application Server 的实际安装目录。以下是

WebSphere Application Server 在各种操作系统上的缺省安装目录:

AIX /usr/WebSphere/AppServer

400 /QIBM/ProdData/WebAS5/Base

Linux /opt/WebSphere/AppServer

Solaris /opt/WebSphere/AppServer

Windows C:\Program Files\WebSphere\AppServer

WAS_userdir

400 此变量代表在 iSeries 机器上可以修改或需要用户配置的所有由 WebSphere Application Server 使用的数据所在的目录。此目录的缺省值是:

400 /QIBM/UserData/WebAS5/Base/*WAS_instance_name*

WC_installdir

此变量代表机器上 WebSphere Commerce 的实际安装目录。以下是 WebSphere Commerce 在各种操作系统上的缺省安装目录:

AIX /usr/WebSphere/CommerceServer55

400 /QIBM/ProdData/CommerceServer55

Linux /opt/WebSphere/CommerceServer55

Solaris /opt/WebSphere/CommerceServer55

Windows C:\Program Files\WebSphere\CommerceServer55

WC_userdir

400 此变量代表在 iSeries 系统上可以修改或需要用户配置的所有由 WebSphere Commerce 使用的数据所在的目录。此目录的缺省值是:

400 /QIBM/UserData/CommerceServer55

第 1 部分 WebSphere Commerce 安全性概念

本部分提供了对 WebSphere Commerce 安全性的概念性概述。

第 1 章 WebSphere Commerce 安全性模型简介

本章描述了 WebSphere Commerce 安全性模型以及各种 WebSphere Commerce 安全性概念。

概述

本文档中的信息描述了认证、授权、策略和机密性的概念:

什么是认证?

认证是验证用户或应用程序是其所宣称身份的过程。在 WebSphere Commerce 系统中，所有访问系统的用户和应用程序都需要认证，但临时用户例外。用户认证过程始终在 SSL 下执行。这确保了使用网络监听程序的第三方在用户提交密码时无法*窥探*网络。在认证过程期间从不对密码解密，这与一般的安全性做法相同。使用 128 位密钥（称为*商家密钥*）对所有用户密码进行单向混编和加密。在 WebSphere Commerce 系统的安装和配置期间指定商家密钥。

WebSphere Commerce 系统具有其自己的密码用于管理目的。作为 WebSphere Commerce 站点范围安全性策略的一部分，应当定期更改这些密码。关于如何更改 WebSphere Commerce 系统密码的详细信息，请参阅第 63 页的第 6 章，『设置和更改密码』。

什么是授权?

授权是确定用户是否可以对资源执行特定操作的过程。通过管理 WebSphere Commerce 资源的访问控制策略可确定授权。在 WebSphere Commerce 系统中，在两个方面需要访问控制:

- 为保护 WebSphere Commerce Enterprise JavaBeans™（EJB Bean）防止未授权的访问。在第 161 页的第 16 章，『启用 WebSphere Application Server 安全性』中讨论了此过程。
- 为确保只有经授权方才可执行不同组的 WebSphere Commerce 命令。*《WebSphere Commerce 编程指南和教程》*文档中关于『访问控制』一节讨论了此过程。

什么是访问控制策略?

假定您已完成了对将参与电子交易站点的组织和用户的定义，现在您可通过一组策略（称为*访问控制*的过程）来管理其活动。

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从注册到管理拍卖、到更新产品目录和核准订单，以及运作和维护电子交易站点所需的所有其它数百种活动。

策略授予用户对您站点的访问权。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。

WebSphere Commerce 的授权模型基于访问控制策略的强制实施。由访问控制策略管理器强制实施访问控制策略。总的来说，当用户试图访问受保护资源时，访问控制策略

管理器首先确定该用户所适用的访问控制策略，然后基于所适用的访问控制策略，确定是否允许用户对给定资源执行请求的操作。

什么是审计跟踪?

在计算中，*审计跟踪*用于指用来跟踪计算机活动的电子或纸质日志。例如，雇员可能对公司网络的一部分（例如应收帐款）具有访问权，但是可能未被授予对系统其它部分（例如工资单）的访问权。如果该雇员试图通过输入密码来访问未经授权的部分，则将该不适当的活动记录在审计跟踪中。

在电子交易系统中，审计跟踪用于记录客户活动。审计跟踪记录客户与系统的初始接触以及后续操作（例如对产品或服务的支付和交付）。公司可使用审计跟踪来响应任何查询或投诉。还可使用审计跟踪来调整帐户、为未来规划和预算提供分析和历史信息，以及提供销售记录以备税务审计之用。

审计跟踪还可用于调查计算机空间和因特网上的计算机犯罪。要曝光个人对系统进行的恶意攻击，调查员可遵循犯罪者所留下的审计跟踪。有时计算机犯罪的罪犯无意地在活动日志中（或者可能通过聊天室日志）留下了其因特网服务供应商的审计跟踪痕迹。

什么是机密性?

机密性是保护敏感信息免受非意在的接收方译码的过程。在 WebSphere Commerce 系统中，当敏感信息从用户浏览器流动到 WebSphere Commerce 服务器以及从 WebSphere Commerce 服务器流动回到用户的浏览器时，要求机密性。如第 171 页的第 17 章，『为 IBM HTTP Server 的生产启用 SSL』中所讨论，使用安全套接字层（SSL）为此方案提供了机密性。

机密性还是用在会话管理方面的硬性要求。因为超文本传输协议（HTTP）是无状态的，因此 *cookie* 通常用于持续地向 WebSphere Commerce 服务器标识用户。如果此 cookie 被盗，则可能危及该用户帐户的安全。这通常称为*会话劫持*。如第 57 页的第 5 章，『会话管理』所讨论，WebSphere Commerce 通过使用 cookie 指定的独特功能，来防止会话劫持。

常规安全性注意事项

进行中的安全性评估

WebSphere Commerce 产品线通常经受来自一个独立的 IBM 安全性专家小组的安全性分析。这些专家从仅可通过浏览器访问 WebSphere Commerce 的用户，到在与 WebSphere Commerce Server 所运行的同一系统上拥有帐户的更有特权的用户，以不同的用户观察点来执行安全性分析。来自安全性专家所作分析的反馈用于持续地改进 WebSphere Commerce 的安全性。

WebSphere Commerce 5.5 中的安全性改进

WebSphere Commerce 5.5 已经把策略组预订添加到访问控制基础结构中。

在 WebSphere Commerce 5.4 中，策略应用于由策略所有者的后代所拥有的资源。如果在同一组织层次结构中的不同组织需要不同的访问控制级别，获取不同的级别是困难的。而且，如果组织层次结构很深，理解应用于组织的接近层次结构底层的所有策略也是令人迷惑的。

为了使 WebSphere Commerce 5.5 中的事情更简单更直观，首先要根据业务和访问控制要求将策略分成策略组。例如，一个策略组可以使所需的策略支持合同，而另一个可以只允许注册用户购物。然后，按照组织的业务和访问控制要求，组织可以显式地预订适当的策略组。当组织预订策略组时，只有在这些策略组的策略会应用于组织资源。不会应用它的上级组织策略。然而，如果组织没有显式地预订到策略组，它会继承其最近的上级正在预订的策略预订。

关于策略组的概述，请参阅第 15 页的第 3 章，『授权概念』中讨论“策略组”的部分。

WebSphere Commerce 5.4 中的安全性改进

以下部分列出了 WebSphere Commerce 5.4 中相对于 WebSphere Commerce Suite 5.1 的以及 WebSphere Commerce 5.5 中保留的安全性增强。在 WebSphere Commerce Business Edition 5.1 发行版中已完成了这些增强中的大部分。这些增强总体上适用于:

- WebSphere Commerce 站点管理员
- 系统管理员
- WebSphere Commerce 开发者

请注意有时这些角色是可互换的。

对于站点管理员的增强

以下是总体上针对站点管理员的 WebSphere Commerce 安全性增强:

访问控制

- **访问控制框架** — 关键的增强是在 WebSphere Commerce 5.4 中已经实现并在 WebSphere Commerce 5.5 中保留的新访问控制框架（以及 WebSphere Commerce 5.5 的新策略组增强)。该新框架使用访问控制策略来确定是否允许给定用户对给定资源执行给定操作。新访问控制框架提供了细粒度的访问控制。它与 WebSphere Application Server 提供的访问控制结合（但并不代替后者）工作。在第 75 页的第 3 部分，『管理安全性授权』中详细描述了新访问控制框架。

  新访问控制框架以下列方式增强了先前的访问控制:

  它是富有表现能力的...

  它捕获大量各种访问策略的意图。该框架是通用的，因此它可处理一系列广大的用户组、资源组、操作组和关系组。

  它是分层的...

  访问控制策略属于策略组。组织预订的策略组也可以隐式地应用于它的子组织。

  它是可定制的...

  访问控制策略已从应用程序代码外部化，因此无需重新编译代码就可完成对策略的更改。

它是压缩的...

新框架伸缩自如。访问控制策略的数目随商务过程的数目（而不是对象的数目）增长而增长。大多数组合框架基于隐式条件，因此只要满足条件，则策略将适用。

- **交叉站点脚本编制** — 使用 WebSphere Commerce 配置管理器的“交叉站点脚本保护”节点，拒绝包含指定为不允许的属性或字符的任何用户请求。在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。

认证

- **密码存储** — WebSphere Commerce 在 WebSphere Commerce 数据库中使用 SHA-1 散列法方案加密并存储密码的单向散列，而不是存储密码本身。这确保了用户密码不能由任何人（包括站点管理员或系统管理员）解密。
- **密码失效** — 使用 WebSphere Commerce 配置管理器的“密码失效”节点，要求用户在第一次登录系统时更改密码。在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。
- **帐户策略** — 通过使用 WebSphere Commerce 管理控制台的“帐户策略”页面来为站点设置帐户策略，以定义与帐户相关的使用中的策略。在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。
- **密码策略** — 使用 WebSphere Commerce 管理控制台的“密码策略”页面来为站点设置密码策略以控制用户的密码选择特征。在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。
- **帐户锁定策略** — 使用 WebSphere Commerce 管理控制台的“帐户锁定策略”页面来为站点设置帐户锁定策略以减少危及用户帐户安全的机会。在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。

授权

受密码保护的命令 — 使用 WebSphere Commerce 配置管理器的“受密码保护的命令”节点，当用户正在运行涉及运行指定命令的请求时，要求用户输入密码。在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。

加密的数据

数据库更新工具 — 使用 WebSphere Commerce 配置管理器的“数据库更新工具”节点，更新 WebSphere Commerce 数据库中的加密数据（例如密码和信用卡信息）以及商家密钥。在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。

会话管理

登录超时 — 使用“登录超时”节点，注销在某一延长的时段中未活动的用户并请求他们登录回系统。通过 WebSphere Commerce 配置管理器调用此增强，且在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。

记录

访问记录 — 通过启用访问记录，快速识别出对 WebSphere Commerce 的任何安全性威胁。通过 WebSphere Commerce 配置管理器调用此增强，且在第 43 页的第 4 章，『增强站点安全性』中对此作了详细描述。

对于系统管理员的增强

以下是总体上针对站点管理员的、在 WebSphere Commerce 5.4 建立的并在 WebSphere Commerce 5.5 中保留的安全性增强:

- 一个重要的安全性增强是能够配置 WebSphere Commerce 管理工具在非标准端口号（例如端口 8000 相对于端口 443）上运行。通过将访问限制到此端口，可将对管理工具的访问限制为本地网络或内部网。
- 通过使用“启动安全性检查”页面，从 WebSphere Commerce 管理控制台启动安全性程序，该程序检查并删除可能包含潜在的安全性隐患的临时 WebSphere Commerce 文件。

对于 WebSphere Commerce 程序员的增强

关键的增强是在 WebSphere Commerce 5.4 中实现并在 WebSphere Commerce 5.5 中保留的新访问控制框架。该框架使用访问控制策略来确定是否允许给定用户对给定资源执行给定操作。新访问控制框架提供了细粒度的访问控制。它与 WebSphere Application Server 提供的访问控制结合（但并不代替后者）工作。在第 75 页的第 3 部分，『管理安全性授权』中详细描述了新访问控制框架。

新访问控制框架以下列方式增强了先前的访问控制:

它是富有表现能力的...
它捕获大量各种访问策略的意图。该框架是通用的，因此它可处理一系列广大的用户组、资源组、操作组和关系组。

它是分层的...
由组织所拥有的访问控制策略同样应用于子组织。

它是可定制的...
访问控制策略已从应用程序代码外部化，因此无需重新编译代码就可完成对策略的更改。

它是压缩的...
新框架伸缩自如。访问控制策略的数目随商务过程的数目（而不是对象的数目）增长而增长。大多数组合框架基于隐式条件，因此只要满足条件，则策略将适用。

关于程序员所要考虑的安全性注意事项的更多信息，请参阅《*WebSphere Commerce 编程指南和教程*》文档。

WebSphere Commerce Suite 5.1 Professional Edition 中的安全性改进

Commerce Suite 5.1 代表新的电子交易体系结构，并且是对基于 C++ 的 Commerce Suite 4.1 的完全重写。它包含了先前 WebSphere Commerce Suite 版本的所有安全性功能，而且添加了新的安全性改进。WebSphere Commerce 5.5 继承了这些改进。

Commerce Suite 5.1 继续提供保护防止对 WebSphere Commerce Suite 管理员和购物者资源的未授权访问，该保护由较早发行版通过以下方式提供:

- 继续支持访问控制功能，这些功能确保 WebSphere Commerce Suite 用户在获得对敏感信息的访问权或者提交敏感信息之前，是经过认证的或处于 SSL 方式。
- 将 WebSphere Commerce Suite 命令指定给组，以便只有站点管理员或商店级别的管理员可执行特定命令，遵循了与 Commerce Suite 4.1 相同的模型。

一般安全性增强

由于 Commerce Suite 5.1 以 Java™ 的重写，除去了困扰用 C++ 所写软件的大量内在安全性问题。Java 不使用指针，因此它消除了缓冲区溢出问题，而这是大多数基于 C++ 的软件的安全性薄弱环节。通过遵循行业标准 J2EE 规范，WebSphere Commerce 使用强类型检查以确保服务器不执行由不正当个人所指定的无赖语句。

在 WebSphere Commerce 系统中，使用了工业标准三重 DES（数据加密标准）算法来保护敏感信息。对包含三重 DES 算法的数据包进行数字签名，以便在数据包遭篡改的情况下，WebSphere Commerce 服务器将不启动。WebSphere Commerce 5.5 中保留了这些增强。

会话管理

完全重写了 WebSphere Commerce 会话管理以获取最大安全性，它使用独特技术以确保 cookie 不被盗。使用仅通过 SSL（安全套接字层）流动且由加密时间戳记组成的认证 cookie，重写的会话管理设计防止了会话劫持。

认证

使用商家指定的 128 位密钥，安全地加密了 WebSphere Commerce 服务器在执行期间所需的系统和应用程序密码，并将它们存储在 WebSphere Commerce 配置文件中。加密了出现在用户 URL 输入框中的敏感信息以保护购物者防止未授权的泄露。

记录

WebSphere Commerce 日志系统设计时以安全性为关键的注意事项，从而敏感信息（例如购物者密码和信用卡信息）缺省情况下不被记录到 WebSphere Commerce 日志文件中。

第 2 章 认证

WebSphere Commerce 将认证视为验证用户或应用程序是其所宣称身份的过程。本部分描述了 WebSphere Commerce 认证的若干方面的详细信息。

WebSphere Commerce 认证模型

WebSphere Commerce 认证模型基于以下概念:

- 提问机制
- 认证机制
- 用户注册表

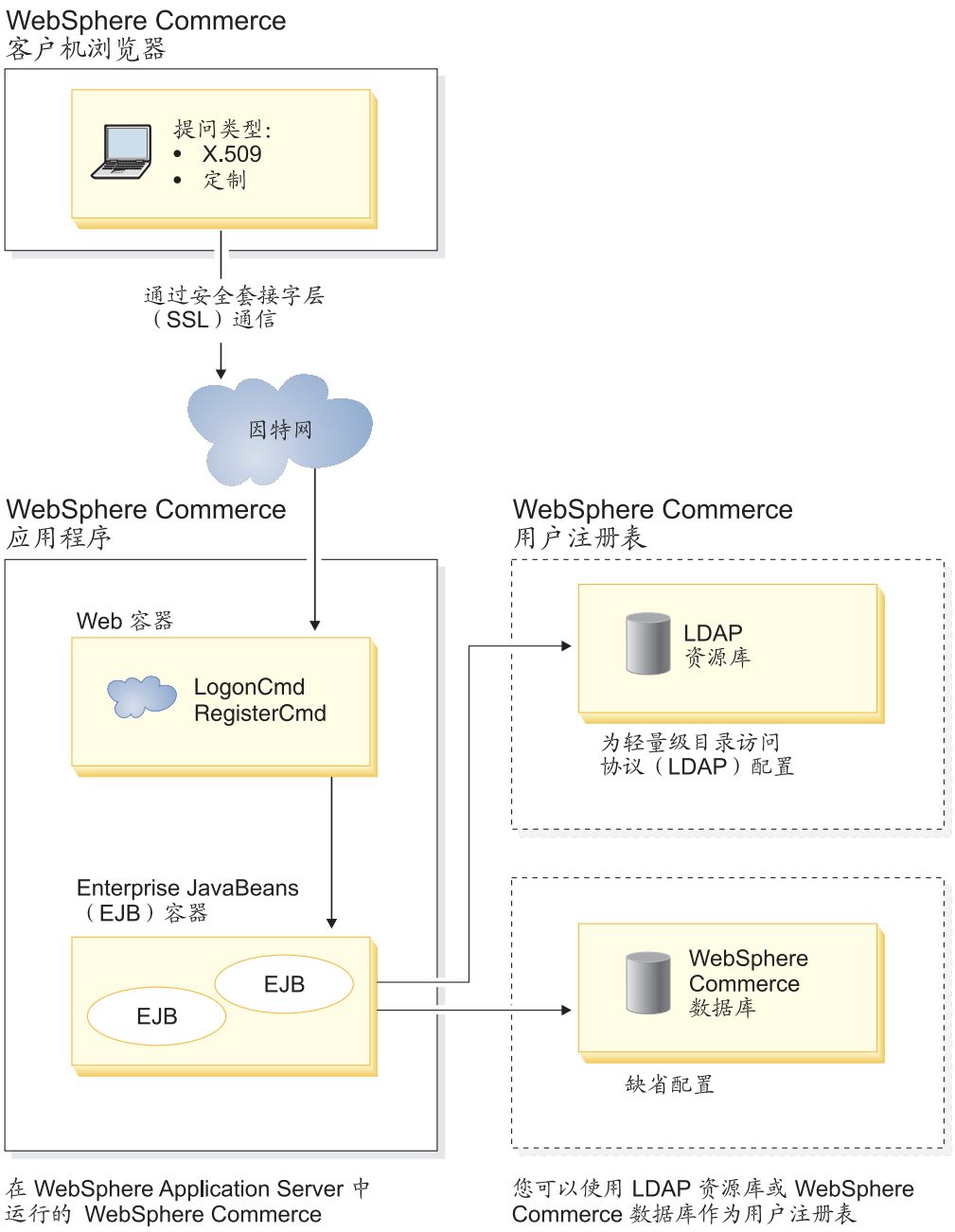


图 1. WebSphere Commerce 安全性模型

提问机制

提问机制指定服务器如何提问以及检索来自用户的认证数据。WebSphere Commerce 支持以下认证方法或提问机制:

基于表单或定制认证方式

此认证机制通过 HTML 页面或 JSP 表单允许特定于站点或商店的登录。

基于证书的认证方式（X.509 证书）

证书提问机制意味着配置 Web 服务器来通过 SSL 执行相互认证。要求客户机呈示证书以建立连接。然后此证书成为映射到用户注册表的凭证。

认证机制

*认证机制*通过对照关联的用户注册表验证用户的认证数据来认证用户。认证过程之后，WebSphere Commerce 发出将在每个后续请求中与用户关联的认证令牌。此令牌在用户注销或关闭浏览器时终止。

证书验证

这是验证 X.509 客户证书受信于 Web 服务器且还符合 Web 服务器证书策略的过程。WebSphere Commerce 还对照 WebSphere Commerce 数据库验证 X.509 证书。Web 服务器对证书执行粗粒度的访问控制，而 WebSphere Commerce 对证书执行细粒度的访问控制。

LDAP 绑定

这是通过执行用于认证用户的 LDAP 绑定操作来验证所提供的提问信息是否有效的过程。

数据库绑定

这是将认证过程期间提供的用户标识和密码与存储在 WebSphere Commerce 数据库中的认证信息进行比较，来验证前者是否有效的过程。

用户注册表

用户注册表是包含用户信息以及用户的认证信息（例如密码）的资源库。由主体（即表示用户注册表中的个人用户或系统实体）提供的认证信息可通过对照用户注册表来验证或确认。

WebSphere Commerce 基于两个用户域来支持用户注册表：LDAP 用户注册表和 WebSphere Commerce 数据库。

WebSphere Commerce 支持以下 LDAP 供应商：

- AIX 400 Linux Solaris Windows IBM SecureWay® Directory
- AIX Solaris Windows Netscape Directory Server
- 2000 Windows 2000 Active Directory

凭证

WebSphere Commerce 服务器支持基于验证凭证（例如证书、令牌或“用户标识 - 密码”对）的认证机制。对照支持此类方案的用户注册表来验证凭证。

WebSphere Commerce 令牌

WebSphere Commerce 使用安全认证 cookie 来管理认证数据。认证 cookie 仅通过 SSL 流动，且出于最大的安全性考虑而加盖了时间戳记。此 cookie 用于每当执行敏感命令（例如要求输入用户信用卡号码的 `DoPaymentCmd`）时认证处于 SSL 连接下的用户。此 cookie 可能由未授权用户盗用的风险已极小化。

第二个在处于 SSL 连接或非 SSL 连接下的浏览器和服务器之间流动的 cookie 用于验证处于非 SSL 连接下的用户。

WebSphere Application Server LTPA 令牌

LTPA 令牌是一段数据，它包含必要的用户信息来确定用户所请求资源的访问许可权。它包含认证数据以及 WebSphere Application Server LTPA 服务器的数字签名。

在 WebSphere Application Server 轻量级第三方认证方案的情况下，包含用户有关信息的 LDAP 目录是执行认证时对照的用户注册表。资源服务器与 WebSphere Application Server 安全性服务器取得联系，并将 LTPA 指定为认证机制。它还提供与请求关联的认证数据。然后 WebSphere Application Server 安全性服务器对照 LTPA 服务器来验证认证数据，并返回 LTPA 令牌。

单一注册

HTTP 单一注册背后蕴藏的原理是为不同的 Web 应用程序保留用户认证。它的目标是:避免在给定信任域中多次提示用户提供安全性凭证，这样的域包含:

- 协作但是不同的 WebSphere Application Server 服务器。
- 协作应用程序（例如象 IBM SecureWay Directory Server 那样的 LDAP 服务器）。

在单一注册（SSO）方案中，HTTP Cookie 用于将用户的认证信息传播到不同的 Web 服务器上，使用户不必在每次新的客户机／服务器会话（假定是基本认证方式）时输入认证信息。

关于对 WebSphere Commerce 实现单一注册的步骤，请参阅第 69 页的第 7 章，『单一注册』。

认证策略

认证策略是适用于认证过程及 WebSphere Commerce 对认证数据的验证的规则集。如以下各部分中所述，WebSphere Commerce 支持帐户策略、其它与认证相关的策略以及会话策略。

帐户策略

以下部分描述了 WebSphere Commerce 提供的帐户策略:

帐户策略

WebSphere Commerce 管理控制台的帐户策略页面允许您设置帐户策略。 帐户策略定义与帐户相关的策略，例如密码和帐户锁定策略。

一旦创建了帐户策略，则可将策略指定给用户。请注意在帐户策略正在使用中（即已将帐户策略指定给用户）的情况下不能删除帐户策略。

关于创建帐户策略的信息，请参阅第 52 页的『设置帐户策略』。

另见 WebSphere Commerce 联机帮助中的参考主题 “缺省认证策略”。

帐户锁定策略

WebSphere Commerce 管理控制台的 “帐户锁定策略” 允许您为 WebSphere Commerce 内的不同用户角色设置帐户锁定策略。 帐户锁定策略在对帐户启动了恶意操作的情况下将禁用该用户帐户，以便减少操作危及帐户安全的机会。

帐户锁定策略强制实施以下项:

- 帐户锁定阈值。这是禁用帐户前无效登录尝试的数目。
- 连续失败登录延迟。这是在两次尝试登录失败之后，不允许用户登录的时间段。对每个连续的登录失败，按配置的时间延迟值（例如 10 秒）来增加延迟。

关于创建帐户锁定策略的信息，请参阅第 53 页的『设置帐户锁定策略』。

密码策略

WebSphere Commerce 管理控制台的“密码策略”页面让您能够控制用户的密码选择以便定义密码的特征，来确保密码符合站点的安全性策略。

此功能定义密码必须遵循的属性。密码策略强制实施以下条件:

- 用户标识和密码是否能够匹配。
- 连续字符的最大出现次数。
- 任意字符的最多出现次数。
- 密码的最大使用寿命。
- 字母字符的最小数目。
- 数字字符的最小数目。
- 密码的最小长度。
- 是否可重新使用用户先前的密码。

关于创建密码策略的信息，请参阅第 52 页的『设置密码策略』。

另见 WebSphere Commerce 联机帮助中的参考主题“缺省认证策略”。

其它与认证相关的策略

以下部分描述了 WebSphere Commerce 中提供的其它与认证相关的策略:

密码失效

使用配置管理器的“密码失效”节点来启用或禁用密码失效功能。当启用此功能时，如果用户的密码已过期，则要求 WebSphere Commerce 用户改变他们的密码。在此情况下，用户会被重定向到要求他们更改密码的页面。用户要能够访问站点上的任何安全页面，必须先更改他们的密码。

关于使用“密码失效”节点的信息，请参阅第 47 页的『启用密码失效』。

受密码保护的命令

使用配置管理器的“受密码保护的命令”节点来启用或禁用“受密码保护的命令”功能。当启用此功能时，WebSphere Commerce 会在继续处理请求（该请求运行指定的 WebSphere Commerce 命令）之前，要求登录到 WebSphere Commerce 的注册用户输入其密码。

警告: 配置受密码保护的命令时，显示在命令选择列表中的一些命令可由一般用户或临时用户执行。将此类命令配置为受密码保护将限制一般用户和临时用户对这些命令的运行。因此，在将命令配置为受密码保护时，应当谨慎。

注: WebSphere Commerce 在可用命令列表中将仅显示在 `URLREG` 表中指定为已认证或设置了 `https` 标志的命令。

关于使用“受密码保护的命令”节点的信息，请参阅第 47 页的『启用受密码保护的命令』。

会话策略

在 WebSphere Commerce 中，会话策略体现在登录超时策略中。

使用登录超时策略，WebSphere Commerce 将使用“登录超时”节点注销某一延长的时段中未活动的用户并请求他们登录回系统。通过 WebSphere Commerce 配置管理器调用此增强，且在第 46 页的『启用登录超时』中对此作了详细描述。

第 3 章 授权概念

WebSphere Commerce 将访问控制或授权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 中的授权或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。

业务模型

在 WebSphere Commerce 5.4 中，站点管理员必须在您创建实例之后做出以下决策:

1. 适合于站点的组织结构
2. 分配给特定组织的角色
3. 所需的访问控制策略

在做出所有这些决定之后，那么可对照适当的组织发布商店。

在 WebSphere Commerce 5.5 中，已通过创建业务模型简化了这个过程。业务模型提供了针对特定的电子交易解决方案的组织结构、角色、访问控制策略和预订义的商店。业务模型可以用作基本的开发舞台，可向其添加、删除或更改内容。

随 WebSphere Commerce 5.5 提供了以下业务模型:

- 消费者直销
- B2B 直销
- 需求链
- 主管
- 供应链

为了了解业务模型以及 WebSphere Commerce 的访问控制组件，必须首先了解电子交易站点的典型组织层次结构。

注: 关于业务模型的更多信息，请参阅《*WebSphere Commerce 基础指南*》。

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。

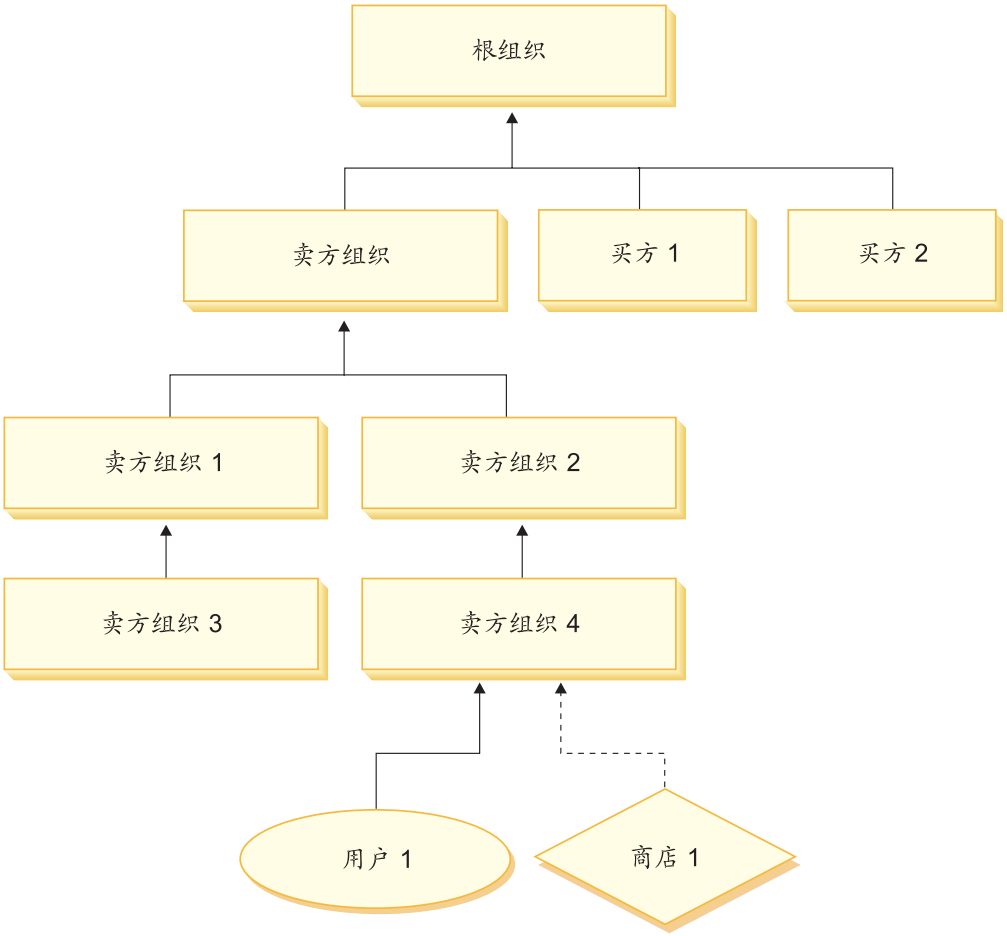


图 2. “商家到商家”站点的组织层次结构

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（即创建适当的角色并向其分配成员）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”的客户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。

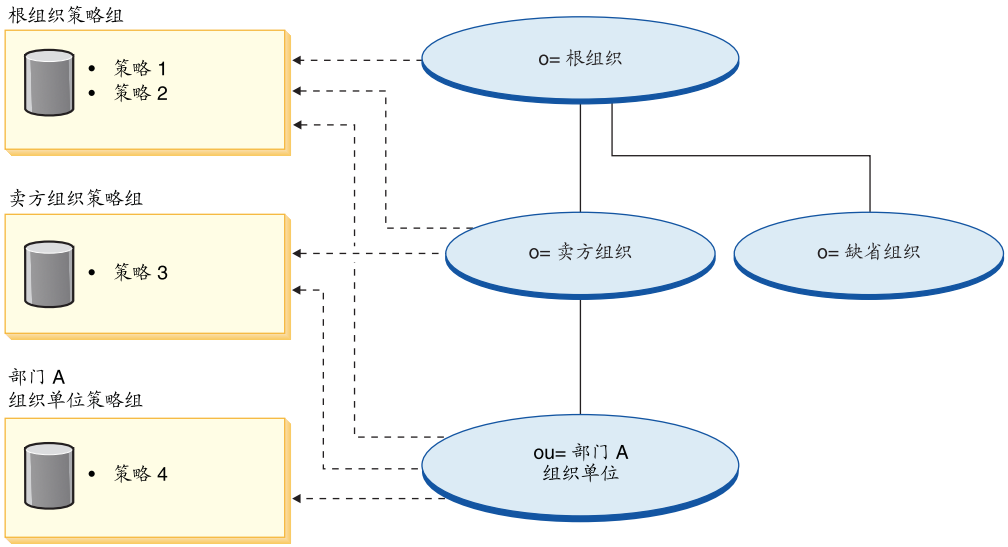
买方管理员的责任总结如下:

- 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 WebSphere Commerce 联机帮助。

策略组

WebSphere Commerce 5.5 支持各种业务模型，并且每个业务模型都有自己的访问控制策略集合。为了将模型内的策略集合分组，创建了策略组。策略将被显式地分配到适当的策略组，然后组织可以预订这些策略组中的一个或多个。例如，在下图中，卖方组织预订卖方组织策略组和根组织策略组。

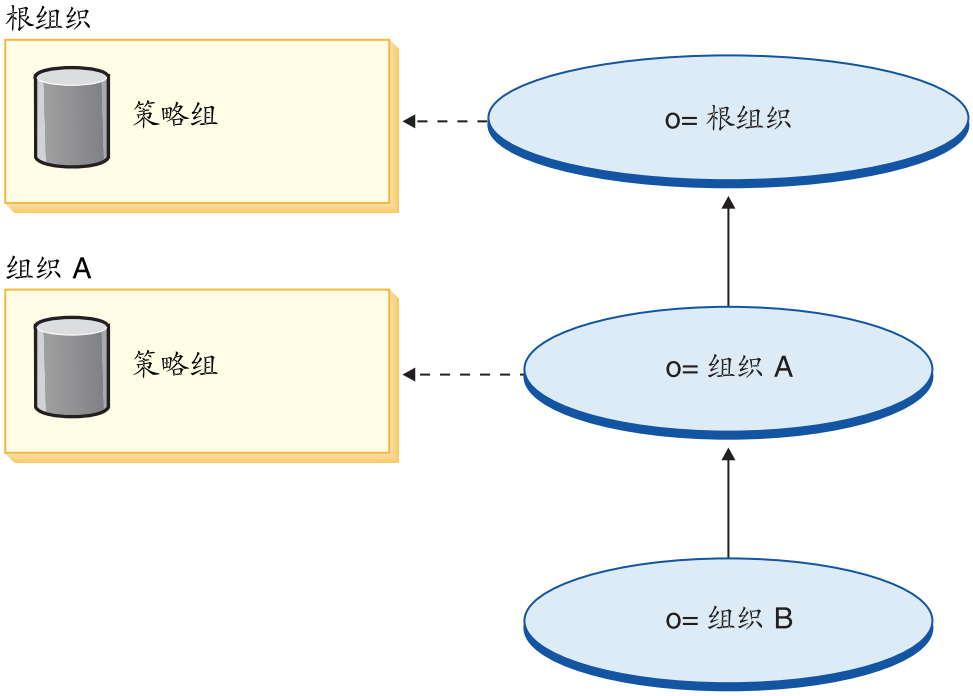


策略指定给策略组。例如，在上图中，策略 1 和策略 2 指定给根组织策略组，策略 3 指定给卖方组织策略组，策略 4 指定给部门 A 组织单位策略组。

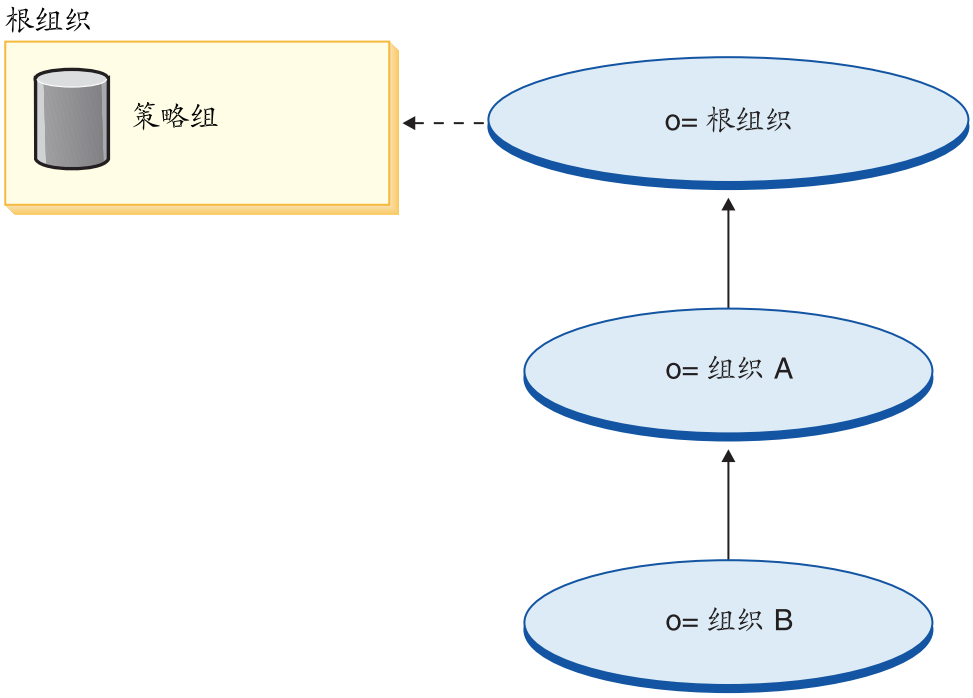
策略组预订

在先前版本的 WebSphere Commerce 中，策略适用于策略所有者组织的子代拥有的所有资源。例如，如果组织 A 有某个策略并且是组织 B 的父组织，那么组织 B 隐式地也拥有该策略。现在，在 WebSphere Commerce 5.5 中，组织可以预订策略组。在 WebSphere Commerce 5.5 中，如果组织 B 没有预订任何策略组，那么访问控制框架将开始向上搜索组织层次结构，直到它遇到一个预订了至少一个策略组的组织。如果组织 B 的直接父组织组织 A 预订了策略组，则搜索停止，策略适用于组织 A 和 B。如

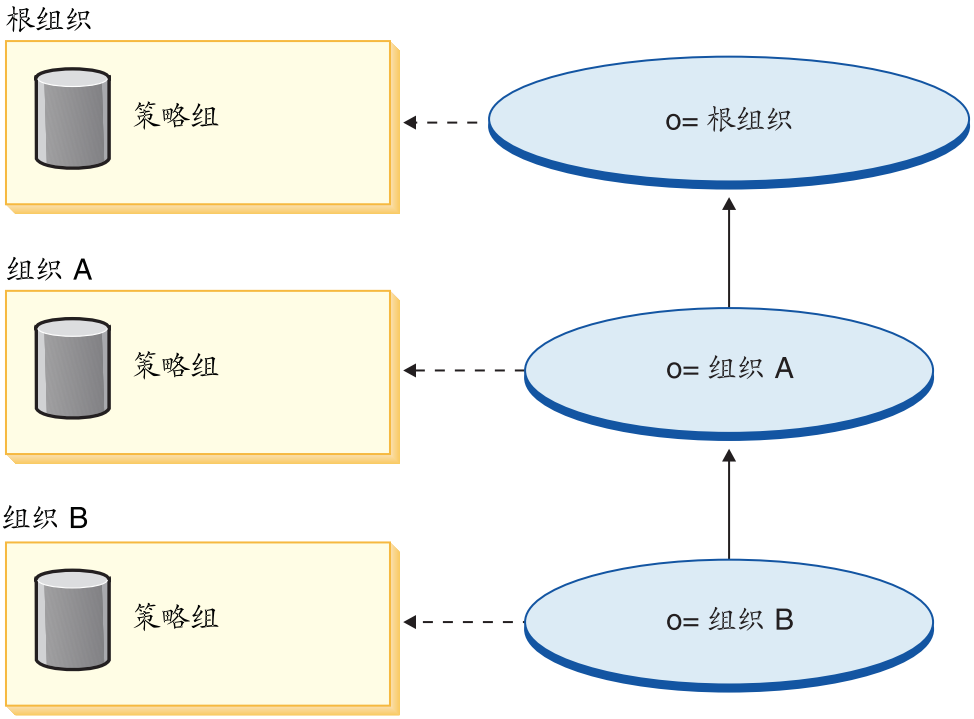
下图中所示。



如果组织 A 没有预订策略组，则搜索继续沿着组织层次结构向上进行，直到到达带有预订的组织。这如下图所示，图中的根组织预订了策略组。该组中的策略适用于组织 B 和组织 A。



如果组织 B 预订了策略组，则搜索停止于组织 B，所以只有组织 B 策略组中的策略适用于组织 B。



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，一个成员组与多个成员组类型关联。

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。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。站点管理员、买方管理员、卖方管理员或渠道经理使用 WebSphere Commerce 组织管理控制台将角色指定给用户或显示地将用户指定给访问组。

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 MBRGRPCOND 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。而且，由于多访问组可以应用于同一用户属性，因此向用户指定属性可以隐式地包括在多访问组内的该用户。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客户提供的俱乐部。成为用户组的成员可使客户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客户经常购买旅行书和行李包，则可将这些客户指定为称为“高级客户的旅行俱乐部”的成员组。类似地，可创建用户组以奖励经常光顾的客户。

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策略中，操作是 Execute，资源是正在执行的命令。在视图的基于角色的策略中，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，在数据 bean 策略中，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。如果拥有资源的组织没有预订策略组，那么就会应用策略组中最近的上级组织预订的策略。

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 编程指南和教程*》。

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进行指定，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，则这一部分的 RELATIONSHIP_CHAIN 得到满足。

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 135 页的『定义关系组』。

访问控制策略类型

有两种类型的访问控制策略:

- 可分组标准策略（策略类型 -2）
- 可分组模板策略（策略类型 -3）

可分组模板策略和可分组标准策略都必须属于某个策略组，以便应用于系统中。在组织中应用一次可分组标准策略，这些组织是预定包含该策略的策略组的组织。

实际上可分组模板策略是动态的，因为它们具有一个访问组，在系统正在运行的时候，该访问组的作用域会达到拥有资源的组织。例如，当此类策略适用于组织 XYZ 所拥有的资源时，它会检查用户是否担任了组织 XYZ 或其上级的指定角色之一。

特殊缺省访问控制策略

以下策略需要一些额外解释:

- 站点管理员可进行任何操作（SiteAdministratorsCanDoEverything）
- 准用户客户服务组代表客户执行准用户命令（BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup）

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。

BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup 策略是一个特殊策略，它允许某些管理用户代表其他用户运行指定的命令。例如，当客户请求客户服务代表代表他创建订单时，就需要此策略。在此案例中，客户服务代表可以运行命令以至于看上去像是客户自己在运行命令一样。

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。

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。在此案例中，组织 X 必须支持“产品经理”角色。通常，在把组织的角色指定给任何用户前，该组织必须支持该角色。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: 为用户和组织指定角色在 MBRROLE 表中进行。

随 WebSphere Commerce 附带的缺省角色可分为以下类别:

- 技术操作角色
- 市场营销角色
- 操作角色
- 客户服务角色
- 商务关系角色
- 产品管理和销售策略角色

在 WebSphere Commerce 5.5 中，每个角色都与一个或多个业务模型相关联。在每个模型内，一个角色可以使用贸易加速器、管理控制台和组织管理控制台工具执行选择数目的任务。关于业务模型的更多信息，请参阅《*WebSphere Commerce 基础*》。

以下图表显示了每个角色对每个工具所具有的访问权。在将角色分配给用户之前，请确保您掌握有关适用于该角色的访问限制的正确信息。

映射到每个商店样本的 WebSphere Commerce 工具的角色

表 1. 映射到 WebSphere Commerce 工具的角色

角色	样本	工具
客户代表	• B2B 直销: 多乐五金	• 加速器
买方管理员	• B2B 直销: 多乐五金	• 组织管理控制台
买方核准员	• B2B 直销: 多乐五金	• 组织管理控制台
买方（销售方）	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金	• 加速器
买方（购买方）	• B2B 直销: 多乐五金 • 主管: 主管商店 • 供应链: 供应商主管商店	此角色可用于这些样本中，但不能使用任何特定工具。
类别经理	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金 • 需求链: 主管商店，产品目录有用资源商店, • 主管: 主管商店，产品目录有用资源商店 • 供应链: 产品目录有用资源商店，供应商主管商店	• 加速器
渠道经理	• 需求链: 渠道中心 • 主管: 主管中心 • 供应链: 商店目录	• 加速器 • 组织管理控制台
客户服务代表	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金	• 加速器
客户服务主管	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金	• 加速器

表 1. 映射到 WebSphere Commerce 工具的角色 (续)

角色	样本	工具
后勤部经理	• B2B 直销: 多乐五金 • 供应链: 供应商主管商店	• 加速器
市场部经理	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金 • 需求链: 渠道中心，主管商店，转销商商店前台有用资源商店 • 主管: 主管商店，主管商店前台有用资源商店	• 加速器
业务经理	• 消费者直销: 时尚潮流 • 需求链: 主管商店 • 主管: 主管商店	• 加速器
提货装货员	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金	• 加速器
采购买方	• B2B 直销: 多乐五金 • 供应链: 供应商主管商店	此角色可用于这些样本中，但不能使用任何特定工具。
采购买方管理员	• B2B 直销: 多乐五金 • 供应链: 供应商主管商店	此角色可用于这些样本中，但不能使用任何特定工具。
产品经理	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金	• 加速器
收货员	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金	• 加速器
注册客户	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金 • 需求链: 渠道中心，主管商店 • 主管: 主管中心，主管商店 • 供应链: 商店目录，供应商主管商店	此角色可用于这些样本中，但不能使用任何特定工具。
退货管理员	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金	• 加速器
销售经理	• B2B 直销: 多乐五金 • 供应链: 供应商主管商店	• 加速器

表 1. 映射到 WebSphere Commerce 工具的角色 (续)

角色	样本	工具
卖方	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金 • 需求链: 主管商店 • 主管: 主管商店 • 供应链: 供应商主管商店	• 加速器
卖方管理员	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金 • 需求链: 渠道中心，主管商店 • 主管: 主管中心，主管商店 • 供应链: 商店目录，供应商主管商店	• 组织管理控制台
站点管理员（根组织）	• 消费者直销: 时尚潮流 • B2B 直销: 多乐五金 • 需求链: 渠道中心，主管商店，产品目录有用资源商店，转销商商店前台有用资源商店 • 主管: 主管中心，主管商店，产品目录有用资源商店，主管商店前台有用资源商店 • 供应链: 商店目录，供应商主管商店，产品目录有用资源商店，供应商有用资源商店	• 加速器 • 组织管理控制台 • 管理控制台

注:

1. 站点管理员是对管理控制台拥有访问权的唯一角色。
2. 关于特定角色以及这些角色可以访问的每个工具中的菜单的更多信息，请参阅 WebSphere Commerce Production 联机帮助中的 “Roles” 文件。
3. 关于每家样本商店的更多信息，请参阅 WebSphere Commerce 生产和开发联机帮助中的 “商店”

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

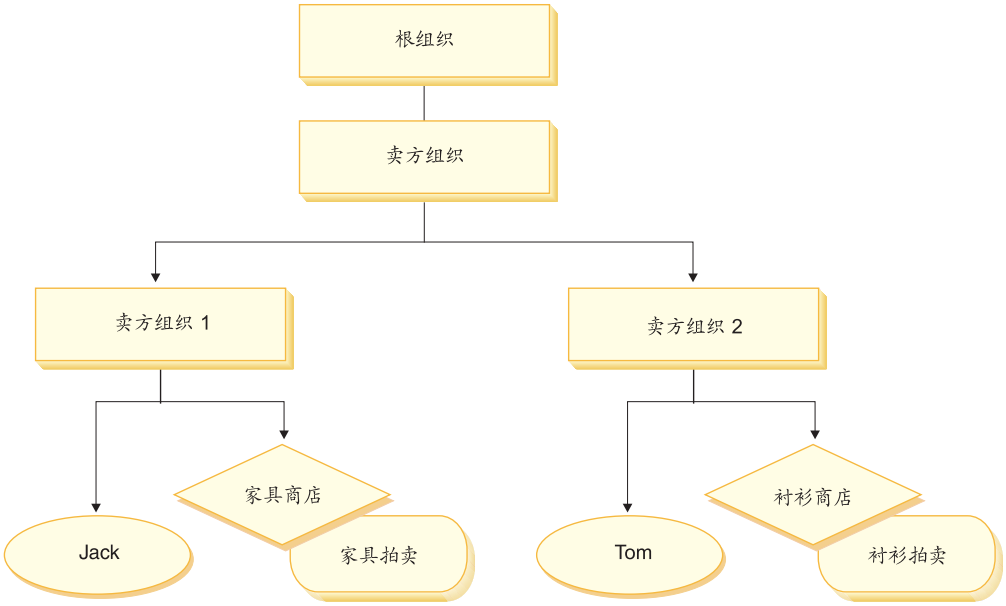
*策略管理器*是确定是否允许当前用户对指定资源执行指定操作的访问控制组件。访问控制策略以 XML 格式指定。实例创建期间，将缺省策略和策略组装入相应的数据库表中。当启动 WebSphere Commerce Application Server 时，访问控制信息高速缓存在内

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 管理控制台中的适当的注册表来完成。如果策略数据已更改，则应该更新“访问控制策略”注册表。如果策略数据组已更改，则应该更新“访问控制策略组”注册表。重新启动 WebSphere Commerce 也将导致更新高速缓存。

当用户试图对受保护的资源执行操作时，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。

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。

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 29 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:

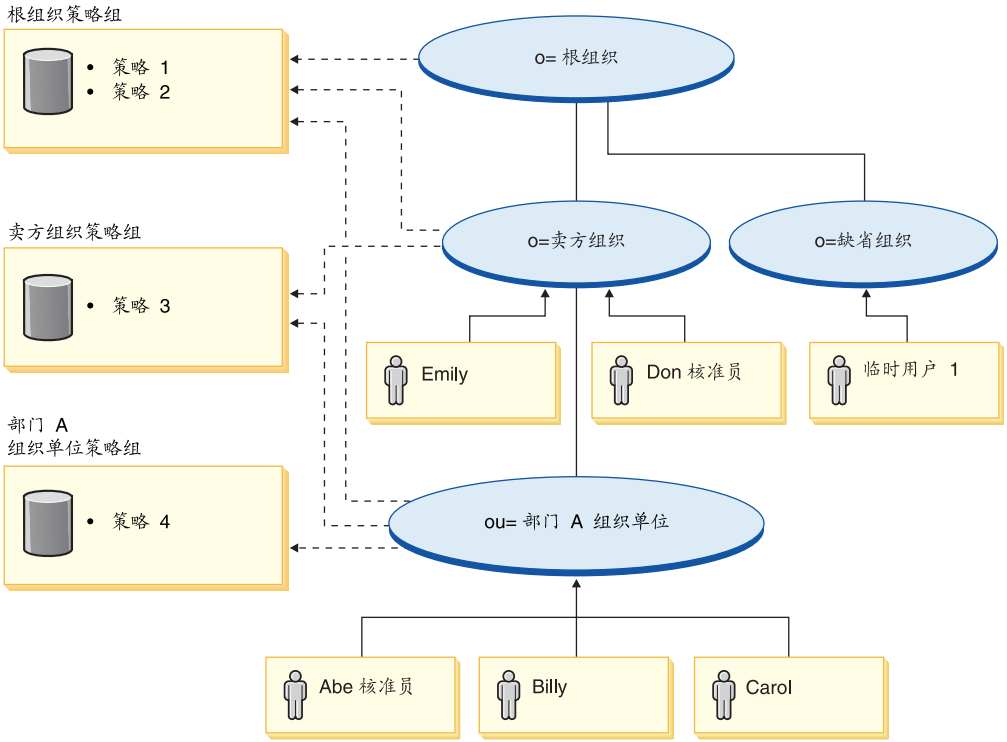
- 命令实现 getResources() — 此方法指定需要对当前操作进行检查的资源实例；在这里现在命令是操作。WebSphere Commerce 运行时将强制当前用户具有 getResources() 指定的所有资源的访问权限。缺省情况下，getResources() 返回 null，即，它不执行任何资源级别的检查。
- 命令调用 checkIsAllowed(Object Resource, String Action) — 当运行时调用 getResources() 时，命令编写器不知道需要检查哪些资源的情况下，命令可以按照需要调用此 checkIsAllowed() 方法，以确定当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 bean 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。

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可分组标准访问控制策略和可分组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。关于可分组标准策略和可分组模板策略的更多信息，请参阅第 25 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组织:

- 根组织
- 卖方组织
- 缺省组织
- 部门 A 组织单位

图中的实线指示所有权，点划线指示预订。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 组织单位的父组织。

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 组织单位。临时用户 1 尚未注册，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 组织单位的核准员角色。

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到站点中至少一个组织的所有用户。
- 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 组织单位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。

评估可分组的标准策略

本部分引导您完成可分组的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, - ]
```

这是一个可分组的标准的基于角色的策略，它是根组织、卖方组织和决策 A 组织单位正在预订的根组织策略组的一部分。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 ]
```

这是一个可分组的标准的资源层次策略，它是根组织、卖方组织和决策 A 组织单位正在预订的根组织策略组的一部分。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, - ]
```

这是一个可分组的标准资源级别策略，它是卖方组织和部门 A 组织单位正在预订的卖方组织策略组的一部分。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, - ]
```

这是一个可分组的标准的资源级别的策略，它是部门 A 预订的部门 A 组织单位策略组的一部分。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. 因为没有指定任何商店标识，所以将命令的所有者设置为根组织。因此，只有那些属于由根组织预订的策略组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 是根组织正在预订的策略组的一部分。
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。因为部门 A 预订了策略组，所以属于那些策略组的所有策略都将应用: 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，只有那些属于由根组织预订的策略组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。因为部门 A 预订了策略组，所以属于那些策略组的所有策略都将应用: 策略 1、2、3 和 4。
2. 策略 3 授予访问权，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，只有那些属于由根组织预订的策略组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。因为卖方组织预订了策略组，所以属于那些策略组的所有策略将适用: 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 1 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. 因为没有指定任何商店标识，所以将命令的所有者设置为根组织。因此，只有那些属于由根组织预订的策略组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 1 不是注册用户访问组的成员。

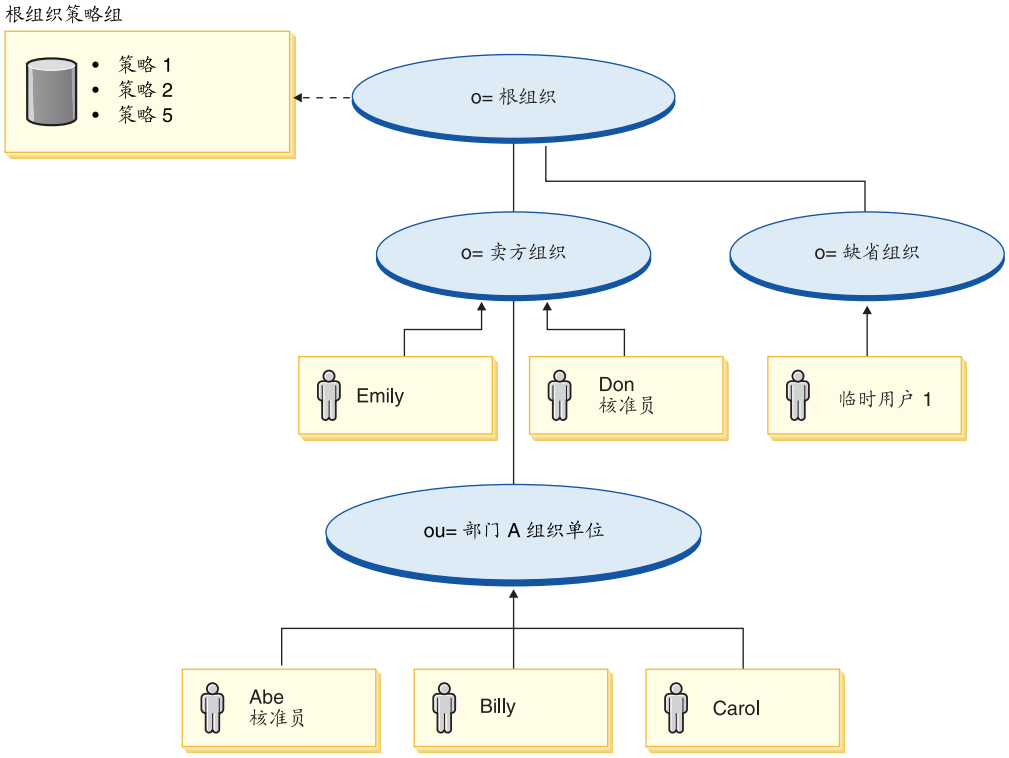
资源级别的检查:

1. 因为命令级别的检查失败，因此不会执行资源级别的检查。

因为临时用户 1 未通过命令级别的检查，因此他不能更新他自己的文档。

评估可分组的模板策略

本部分基于下面图表中显示的配置。



与更新文档相关的访问控制策略

在此配置中，访问控制策略 1 和 2 仍适用，但是可分组的标准策略 3 和 4 现在由可分组的模板策略 5 替换。关于策略 1 和 2 的更多信息，请参阅第 32 页的『评估可分组的标准策略』。

策略 5:

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

此策略是可分组的模板资源级别策略。它是根组织正在预订的根组织策略组的一部分。可分组模板策略动态应用于在运行时期间拥有资源的组织。这些策略通常使用参数化的访问组。在此例中，使用以下参数化的访问组:

- 组织核准员：此组隐式地包含了具有拥有文档资源的组织或其上级组织的核准员角色的所有用户。

方案

以下方案基于先前的只有一个策略组的图表中显示的配置。根组织策略组包含策略 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，只有那些属于由根组织预订的策略组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、2 和 5。
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。部门 A 没有预订任何策略组，因此访问控制框架将开始向上搜索组织层次结构，直到它遇到一个预订了至少一个策略组的组织。部门 A 的直接父组织 “卖方组织” 也没有预订策略组。继续沿组织层次结构向上，直到根组织。此组织预订了一个策略组；那么可以应用它的策略：策略 1、2 和 5。
2. 可分组的模板策略 5 应用于拥有资源的组织：部门 A。此参数化的访问组（组织核准员）动态地将作用域定为当前资源上下文，这样它将检查用户是否满足拥有资源的组织或其上级组织的访问组条件。在此例中，因为 Don 是卖方组织（部门 A 的上级组织）核准员，所以他满足访问组的条件。因为他正在对文档资源执行 “更新文档” 命令操作，也满足策略 5 的其它要素，所以通过了资源级别的策略检查。

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，只有那些属于由根组织预订的策略组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、2 和 5。
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。卖方组织没有预订任何策略组，因此访问控制框架将开始向上搜索组织层次结构，直到它遇到一个预订了至少一个策略组的组织。继续沿组织层次结构向上，直到根组织。此组织预订了一个策略组；那么可以应用它的策略：策略 1、2 和 5。

2. 可分组的模板策略 5 应用于拥有资源的组织: 卖方组织。此参数化的访问组（组织核准员）动态地将作用域定为当前资源上下文，这样它将检查用户是否满足拥有资源的组织或其上级组织的访问组条件。在此例中，因为 Abe 是部门 A 组织单位（卖方组织的上级组织）核准员，所以他不满足访问组的条件。

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: 该策略是资源层次策略。它的策略类型是可分组模板。

在第一个示例中，将学习如何使用 WebSphere Commerce 组织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 组织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。

在组织管理控制台中查找策略

1. 登录到 WebSphere Commerce 组织管理控制台。从“访问管理”菜单，选择**策略**。
2. 由于根组织拥有大多数的缺省访问控制策略，因此从列表框选择根组织。
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**以查看在该策略中使用的成员（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 AuctionAdministratorForOrg 开头。符号 ForOrg 表示这是一个可分组模板策略。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。

在 XML 文件中策略看上去如下:

```
<!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
-->
<Policy
Name="AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="groupable 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: 策略的类型，例如可分组标准或可分组模板。

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。要查看哪些操作金额资源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 组织管理控制台的“策略”页面上查找策略。

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 75 页的第 3 部分，『管理安全性授权』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 2 部分 管理安全性认证

本部分描述通常可由 WebSphere Commerce 站点管理员执行的安全性认证任务。

第 4 章 增强站点安全性

要增强 WebSphere Commerce 站点的安全性，可在 WebSphere Commerce 配置管理器中启用任何以下功能:

- 使用“登录超时”节点注销在某一延长的时段中未活动的用户并要求他们登录回系统。关于详细信息，请参阅第 46 页的『启用登录超时』。
- 使用“密码失效”节点，要求用户在第一次登录系统时更改密码。关于详细信息，请参阅第 47 页的『启用密码失效』。
- 使用“受密码保护的命令”节点，当用户正在运行涉及运行指定命令的请求时，要求用户输入密码。关于详细信息，请参阅第 47 页的『启用受密码保护的命令』。
- 使用“数据库更新工具”节点，更新 WebSphere Commerce 数据库中的加密数据（例如密码和信用卡信息）以及商家密钥。关于详细信息，请参阅第 48 页的『更新加密数据』。
- 使用“交叉站点脚本保护”节点，拒绝包含指定为不允许的属性或字符的任何用户请求。关于详细信息，请参阅第 49 页的『启用交叉站点脚本保护』。
- 通过启用访问记录，快速识别出对 WebSphere Commerce 的任何安全性威胁。关于详细信息，请参阅第 51 页的『启用访问记录』。

并且，可在 WebSphere Commerce 管理控制台的“安全性”下拉菜单中启用以下功能:

- 通过使用“帐户策略”页面来设置站点的帐户策略，以定义与帐户相关的使用中的策略。关于详细信息，请参阅第 52 页的『设置帐户策略』。
- 使用“密码策略”页面来设置站点的密码策略以控制用户的密码选择特征（仅当对照 WebSphere Commerce 数据库来认证用户时）。关于详细信息，请参阅第 52 页的『设置密码策略』。
- 使用“帐户锁定策略”页面来设置站点的帐户锁定策略以减少危及用户帐户安全的机会（仅当对照 WebSphere Commerce 数据库来认证用户时）。关于详细信息，请参阅第 53 页的『设置帐户锁定策略』。
- 通过使用“启动安全性检查”页面，启动安全性程序，该程序检查并删除可能包含潜在的安全性隐患的临时 WebSphere Commerce 文件。关于详细信息，请参阅第 54 页的『启动安全性检查』。

关于相关概念的信息，请参阅 WebSphere Commerce 联机帮助中的以下主题:

- 配置管理器
- WebSphere Commerce 配置文件
- 管理控制台
- 安全性

关于相关任务的信息，请参阅 WebSphere Commerce 联机帮助中的以下主题。

- 启动配置管理器
- 打开管理控制台

关于 Internet Information Services（IIS）Web 服务器的安全性注意事项

注意事项

如果您在使用 WebSphere Commerce 的同时使用 IIS Web 服务器，那么就需要注意以下安全性注意事项，并采取建议措施以使 WebSphere Commerce 数据的任何安全隐患达到最小。

问题：对 IIS Web 服务器，对虚拟目录的读许可权提供了访问 JSP 文件源代码的权利。为了阻止下载 JSP 源代码，如果您正在使用 IIS Web 服务器，则必须在物理上将 Web 页面的静态内容和动态内容分开。这是因为 IIS 安全性是基于目录位置，而不是文件类型的。在缺省 IIS 配置下，图像文件和 JSP 文件位于单一别名的下面。只可在用于测试目的时才可使用缺省配置。

解决方案：保护所有的 Web 有用资源，*当静态内容要移到不同的只有读许可权的虚拟目录时，动态内容必须使用只有执行许可权（不可读）的虚拟目录来访问*。关于在虚拟目录上设置许可权的更多信息，请参阅 IIS 帮助信息中的指示信息。还建议您参考 Microsoft® Corporations 关于安全性补丁和配置策略的最新文档。

安全性视图

使用 WebSphere Commerce 的某些安全性功能之前，要求您在可使用该功能之前为商店定义关联的视图。以下信息描述如何定义下列视图:

- 登录超时（请参阅『登录超时』）
- 密码失效（请参阅第 45 页的『密码失效』）
- 受密码保护的命令（请参阅第 45 页的『受密码保护的命令』）
- 交叉站点脚本保护（请参阅第 46 页的『交叉站点脚本保护』）

关于创建视图和开发商店前台的一般信息，请参阅《*WebSphere Commerce 商店开发指南*》。

登录超时

要使用登录超时安全性功能，需要为商店定义 LoginTimeoutErrorView 和 ReLogonFormView 视图。

LoginTimeoutErrorView

如果登录超时信息不正确，则 WebSphere Commerce 会将用户的浏览器重定向到此视图。如果发生此情况，则可能是因为有人篡改了 cookie。

表 2. LoginTimeoutErrorView 属性

ECConstants.EC_LOGIN_TIMEOUT_ERROR_MSGCODE	
	1 失效时间设置为错误的值。
	2 登录时间设置为错误的值。
	3 失效或登录时间设置为错误的值。

ReLogonFormView

在用户会话失效后向用户显示此视图。它需要向用户提供表单以输入用户的登录标识和密码。提交按钮将调用 Logon 命令。还应有“取消”按钮将用户重定向到另一页面，在大多数情况下是商店前台页面。

ReLogonFormView 没有属性。

表 3. ReLogonFormView 表单属性

ECUserConstants.EC_UREG_LOGONID	用户登录标识。
ECUserConstants.EC_UREG_LOGONPASSWORD	用户登录密码。
ECUserConstants.EC_RELOGIN_URL	在提供的凭证无效的情况下显示的 URL。大多数情况下，是此视图的名称。
ECConstants.EC_STORE_ID	商店标识。
ECConstants.EC_URL	在所输入的凭证属于另一用户的情况下显示的 URL。大多数情况下，这应是商店主页，或是用在商店登录页面中的同一 URL。

密码失效

要使用密码失效安全性功能，需要为商店定义 ChangePassword 视图。

ChangePassword

在用户密码已失效的情况下显示此视图。它应向用户提供表单以输入当前（已失效的）密码和新密码。“提交”按钮调用 ResetPassword 命令。还应有“取消”按钮将用户重定向到另一页面，在大多数情况下是商店前台页面。

表 4. ChangePassword 属性

ECConstants.EC_PASSWORD_EXPIRED_FLAG	**1** 用户密码已失效。为了同用于密码更改功能的视图区分此视图（因为它们是相同的），需要此属性。用于密码更改的视图可由用户调用，而在这两种情况下指定给此视图的 JSP 应是一样的。为了确定显示哪个视图，JSP 应查找此属性。 **null** 属性不是位于 URL 上。这是正常的密码更改行为
ECUserConstants.EC_UREG_LOGONID	当前用户登录标识。
ECConstants.EC_LOGIN_RETURN_URL	在成功地更改了密码之后，将浏览器重定向至的 URL。此 URL 将被传递到名为 ECConstants.EC_URL 的操作命令。

表 5. ChangePassword 表单属性

ECUserConstants.EC_UREG_LOGONID	用户的登录标识。已将当前登录标识传递到视图中。
ECUserConstants.EC_UREG_LOGONPASSWORDOLD	旧密码。
ECUserConstants.EC_UREG_LOGONPASSWORD	新密码。
ECUserConstants.EC_UREG_LOGONPASSWORDVERIFY	新密码验证。
ECConstants.EC_URL	在成功地更改了密码之后，将用户重定向至的 URL。已将值传递到视图中。
ECUserConstants.EC_RELOGIN_URL	在密码更改不成功的情况下将浏览器重定向至的 URL。

受密码保护的命令

要使用“受密码保护的命令”安全性功能，需要为商店定义 PasswordReEnterErrorView 和 PasswordReEnterFormView 视图。

PasswordReEnterErrorView

此视图用于以下方案:

- 用户未能提供正确的密码且已注销。

- 认证已失败。

在两种情况下，用户都应当有办法通过当前页面上的链接继续到另一页面。

表 6. PasswordReEnterErrorView 属性

ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	**0** 当试图认证用户时发生问题。 **null** 属性不是位于 URL 上。用户未能提供密码且已注销。

PasswordReEnterFormView

在用户尝试执行受密码保护的命令时显示此视图。它应向用户提供表单以输入密码。应有两个输入字段以输入密码。

表 7. PasswordReEnterFormView 属性

ECConstants.EC_PASSWORD_REREQUEST_URL	使用表单的“提交”按钮运行此 URL。
ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	消息代码，它指定显示给用户的消息: **1** 输入的密码不匹配。 **2** 未输入密码。 **3** 输入了不正确的密码。

操作: 将此 URL 作为参数传递，参数名为:

表 8. PasswordReEnterFormView 表单属性

ECConstants.EC_PASSWORD_REREQUEST_PASSWORD1	第一个密码。
ECConstants.EC_PASSWORD_REREQUEST_PASSWORD2	第二个密码。

交叉站点脚本保护

要使用交叉站点脚本编制安全性功能，需要为商店定义 ProhibitedAttrsErrorView、ProhibitedCharacterErrorView 和 ProhibCharEncodingErrorView 视图。

ProhibitedAttrsErrorView

在由于请求包含禁止的属性而未处理请求的情况下向用户显示此视图。

ProhibitedCharacterErrorView

在由于请求包含禁止的字符而未处理请求的情况下向用户显示此视图

ProhibCharEncodingErrorView

它与上述的 ProhibitedCharacterErrorView 相同。

启用登录超时

注: 要为商店使用登录超时安全性功能，需要如第 44 页的『登录超时』所述为商店定义 LoginTimeoutErrorView 和 ReLogonFormView 视图。

使用配置管理器的“登录超时”节点来启用或禁用登录超时功能。当启用此功能时，将从系统中注销在延长时间段内处于非活动状态的 WebSphere Commerce 用户，并请求他重新登录。如果用户后来登录成功，则 WebSphere Commerce 运行该用户以前发出的原始请求。如果用户登录失败，则废弃原始请求，用户仍然处于从系统注销的状态。

请注意，对于 WebSphere Commerce 工具（例如管理控制台、WebSphere 贸易加速器等），登录超时不向用户显示重新登录页面。而是关闭浏览器窗口，由用户自己决定是否登录回工具。因此，在工具的情况下，不处理用户提交的原始请求。

要启用此功能:

1. 启动配置管理器并如下遍历到实例的“登录超时”节点: **WebSphere Commerce > *host_name* > 实例列表 > *instance_name* > 实例属性 > 登录超时**
2. 要激活登录超时功能，请单击**启用**复选框。
3. 在“值”字段输入登录超时值（秒数）。
4. 要将所作的更改应用到配置管理器，请单击**应用**。
5. 在成功更新实例配置之后，将接收到一条表明成功更新的消息。
6. 通过 WebSphere Application Server 管理控制台，先停止然后重新启动 WebSphere Commerce 服务器实例。

请注意登录超时值以毫秒为单位存储在 *instance*.xml 文件中，而配置管理器中的值是以秒为单位输入的。

启用密码失效

注: 要使用密码失效安全性功能，需要如第 45 页的『密码失效』所述为商店定义 ChangePassword 视图。

使用配置管理器的“密码失效”节点来启用或禁用密码失效功能。当启用密码失效时，如果用户的密码已过期，则要求 WebSphere Commerce 用户改变他们的密码。在此情况下，用户会被重定向到要求他们更改密码的页面。用户要能够访问站点上的任何安全页面，必须先更改他们的密码。要启用此功能:

1. 启动配置管理器并如下遍历到实例的“密码失效”节点: **WebSphere Commerce > *host_name* > 实例列表 > *instance_name* > 实例属性 > 密码失效**
2. 要激活密码失效功能，请单击**启用**复选框。
3. 要将所作的更改应用到配置管理器，请单击**应用**。
4. 在成功更新实例配置之后，将接收到一条表明成功更新的消息。
5. 通过 WebSphere Application Server 管理控制台，先停止然后重新启动 WebSphere Commerce 服务器实例。

启用受密码保护的命令

注: 要使用“受密码保护的命令”安全性功能，需要如第 45 页的『受密码保护的命令』所述为商店定义 PasswordReEnterErrorView 和 PasswordReEnterFormView 视图。

使用配置管理器的“受密码保护的命令”节点来启用或禁用“受密码保护的命令”功能。当启用此功能时，WebSphere Commerce 会在继续处理请求（该请求运行指定的 WebSphere Commerce 命令）之前，要求登录到 WebSphere Commerce 的注册用户输入其密码。

警告: 配置受密码保护的命令时，显示在命令选择列表中的一些命令可由一般用户或临时用户执行。将此类命令配置为受密码保护将限制一般用户和临时用户对这些命令的运行。因此，在将命令配置为受密码保护时，应当谨慎。

要启用此功能:

1. 启动配置管理器并如下遍历到实例的“受密码保护的命令”节点: **WebSphere Commerce > *host_name* > 实例列表 > *instance_name* > 实例属性 > 受密码保护的命令**
2. 在“常规”选项卡中:
   a. 要激活“受密码保护的命令”功能，请单击**启用**。
   b. 在“重试”字段中输入重试次数。(重试次数的缺省值是 3。)
3. 在“高级”选项卡中:
   a. 从“受密码保护的命令列表”窗口的列表中选择希望保护的 WebSphere Commerce 命令，并单击**添加**。所选择的命令会列在“当前受密码保护的列表”窗口中。
   b. 如果希望对任何 WebSphere Commerce 命令禁用密码保护，请在“当前受密码保护的命令列表”窗口中选择该命令，并单击**除去**。
4. 要将所作的更改应用到配置管理器，请单击**应用**。
5. 在成功更新实例配置之后，将接收到一条表明成功更新的消息。
6. 通过 WebSphere Application Server 管理控制台，先停止然后重新启动 WebSphere Commerce 服务器实例。

注: WebSphere Commerce 在可用命令列表中将仅显示在 `URLREG` 表中指定为已认证或设置了 `https` 标志的命令。

更新加密数据

使用配置管理器的“数据库”节点所提供的“数据库更新工具”，在给定实例的一个或多个 WebSphere Commerce 数据库中更改商家密钥并更新所有加密的数据(如密码或信用卡号)。要使用该工具:

1. 启动配置管理器并如下遍历到指定的数据库条目: **WebSphere Commerce > *host_name* > 实例列表 > *instance_name* > 实例属性 > 数据库 > *database_name***
2. 用鼠标右键单击 *database_name* 并选择**运行数据库更新工具**
   - 选择**更新此实例的所有数据库**来迁移选定实例的所有数据库的加密数据。

     400 因为 iSeries 支持单数据库配置，因此这个选项不适用于 iSeries。
   - 通过从下拉列表中选择数据库，并选择**更新选定的数据库**，来迁移特定数据库的加密数据(缺省值)。
3. 从“操作项”框中选择希望运行的操作，并在“参数”字段中填入必需的信息:

操作	参数	必需的操作

更改商家密钥	旧的商家密钥	输入在创建当前 WebSphere Commerce 实例时使用的现有商家密钥。
	新的商家密钥	输入新的商家密钥。这是 16 位十六进制数字，以供配置管理器重新加密当前已加密数据。商家密钥至少必须有一个字母数字字符（a 到 f）和一个数字字符（0 到 9）。任何字母数字字符都必须以小写字母形式输入，同一字符在同一行中不能输入四次以上。

4. 单击**确定**对选定的 WebSphere Commerce 数据库或对所有 WebSphere Commerce 数据库运行数据库更新工具。
5. 在成功更新实例配置之后，将接收到一条表明成功更新的消息。
6. 通过 WebSphere Application Server 管理控制台，先停止然后重新启动 WebSphere Commerce 服务器实例。

启用交叉站点脚本保护

注: 要为商店使用交叉站点脚本安全性功能，需要如第 46 页的『交叉站点脚本保护』所述为商店定义 `ProhibitedAttrsErrorView`、`ProhibitedCharacterErrorView` 和 `ProhibCharEncodingErrorView` 视图。

使用配置管理器的“交叉站点脚本保护”节点来启用或禁用实例的交叉站点脚本保护。 当启用时，交叉站点脚本保护拒绝任何包含指定为不允许的属性或字符串的用户请求。可以在配置管理器的此节点中指定禁止的属性或字符串。也可通过允许特定命令的指定属性值包含禁止的字符串，从交叉站点脚本保护中排除该命令。缺省情况下，交叉站点脚本保护是禁用的。

警告: 交叉站点脚本保护是限制性功能，因为它将限制基于配置的命令的执行。 该功能不检查什么属性或字符串已定义为禁止，因此当您配置它时，请确保禁止的属性不是由命令使用的那些属性。还请确保禁止的字符串不是通常传递给命令的那些值。配置此功能时请格外谨慎。

要启用此功能:

1. 启动配置管理器并如下遍历到实例的“交叉站点脚本保护”节点: **WebSphere Commerce > *host_name* > 实例列表 > *instance_name* > 实例属性 > 交叉站点脚本保护**
2. 使用“常规”选项卡激活“交叉站点脚本保护”功能，如下所示:
   a. 单击**启用**。
   b. 要添加希望对 WebSphere Commerce 命令禁止的属性，请用鼠标右键单击“禁止的属性”表并选择**添加行**。输入希望禁止的属性。每行仅可指定一个属性。
   c. 要从“禁止的属性”表中除去属性，请在表中突出显示并用鼠标右键单击包含该属性的行，并选择**删除行**。
   d. 要添加希望对 WebSphere Commerce 命令禁止的字符串，请用鼠标右键单击“禁止的字符”表并选择**添加行**。添加希望禁止的字符串。每行仅可指定一个字符串。
   e. 要从“禁止的字符”表中除去字符，请在“禁止的字符”表中突出显示并用鼠标右键单击包含该字符的行，并选择**删除行**。

注意: 缺省情况下在“禁止的字符”字段中指定了以下字符串。这些字符串在恶意的交叉站点脚本编制攻击中最常用作脚本编制标记:

- `<SCRIPT`
- `<SCRIPT`
- `<%` 和 `<%`

.

3. 如下通过让特定命令的指定属性的值包含禁止的字符串，来使用“高级”选项卡从交叉站点脚本保护中排除该 WebSphere Commerce 命令:
   a. 从“命令列表”框中选择命令。
   b. 输入用逗号分隔的一列属性（在“排除属性的列表”窗口中，禁止的字符对这些属性是允许的）并单击**添加**。
   c. 要连同属性一起除去一个命令，请从“排除命令的列表”窗口中选择该命令并单击**除去**。

   还可以通过选择属性并单击**除去**，来除去命令的特定属性。
4. 要将所作的更改应用到配置管理器，请单击**应用**。
5. 在成功更新实例配置之后，将接收到一条表明成功更新的消息。
6. 通过 WebSphere Application Server 管理控制台，先停止然后重新启动 WebSphere Commerce 服务器实例。

注:

1. 当命令从交叉站点脚本保护中排除时，将使用 HTML 符号编码对指定属性的值进行编码。例如，命令 `cmd1?user=<Thomas>` 编码为 `ascmd1?user=&#60;Thomas&#62;`
2. 当在“禁止的字符”字段中指定字符串时，请注意:
   - 某一字符序列如果遵循 URL 编码标准，则可引起该字符串转换为单个字符。例如，字符串 `<%bb` 将转换为字符串 `<X`，其中 *X* 是十六进制表示值为 HEX ’bb’（十进制 187）的单个字符。在此情况下，如果字符串 `<%bb` 在 URL 中传递，交叉站点脚本保护将不会捕获该字符串。
   - 某一字符序列如果不遵循 URL 编码标准，则可引起字符串转换失败。例如，字符串 `<%gg` 将引起转换失败，因为 HEX ’gg’ 不是有效的十六进制值表示。在此情况下，字符串 `<%gg` 将引起异常，导致无论启用交叉站点脚本保护与否，对包含此字符串的 URL 请求没有相应。

示例: 请考虑以下示例:

- 禁止的字符串: `<SCRIPT`、`<%`

  禁止的属性: `mycomment`、`description`

命令	状态
cmd1?description=Available...	拒绝
cmd2?userid=Thomas...	接受
cmd3?mycomment=<SCRIPT>...	拒绝
cmd4?password=<%...%>...	拒绝

- 如果希望允许 `cmd1` 命令的属性 `text` 包含禁止的字符串（`<SCRIPT`、`<%`），而对其它属性（如属性 `txt`）则不允许，那么可以排除 `cmd1` 并将 `text` 指定为例外的属性。

命令	状态
cmd1?text=<SCRIPT>...	接受
cmd1?text=<%...%>...	接受
cmd1?txt=<SCRIPT>...	拒绝
cmd1?txt=<%..%>...	拒绝

启用访问记录

当启用时，访问日志记录功能记录到 WebSphere Commerce 服务器的所有进入请求，或者仅记录导致访问冲突的请求。访问冲突的示例是：认证失败、执行命令的权限不够，或者重新设置违反了站点密码规则的密码。启用时，访问日志记录使 WebSphere Commerce 管理员能够快速地识别出对 WebSphere Commerce 系统的安全性威胁。

当发生认证失败或授权失败事件时，将以下信息记录到访问日志文件数据库表 ACCLOGMAIN 和 ACCLOGSUB 中：

- 客户机主机名
- 运行命令的线程标识
- 客户机用户标识
- 事件发生时间
- 运行的命令
- 为其运行命令的商店
- 对其执行操作的资源
- 访问控制检查的结果

要启用访问记录，请执行以下操作：

1. 启动配置管理器
2. 选择 **主机名** > **实例** > **Instance_List**，然后打开**组件**文件夹。
3. 选择 **AccessLoggingEventListener**。
4. 在“常规”面板中，激活**启用组件**复选框。
5. 选择“高级”面板并启用**启动**。
6. 单击**应用**。
7. 退出配置管理器。
8. 重新启动 WebSphere Application Server。

要更改日志文件的大小，或指定是否记录所有请求，需要手工编辑位于 WebSphere Commerce 实例子目录中的 WebSphere Commerce 实例的 *instance*.xml 文件：

1. 在编辑器中打开实例的 *instance*.xml 文件。
2. 定位以下节点，该节点位于 <LogSystem>/<activitylog> 节点中：

   ```
   <accessLogging cacheSize="aa" logAllRequests="bbbbb" />
   ```

   其中：

   - *aa* 是整数值，指定将条目写入数据库前将记录到内存中的条目的最大数目。通常较大的数值将导致对于访问记录的性能改进。缺省值是 32。

- *bbbbb* 是 true 或 false。值为 true 即指记录所有进入请求。值为 false 即指仅记录访问冲突。要防止过多的或不必要的记录，建议使用 false 值。仅当怀疑站点存在认证问题或安全性违例时才使用 true。缺省值是 false。

3. 当完成更新时，保存 WebSphere Commerce 实例的 *instance*.xml 文件。
4. 重新启动 WebSphere Application Server。

在以下示例中，访问记录在向数据库表记录条目之前，在内存中保存 3 个条目。并且，它记录到 WebSphere Commerce 服务器的所有进入请求:

```
<accessLogging cacheSize="3" logAllRequests="true" />
```

设置帐户策略

WebSphere Commerce 管理控制台的“帐户策略”页面允许您设置帐户策略。此页面列出了所有现有的帐户策略，包括缺省情况下随 WebSphere Commerce 提供的任何预订义的帐户策略。帐户策略定义与帐户相关的策略，例如密码和帐户锁定策略。在此页面上:

- 可通过单击**新建**创建新的帐户策略。
- 可以通过在列表中选择策略并单击**更改**来更改现有的帐户策略特征。
- 可以通过在列表中选择策略并单击**删除**来删除现有账户策略。

要创建新的帐户策略:

1. 打开 WebSphere Commerce 管理控制台。
2. 从管理控制台的“安全性”下拉菜单中，单击**帐户策略**。
3. 在帐户策略页面上，单击**新建**来创建新的帐户策略。
4. 在“名称”字段中输入帐户策略名称（例如 my_account_policy）。
5. 从“密码策略”菜单中，选择预先存在的密码策略。
6. 从“帐户锁定策略”菜单中，选择预先存在的帐户锁定策略。
7. 单击**确定**。

一旦创建了帐户策略，则可将策略指定给用户。请注意如果帐户策略在使用中（即已将账户策略指定给用户）的情况下不能删除帐户策略。

关于附加信息，请参阅第 55 页的『缺省的认证策略』。

设置密码策略

WebSphere Commerce 管理控制台的“密码策略”页面让您能够控制用户的密码选择以便定义密码的特征，来确保密码符合站点的安全性策略。此页面列出了所有现有的密码策略，包括缺省情况下随 WebSphere Commerce 提供的任何预订义的密码策略。

密码策略定义密码必须遵循的属性。密码策略强制实施以下条件:

- 用户标识和密码是否能够匹配。
- 连续字符的最大出现次数。
- 任意字符的最多出现次数。
- 密码的最大使用寿命。
- 字母字符的最小数目。

- 数字字符的最小数目。
- 密码的最小长度。
- 是否可重新使用用户先前的密码。
- 可以通过单击**新建**创建新的密码策略。
- 可以通过在列表中选择策略并单击**更改**来更改现有的密码策略特征。
- 可通过在列表中选择密码策略并单击**删除**来删除现有策略。

要创建新的密码策略:

1. 打开 WebSphere Commerce 管理控制台。
2. 从管理控制台的“安全性”下拉菜单中，单击**密码策略**。
3. 在帐户策略页面上，单击**新建**来创建新的密码策略。
4. 在“名称”字段中输入密码策略名称（例如 `my_password_policy`）。
5. 按需要更新以下内容以修改购物者缺省值中的任意值:
   - **用户标识和密码能否匹配?** 定义用户标识和密码是否能够完全一样。从列表中选择是或否。
   - **最大连续字符输入次数**。定义密码中连续字符的最大出现次数。最小值是 2 个连续字符。例如，如果值为 2，则用户无法输入诸如 `aaabc` 的密码。
   - **任意字符的最多出现次数。**定义密码中同一字符可出现的最多次数。最小值是字符出现 1 次。例如，如果值为 2，则用户无法输入诸如 `abcaabc` 的密码。
   - **密码的最大使用寿命。**定义密码可存在的最大时间（以天为单位）。最小值是 1 天。在此时间段之后，将提示用户更改密码。
   - **字母字符的最小数目**。定义密码中需要存在的字母字符的最小数目。最小值是 0 个字母字符。
   - **数字字符的最小数目**。定义密码中需要存在的数字字符的最小数目。最小值是 0 个数字字符。
   - **密码的最小长度**。以字符为单位定义密码的最小长度。最小值是 1 个字符。
   - **是否可重新使用密码?** 定义是否可重新使用用户先前的密码。从列表中选择是或否。
6. 单击**确定**。

注:

1. 在密码策略正在使用中（即已将密码策略指定给用户）的情况下不能删除密码策略。
2. 仅当对照 WebSphere Commerce 数据库认证用户时才强制实施密码策略。

关于附加信息，请参阅第 55 页的『缺省的认证策略』。

设置帐户锁定策略

WebSphere Commerce 管理控制台的“帐户锁定策略”页面允许您为 WebSphere Commerce 内的不同用户角色设置帐户锁定策略。此页面列出了所有现有的帐户锁定策略，包括缺省情况下随 WebSphere Commerce 提供的任何预订义的帐户锁定策略。帐户锁定策略在对帐户启动了恶意操作的情况下将禁用该用户帐户，以便减少操作危及帐户安全的机会。

帐户锁定策略强制实施以下项:

- 帐户锁定阈值。这是禁用帐户前无效登录尝试的数目。
- 连续失败登录延迟。这是在两次尝试登录失败之后，不允许用户登录的时间段。对每个连续的登录失败，按配置的时间延迟值（例如 10 秒）来增加延迟。

要设置帐户锁定策略:

1. 打开 WebSphere Commerce 管理控制台。
2. 从管理控制台的“安全性”下拉菜单中，单击**帐户锁定策略**。
3. “帐户锁定策略”页面列出了所有现有的帐户锁定策略。在此页面上:
   - 可通过单击**新建**创建新策略。
   - 可通过在列表中选择策略并单击**更改**来更改现有策略的特征。
   - 可通过在列表中选择策略并单击**删除**来删除现有策略。

对于新建的帐户锁定策略，在“帐户锁定策略”页面中:

1. 在“名称”字段中输入帐户锁定策略名称（例如 `my_policy`）。
2. 在“帐户锁定阈值”字段中输入帐户锁定阈值。例如，输入 6（即 6 次尝试）
3. 在“等待时间”字段中以秒为单位输入连续失败登录延迟。例如输入 10（即 10 秒）。
4. 单击**确定**。

注:

1. 请注意如果帐户锁定策略在使用中（即已将账户策略指定给用户）的情况下不能删除帐户锁定策略。
2. 仅当对照 WebSphere Commerce 数据库认证用户时才强制实施帐户锁定策略。

启动安全性检查

400 此功能不适用于 WebSphere Commerce for iSeries。

WebSphere Commerce 管理控制台的“启动安全性检查”页面允许您手工地启动安全性程序，该程序检查并删除可能包含潜在的安全性隐患的临时 WebSphere Commerce 文件。通常安全性程序作为已调度作业运行，且在缺省情况下设置为每月运行一次。

要调用安全性检查程序:

1. 打开 WebSphere Commerce 管理控制台。
2. 从管理控制台的“安全性”下拉菜单中，单击**安全性检查程序**。
3. 在“启动安全性检查”页面上，单击**启动**。

安全性检查的结果，包括程序采取的所有操作，都写入“安全性检查日志”窗口以及位于 `logs` 子目录的 `sec_check.log` 文件中:

AIX Linux Solaris `WC_installdir/instances/instance_name/logs`

Windows `WC_installdir\instances\instance_name\logs`

Windows 在非 Windows 平台上，由 WebSphere Commerce 自动设置文件许可权，以使未授权用户不能访问敏感文件。在 Windows 平台上，需要如下手工设置许可权。此过程确保只有管理员组才对敏感文件具有读 / 写 / 执行权利:

1. 在 Windows 资源管理器中，用鼠标右键单击 *drive*:\WebSphere 文件夹。
2. 单击**属性**和**安全性**。缺省情况下 “Everyone” 组对此文件夹具有**所有**许可权。
3. 单击**添加**。
4. 显示一个窗口（选择用户、计算机...）。在此窗口中，选择 **Administrators** 组。

   注: 此处可能有一些意思含糊，因为您可能看到 Administrator 作为一个用户出现，但是您需要添加 Administrator 组，而不是 Administrator 用户。

   单击**添加**然后单击**确定**。
5. 在 “安全性” 选项卡中，已添加了 Administrators 组。需要除去 “Everyone”。选择 **Everyone**，且不选择显示 “允许可继承的许可权....” 方框
6. 在显示的 “安全性” 窗口中单击**除去**。

配置管理器 PDI 加密字段

配置 WebSphere Commerce 实例时，建议您选择 “PDI 加密” 复选框。启用 “PDI 加密” 字段则指定应当对 ORDPAYINFO 和 ORDPAYMTHD 表中的信息进行加密。通过选择该复选框，支付信息以加密格式存储在 WebSphere Commerce 数据库中。

缺省的认证策略

WebSphere Commerce 提供了两个缺省的认证策略:

- 『购物者』
- 第 56 页的『管理员』

购物者

购物者的缺省帐户策略包含购物者的缺省帐户锁定策略和缺省密码策略。

购物者的缺省帐户锁定策略包含以下缺省属性:

属性	缺省值
帐户锁定阈值	6 次尝试
连续失败登录延迟	10 秒

购物者的缺省密码策略包含以下缺省属性:

属性	缺省值
用户标识和密码是否能够匹配	N（不，它们不匹配）
连续字符的最大出现次数	3 个字符
任意字符的最多实例数	4 个实例
密码的最大使用寿命	180 天
字母字符的最小数目	1 个字母字符
数字字符的最小数目	1 个数字字符

属性	缺省值
密码的最小长度	6 个字符
是否可重新使用用户先前的密码	N（不，不可以重新使用它）

向执行自注册的购物者分配了缺省的购物者认证策略 — 购物者。

管理员

管理员的缺省帐户策略包含管理员的缺省帐户锁定策略和缺省密码策略。

管理员的缺省帐户锁定策略包含以下缺省属性:

属性	缺省值
帐户锁定阈值	3 次尝试
连续失败登录延迟	20 秒

购物者的缺省密码策略包含以下缺省属性:

属性	缺省值
用户标识和密码是否能够匹配	N（不，它们不匹配）
连续字符的最大出现次数	3 个字符
任意字符的最多实例数	4 个实例
密码的最大使用寿命	90 天
字母字符的最小数目	1 个字母字符
数字字符的最小数目	1 个数字字符
密码的最小长度	8 个字符
是否可重新使用用户先前的密码	N（不，不可以重新使用它）

向随 WebSphere Commerce 提供的缺省 `wcsadmin` 管理员用户分配了缺省的认证策略 — 管理员。

第 5 章 会话管理

Web 浏览器和电子交易站点使用 HTTP 进行通信。因为 HTTP 是无状态协议（意即每个命令均独立执行而无需知道此前发生的任何命令），因此必须要有一种方法可以管理浏览器端和服务器端之间的会话。

WebSphere Commerce 支持两种类型的会话管理: 基于 cookie 以及 URL 重写。管理员可以选择仅支持基于 cookie 的会话管理，或者选择同时支持基于 cookie 和 URL 重写的会话管理。如果 WebSphere Commerce 仅支持基于 cookie，则购物者的浏览器必须能够接受 cookie。如果同时选择了基于 cookie 和 URL 重写，则 WebSphere Commerce 将先尝试使用 cookie 管理会话；如果购物者的浏览器设置为不接受 cookie，则使用 URL 重写。

基于 cookie 的会话管理

当使用基于 cookie 的会话管理时，Web 服务器将包含用户信息的消息（cookie）发送到浏览器。当用户尝试访问某些页面时，将此 cookie 发送回服务器。通过将 cookie 发送回来，服务器能够标识用户以及从会话数据库中检索用户会话，进而维护用户会话。基于 cookie 的会话在用户注销或关闭浏览器时结束。基于 cookie 的会话管理是安全的且具有性能上的优点。基于 cookie 的会话管理是安全的，因为它使用仅通过 SSL 流动的标识标记。基于 cookie 的会话管理提供了显著的性能益处，因为 WebSphere Commerce 高速缓存机制仅支持基于 cookie 的会话（而不支持 URL 重写）。对于购物者会话，建议使用基于 cookie 的会话管理。

如果不在使用 URL 重写，且希望确保用户在他们的浏览器上启用了 cookie，请在配置管理器的“会话管理”页面上选中 **Cookie 接受测试**。这会通知购物者，如果他们的浏览器不支持 cookie，或者如果他们关闭了 cookie，那么他们将需要支持 cookie 的浏览器来浏览 WebSphere Commerce 站点。

出于安全性原因，基于 cookie 的会话管理使用两种类型的 cookie:

- 非安全会话 cookie

  用于管理会话数据。包含了构造 cookie 时的会话标识、协商语言、当前商店和购物者首选货币。此 cookie 可在 SSL 或非 SSL 连接下在浏览器和服务器之间流动。有两种类型的非安全会话 cookie:

  – WebSphere Application Server 会话 cookie 是基于 servlet HTTP 会话标准的。WebSphere Application Server cookie 在多节点部署中保存到内存或数据库中。关于更多信息，请在 WebSphere Application Server 信息中心（`http://www.ibm.com/software/webservers/appserv/infocenter.html`）中搜索“session management”。

  – WebSphere Commerce 会话 cookie 对于 WebSphere Commerce 是内部的，并且不保存到数据库。

  要选择使用何种类型的 cookie，请在配置管理器的“会话管理”页面上选择 `WCS` 或 `WAS` 作为 **Cookie 会话管理器**参数。

- 安全认证 cookie

用于管理认证数据。认证 cookie 通过 SSL 流动，且打上了时间戳记以达到最大安全性。此 cookie 用于每当执行敏感命令（例如请求用户信用卡号码的 DoPaymentCmd）时认证用户。此 cookie 可能由未授权用户盗用的风险已极小化。每当基于 cookie 的会话管理正在使用中时，始终由 WebSphere Commerce 生成认证代码 cookie。

要查看安全页面，需要会话和认证代码 cookie 两者。

对于 cookie 错误，在以下情况下调用 CookieErrorView:

- 用户从另一位置使用同一登录标识登录。
- cookie 已被破坏和 / 或被篡改。
- 如果将 cookie 接受设置为 “true” 而用户的浏览器不支持 cookie。

将 cookie 用于会话管理

要在 WebSphere Commerce 中使用 cookie，请执行以下操作:

1. 打开配置管理器。
2. 选择**实例**，然后打开**会话管理**文件夹。
3. 选择适当的会话值。
   - Cookie 接受测试

     选择此复选框来检查对于仅支持 cookie 的站点，客户的浏览器是否接受 cookie。
   - Cookie 会话管理器

     选择希望是 WebSphere Commerce 还是 WebSphere Application Server 来管理 cookie。缺省值是 WebSphere Commerce。
     - WebSphere Application Server 会话 cookie 是基于 servlet HTTP 会话标准的。WebSphere Application Server cookie 在多节点部署中保存到内存或数据库中。关于更多信息。请在 WebSphere Application Server 信息中心（http://www.ibm.com/software/webservers/appserv/infocenter.html）中搜索 “session management”。
     - WebSphere Commerce 会话 cookie 对于 WebSphere Commerce 是内部的，且不保存到数据库中。
4. 单击**高级**选项卡。选择适当的会话值。
   - Cookie 路径

     指定 cookie 的路径，它是 cookie 应被发送到的 URL 的子集。通常不能更改此字段。

     关于 cookie 路径的详细信息，请参阅 Netscape 的 Cookie 规范和 RFC 2109。
   - Cookie 域

     指定一个域限制模式。通常不能更改此字段。

     此域指定应该查看 cookie 的服务器。缺省情况下，仅将 cookie 发送回发出这些 cookie 的 WebSphere Commerce Server。缺省情况下，仅将 cookie 返回到保存这些 cookie 的主机。指定域名模式将覆盖此缺省值。模式必须以点开始，且必须包含至少两个点。模式仅与超出起始点一个输入的内容相匹配。例如，“.ibm.com” 是有效的，并且与 “a.ibm.com” 和 “b.ibm.com” 匹配，但不与 “www.a.ibm.com” 匹配。关于域模式的详细信息，请参阅 Netscape 的 Cookie Specification 和 RFC 2109。
5. 单击**应用**。

6. 关闭配置管理器。
7. 通过 WebSphere Application Server 管理控制台，先停止然后重新启动 WebSphere Commerce 服务器实例。

URL 重写

使用 URL 重写时，在返回到浏览器或者获得重定向的所有链接后附加了会话标识。当用户单击这些链接时，将重写格式的 URL 作为客户机请求的一部分发送到服务器。servlet 引擎识别 URL 中的会话标识，并保存它用于为该用户获取正确的对象。要使用 URL 重写，不能将 HTML 文件（具有 .html 或 .htm 扩展名的文件）用于链接。要使用 URL 重写，必须将 JSP 文件用于显示目的。使用 URL 重写的会话在购物者注销时失效。

注: WebSphere Commerce 动态高速缓存与 URL 重写无法互操作。当 URL 重写打开时，您需要禁用 WebSphere Commerce 动态高速缓存。关于更多信息，请参阅《*WebSphere Commerce 管理指南*》中关于动态高速缓存的章节。

使用 URL 重写会话管理

要指定应如何管理会话，请执行以下操作:

1. 打开配置管理器。
2. 选择**实例**，然后打开**会话管理**文件夹。
3. 选择适当的会话值。

   启用 URL 重写。选择此复选框以使用 URL 重写进行会话管理。

   Cookie 会话管理器。选择 WebSphere Application Server。
4. 单击**应用**。
5. 关闭配置管理器。
6. 通过 WebSphere Application Server 管理控制台，先停止然后重新启动 WebSphere Commerce 服务器实例。

为 URL 重写编写 JSP 模板

如果希望使用 URL 重写维护会话状态，请不要在纯 HTML 文件中包含至 Web 应用程序各部分的链接。此限制是必要的，因为在纯 HTML 文件中不能使用 URL 编码。要使用 URL 重写维护状态，会话期间用户请求的每个页面必须具有 Java 解释器可理解的代码。如果在 Web 应用程序和站点的一部分中具有用户可能在会话期间访问的此类纯 HTML 文件，请将它们转换为 JSP 文件。这将影响到应用程序编写者，因为与使用 cookie 维护会话不同，使用 URL 重写维护会话要求应用程序中的每个 JSP 模板必须对 <A> 标记上的每个 HREF 属性使用 URL 编码。如果应用程序中的一个或多个 JSP 模板不调用 encodeURL(String url) 或 encode RedirectURL(String url) 方法，则将丢失会话。

编写链接

使用 URL 重写时，在返回到浏览器或者重定向的所有链接后附加了会话标识。例如，在 Web 页面中此链接:

```
<a href="store/catalog">
```

重写为

```
<a href="store/catalog;$jsessionid$DA32242SSGE2">
```

当用户单击此链接时，将重写格式的 URL 作为客户机请求的一部分发送到服务器。servlet 引擎将 `;$jsessionid$DA32242SSGE2` 识别为会话标识，并保存它用于为该用户获取正确的 `HttpSession` 对象。

以下示例显示了 Java 代码可以如何嵌入到 JSP 文件中:

```
<%
 response.encodeURL ("/store/catalog");
%>
```

要重写返回到浏览器的 URL，请在将 URL 发送到输出流之前，调用 JSP 模板中的 `encodeURL()` 方法。例如，如果不使用 URL 重写的 JSP 模板具有:

```
out.println("<a href=\"/store/catalog\">catalog</a>")"
```

请将之替换为:

```
out.println("<a href=\"");
out.println(response.encodeURL ("/store/catalog"));
out.println("\">catalog</a>");
```

要重写重定向的 URL，请调用 `encodeRedirctURL()` 方法。例如，如果 JSP 模板具有:

```
response.sendRedirect (response.encodeRedirectURL ("http://myhost/store/catalog"));
```

则 `encodeURL()` 和 `encodeRedirectURL()` 方法是 `HttpServletResponse` 对象的一部分。在这两种情况下，这些调用在对 URL 进行编码前将检查是否配置了 URL 重写。如果未配置，则它返回原始 URL。

编写表单: 要编写用于提交的表单，请对表单模板的 `ACTION` 标记调用 `response.encodeURL("Logon");`。例如:

```
String strLoginPost = response.encodeURL("Logon");
<FORM NAME="Logon" METHOD="post" ACTION= <%= strLoginPost %> >
...
</FORM>
```

编写首页: 进入页面（通常是主页）不能包含框架。如果希望在商店中使用框架，可以将无框架页面（具有至商店的链接）作为商店的进入页面。然而，如果商店确实使用框架且客户尝试不先经过进入页面就访问这些带框架的页面，则他们的会话将丢失。如果客户使用**上一页**按钮（仅在具有框架的情况下）返回到进入页面并刷新进入页面，则也可丢失其会话。刷新进入页面将给予他们新的会话标识。作为**上一页**按钮的替代，一个回到进入页面的链接是必需的，以帮助防止此类会话丢失。

商店级别的会话管理

下图展示了 WebSphere Commerce 商店级别的注册基础结构。商店级别的注册使用访问控制角色将购物者与商店关联。

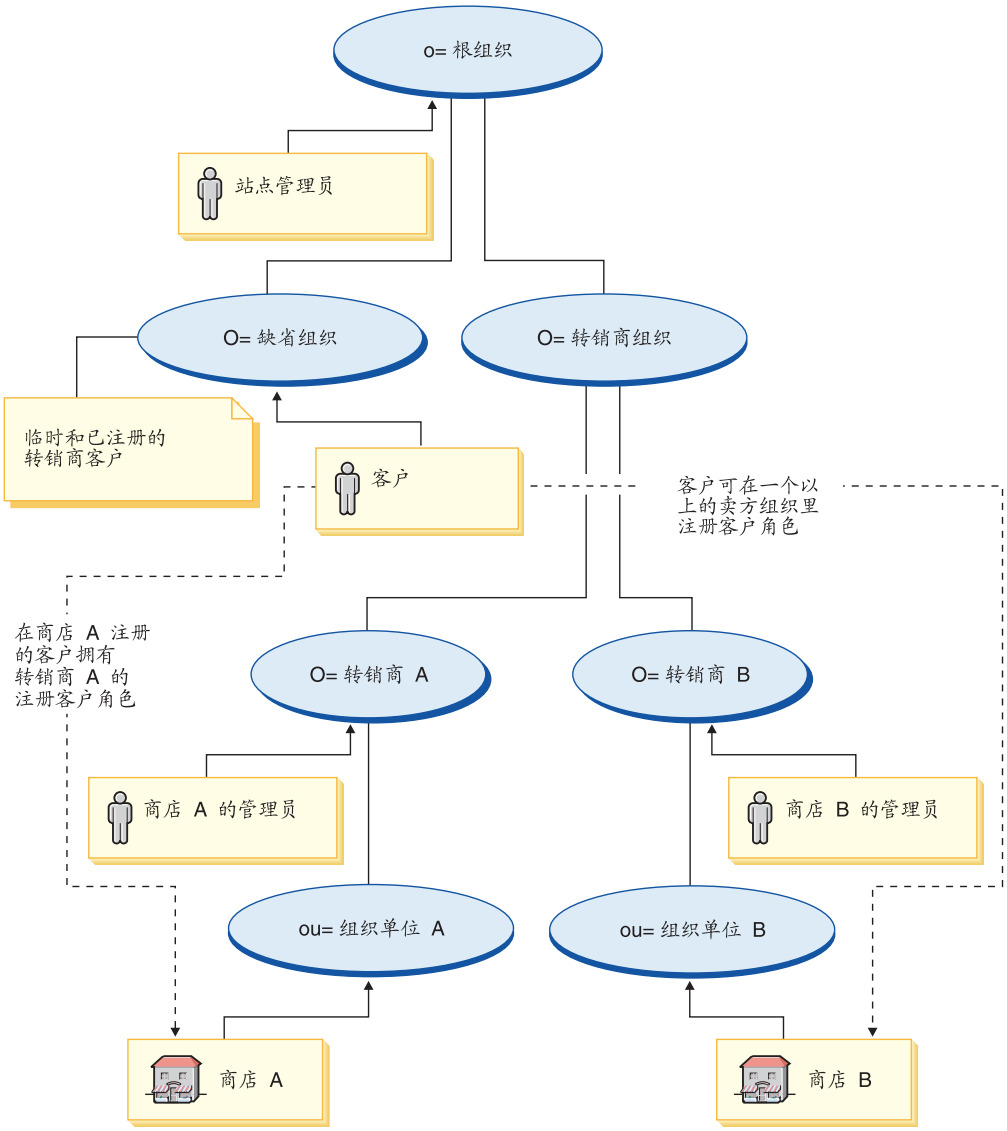


图 3. 商店级别的注册

在商店购物的用户不必是该商店组织的成员，但需要在组织中扮演购物角色（即注册客户）。组织中扮演管理角色的用户通常是通过与组织有上级关系与该组织相关联。

例如，假设您有一家商店，如上图中的商店 A。还假设 Sue 在商店 A 购物，Joe 是商店 A 的雇员，他负责运营的商店 A 的管理事务。要从组织的观点对此方案进行建模，Joe 应置于商店 A 的组织之下，而 Sue 则不应该。由于 Sue 不是商店 A 的雇员，所以 Sue 是通过使她自己在商店 A 组织中扮演购物角色来与商店 A 相关联的。

商店通过查找在商店的组织中扮演购物角色的所有用户确定其所有注册购物者。然后商店的用户管理员可以继续执行商店范围内的活动（如为商店中的所有注册用户设置竞销），或者执行特定的操作（如重新设置注册到其商店的用户的密码）。

请参阅图 3中的图，考虑以下方案:

- Sue 是缺省组织的成员，在转销商 A 的组织中具有购物角色。转销商 A 的父组织是转销商组织。
- 转销商 A 拥有商店 A

- Sue 不具有在转销商 B 的组织中的组织角色
- 转销商 B 拥有商店 B

Sue 登录到商店 A 并同往常一样购物。当 Sue 访问商店 B 时，Sue 作为临时用户被指定一个商店 B 的新的会话身份。如果她再次访问商店 A，则 WebSphere Commerce 使用她先前的商店 A 会话身份中的信息来管理她的会话。

在以下条件下，会对商店 B 重新使用商店 A 的会话身份:

- 商店 A 和商店 B 属于同一个组织。
- Sue 具有一个同时定义在转销商 A 和转销商 B 组织中的角色。

第 6 章 设置和更改密码

WebSphere Commerce 中的大多数组件利用经过操作系统验证的用户标识和密码。关于更改这些密码的信息，请参阅操作系统文档。本章涉及如何设置和更改 WebSphere Commerce 组件的密码，这些组件不通过操作系统验证用户标识和密码。

用户标识、密码和 Web 地址快速参考

在 WebSphere Commerce 环境中，执行管理操作需要一组不同的用户标识。以下列表描述了这些用户标识以及它们必须具备的权限。对于 WebSphere Commerce 用户标识，还标识了缺省密码。

400 **iSeries 用户概要文件**

在安装和配置 WebSphere Commerce 时经常使用和提及两个 iSeries 用户概要文件:

- 您创建的用于安装 WebSphere Commerce 和启动配置管理器的用户概要文件。要安装和配置 WebSphere Commerce，必须使用 USRCLS(*SECOFR) 的 iSeries 用户概要文件或使用 QSECOFR 用户概要文件。如果需要创建用户概要文件，请参阅 iSeries 版的*《WebSphere Commerce 安装指南》*。
- 在创建 WebSphere Commerce 实例时由配置管理器创建的用户概要文件。此用户概要文件也称为*实例用户概要文件*。USRCLS(*USER) 用户概要文件是在每次创建 WebSphere Commerce 实例时由配置管理器创建的。如果需要创建用户概要文件，请参阅 iSeries 版的*《WebSphere Commerce 安装指南》*。

配置管理器用户标识

配置管理器工具的图形界面使您能够修改 WebSphere Commerce 的配置方式。缺省的配置管理器用户标识和密码是 webadmin 和 webibm。

AIX Linux Solaris Windows 可从 WebSphere Commerce 机器或者与 WebSphere Commerce 在同一网络上的任何机器访问配置管理器。

400 对于 iSeries，可从与 iSeries 服务器在同一网络上的任何 Windows 机器访问配置管理器。

IBM HTTP Server 用户标识

AIX Linux Solaris Windows 如果正在使用 IBM HTTP Server，可通过打开 Web 浏览器并输入以下 Web 地址来访问 Web 服务器主页:

```
http://host_name
```

如果已经定制过 Web 服务器，则可能需要在主机名后面输入 Web 服务器首页的名称。

WebSphere Commerce 实例管理员

实例管理员用户标识和密码适用于以下 WebSphere Commerce 工具:

- WebSphere 贸易加速器. 要从运行 Windows 操作系统的远程机器访问 WebSphere 贸易加速器，请打开 Internet Explorer Web 浏览器，并输入以下 Web 地址:

https://*host_name*:8000/accelerator

- WebSphere Commerce 管理控制台. 要从运行 Windows 操作系统的远程机器访问 WebSphere Commerce 管理控制台，请打开 Internet Explorer Web 浏览器，并输入以下 Web 地址:

  https://*host_name*:8002/adminconsole

- WebSphere Commerce 组织管理控制台. 要从运行 Windows 操作系统的远程机器访问 WebSphere Commerce 组织管理控制台，请打开 Internet Explorer Web 浏览器，并输入以下 Web 地址:

  https://*host_name*:8004/orgadminconsole

对于以上工具，请输入您在创建 WebSphere Commerce 实例时输入的管理员用户标识和密码。

注: 切勿除去站点管理员用户标识，且此用户标识应一直具有实例管理员权限。

WebSphere Commerce 要求用户标识和密码遵循以下规则:

- 密码长度必须至少为 8 个字符。
- 密码必须包含至少 1 个数字。
- 密码中同一字符不能出现超过 4 次。
- 密码中同一字符不能重复超过 3 次。

WebSphere Commerce Payments 管理员

当安装 WebSphere Commerce Payments 时，WebSphere Commerce 站点管理员标识自动指定为支付管理员角色。请遵循《*WebSphere Commerce 安装指南*》中的指示信息将 “支付域类” 切换为 WCSRealm（如果尚未完成此步骤）。

支付管理员角色使用户标识能够控制和管理 WebSphere Commerce Payments。

400 **注意:**

- 不要删除或重命名为实例创建的站点管理员用户标识，也不要更改任何预先指定的 WebSphere Commerce Payments 角色，否则与 WebSphere Commerce Payments 集成相关的 WebSphere Commerce 功能将无法工作。

Windows

Windows 用户标识

Windows 用户标识*必须*具有管理员权限。如果正在使用 DB2®，则它要求用户标识和密码符合以下规则:

- 长度不可超过 8 个字符。
- 只能包含字符 A 到 Z、a 到 z、0 到 9、@、#、$ 和 _。
- 不允许以下划线字符（_）开头。
- 用户标识不可以是以下这几个单词，无论是大写、小写或是大小写混合: USERS、ADMINS、GUESTS、PUBLIC 和 LOCAL。
- 用户标识不可以使用以下任何单词开头，无论大写、小写或是大小写混合: IBM、SQL 和 SYS。
- 用户标识不可以与任何 Windows 服务名称相同。
- 用户标识必须在本地机器上定义，且必须属于本地管理员组。

- 用户标识必须具有*担当部分操作系统角色*的高级用户权限。

您可以执行安装，而无须具有*担当部分操作系统角色*的高级用户权限，但是 DB2 安装程序将无法验证您为“管理服务器”指定的帐户。建议任何用于安装 DB2 的用户帐户都具有这种高级用户权限。

重要信息

如果 Windows 用户标识不具有管理员权限，或长度大于 8 个字符，或未在本地机器上定义，则系统将通知您发生错误并将无法继续安装。

如果正在使用 DB2，则您将把此用户标识用作 DB2 数据库用户名（数据库用户登录标识）。

如果需要创建符合以上标准的用户标识，您可从 Windows 联机帮助中找到关于创建 Windows 用户标识的信息。

更改配置管理器密码

在您启动配置管理器时，可以通过在输入用户标识和密码的窗口中单击**修改**来更改配置管理器密码。

备选方案是，要更改配置管理器用户标识或密码，可切换到 WebSphere Commerce 安装路径下的 bin 子目录，并在命令窗口中输入以下命令:

1. 切换到 WebSphere Commerce bin 子目录:

   ```
   cd WC55_installdir/bin
   ```

2. 运行 wcs_encrypt 脚本来获得加密版本的密码:

   AIX 400 Linux Solaris

   ```
   ./wcs_encrypt.sh new_password
   ```

   Windows

   ```
   wcs_encrypt new_password
   ```

3. 打开 *WC55_installdir*/instances 目录中的 PwdMgr.xml 文件，然后用在第 2 步中加密的加密密码来修改登陆密码。

设置 IBM HTTP Server 管理员密码

AIX Linux Solaris Windows 要设置 IBM HTTP Server 管理员密码，

1. 切换到您机器上的 *HTTPServer_installdir*/bin 目录。
2. 输入以下命令:

   AIX Linux Solaris `./htpasswd -b ../conf/admin.passwd user password`

   Windows `htpasswd -b conf\admin.passwd user password` 其中 *user* 和 *password* 是希望对于 IBM HTTP Server 拥有管理权限的用户标识和密码。

现在已经成功地设置了 IBM HTTP Server 管理密码。

注: 如果管理员密码不存在，则需要先运行带 -c 选项的 htpassword 来创建密码。

更改 SSL 密钥文件密码

AIX Linux Solaris Windows 如果正在使用 IBM HTTP Server，请遵守下面的步骤更改 SSL 密钥文件密码。

1. Windows 单击**开始菜单 → 程序 → IBM HTTP Server → 启动密钥管理实用程序**。
2. 从**密钥数据库文件**菜单中，选择**打开**。
3. 切换至机器的 IBM HTTP Server 安装路径下的 ssl 子目录。您的密钥文件（文件扩展名为 .kdb）应当在此文件夹中。如果没有，请遵循第 171 页的第 17 章，『为 IBM HTTP Server 的生产启用 SSL』中概括的指示信息创建新的密钥文件。
4. 从**密钥数据库文件**菜单中，选择**更改密码**。“更改密码”窗口出现。
5. 输入您的新密码，并启用**将密码隐藏到文件中**。
6. 单击**确定**。您的密码已经更改。

现在已经成功地更改了您的 SSL 密钥文件管理密码。

生成 WebSphere Commerce 加密的密码

您可以生成已加密的密码，以从命令行手工重新设置用户密码。还有其它工具（例如 ResetPassword 命令）可以完成相同的任务。要手工重新设置密码，管理员将取得由以下实用程序输出的已加密密码，并更新 USERREG 表的 LOGONPASSWORD 字段。管理员还将用选择的 salt 来更新 USERREG 表的 SALT 字段。

AIX Linux Solaris Windows WebSphere Commerce 允许您生成加密的密码。要生成加密的密码，请执行以下操作:

1. 转至 WebSphere Commerce 安装目录下的 bin 子目录。
2. 从命令行运行以下脚本:

   Windows `wcs_password.bat` *`password SALT merchant_key`*

   AIX Linux Solaris `./wcs_password.sh` *`password SALT merchant_key`*

   其中

   - *password* 是纯文本密码。
   - *SALT* 是用于生成密码的随机字符串。它可以在密码得到更新的特定用户的 USERREG 数据库表的 SALT 列中找到。
   - *merchant_key* 是创建实例期间输入的商家密钥。

400 对于 iSeries，要更改购物者的加密密码，请使用 chgwcspwd.sh 命令。

1. 在 iSeries 系统上启动 QShell 会话。
2. 浏览到以下目录: *WC_installdir*/bin
3. 从命令行运行以下脚本: chgwcspwd.sh（会显示用法参数。）
4. 使用适当的参数再次运行命令。

关于运行该命令的详细信息，请参阅 WebSphere Commerce 生产和开发联机帮助。

生成 WebSphere Commerce Payments 加密的密码

WebSphere Commerce 允许生成 WebSphere Commerce Payments 的加密密码。要生成加密的密码，请执行以下操作:

1. 转至 WebSphere Commerce 安装目录下的 bin 子目录。
2. 从命令行运行以下脚本:

   Windows `wcs_pmpassword.bat password SALT`

   AIX 400 Linux Solaris `./wcs_pmpassword.sh password SALT`

   其中:

   - *password* 是纯文本密码。
   - *SALT* 是用于生成密码的随机字符串。它可以在密码得到更新的特定用户的 USERREG 数据库表的 SALT 列中找到。

复位管理员帐户

如果 WebSphere Commerce 帐户出于某种原因被锁定或禁用，则可以如下解锁或启用该帐户:

如果帐户不是站点管理员的帐户:

1. 打开管理控制台。
2. 单击**访问管理 > 用户**。
3. 双击该用户帐户或从列表中选择该用户帐户并单击**更改**。
4. 在“帐户状态”字段中选择**启用**。
5. 单击**确定**。

如果该帐户是站点管理员的帐户或任何其它用户帐户，则从 DB2 命令窗口或 SQLPlus 提示符（对于 Oracle 数据库）运行以下 SQL 语句:

```
CONNECT TO db_name [USER user_id USING password]
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE LOGONID='logonId'
```

其中

db_name
: 是您的 WebSphere Commerce 数据库名称（例如 MALL）。

user_id 是数据库的数据库管理员用户标识。

password
: 是对应于数据库管理员用户标识的密码。

logonId
: 是要复位的帐户的用户标识（如 wcsadmin）。

例如，要复位 wcsadmin 帐户，如果是作为数据库管理员用户标识登录到系统上，则可以发出以下 SQL 语句:

```
CONNECT TO mall
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE LOGONID='wcsadmin'
```

400 要在 iSeries 平台上输入 SQL 语句，您可以使用 DB2/400 查询管理器和 SQL 开发包，或者可以使用 iSeries 导航器。要使用 IBM iSeries Access 来执行数据库查询，请执行以下操作:

1. 从安装 iSeries 导航器的 PC 启动此导航器。
2. 扩展 iSeries 系统。扩展数据库，用鼠标右键单击关系数据库，然后选择**运行 SQL 脚本**。这会打开“运行 SQL 脚本”窗口。
3. 从“连接”菜单，选择 **JDBC 设置**。单击**服务器**选项卡。
4. 在“缺省库”字段中，擦除任何现有的值，然后输入您实例的数据库模式的名称。缺省情况下，模式名称是实例的名称。单击**确定**以保存更改。
5. 在窗口中输入上面的 SQL 语句。

第 7 章 单一注册

本章概述了如何为 WebSphere Commerce 设置单一注册。

先决条件

要启用单一注册，必须满足以下需求:

- 必须安装和配置了现有的 LDAP 服务器。要配置 LDAP 服务器，请参阅*《WebSphere Commerce 附加软件指南》*。
- 必须将 WebSphere Commerce 安装并配置为使用 LDAP。
- 必须启用了 WebSphere Application Server 安全性。要启用 WebSphere Application Server 安全性，请参阅第 161 页的第 16 章，『启用 WebSphere Application Server 安全性』。

启用单一注册

注意事项

在将单一注册用于 WebSphere Commerce 时对它有一些关键限制。这些限制是:

- LTPA cookie 可以通过不同的 Web 服务器端口。
- 您可能需要修改 `ldapentry.xml` 文件并添加对象类 `ePerson`。这是 `ldapocs` 元素的属性。
- 需要修改 `instance.xml` 并确保 `MigrateUsersFromWCSdb` 标志设为 “ON”。
- 参与单一注册配置的机器必须将它们的系统时钟同步。
- 单一注册仅在可以读取和发出 WebSphere Application Server 轻量级第三方认证（LTPA）令牌的应用程序之间受支持。

要启用单一注册，必须执行以下操作:

1. 启用 WebSphere Application Server 内的单一注册。关于更多信息，请在 WebSphere Application Server 信息中心（`http://www.ibm.com/software/webservers/appserv/infocenter.html`）中搜索 “single sign-on”。选择 **Single Sign-On: WebSphere Application Server** 并完成以下部分:
   - **为 WebSphere Application Server 配置 SSO**。
     - **修改 WebSphere Application Server 安全性设置**。

       注: 下一步是详细说明如何填写 LDAP 字段的，可以忽略而不会有任何问题。
     - **将 LTPA 密钥导出至文件**。
2. 在 WebSphere Commerce 机器上，启动 WebSphere Commerce 配置管理器。
3. 要配置**成员子系统**节点，请执行以下操作:
   a. 在 **WebSphere Commerce** 下展开 *host_name* → **实例列表** → *instance_name* → **实例属性** → **成员子系统**。

b. 在**认证方式**下拉菜单中，选择 **LDAP**。

c. 启用**单一注册**复选框。

d. 在**主机**字段中，输入 LDAP 服务器的全限定主机名。

e. 在**管理员专有名称**字段中输入管理员的专有名称。此名称应当与用在 LDAP 服务器上的名称相同。

f. 在**管理员密码**字段中，输入管理员的密码。此密码应当与用在 LDAP 服务器上的密码相同。确认**确认密码**字段中的密码。

g. 完成每个剩下的字段。

h. 单击**应用**，然后单击**确定**。

4. 配置角色，这些角色将指定给从单一注册（SSO）进入系统的用户。每当用户通过 SSO 连接到系统时，WebSphere Commerce 将会尝试从 `MemberRegistrationAttributes.xml` 文件分配注册类型 = “SSO” 的角色。链接到描述 MRA.xml 的新的一节。

5. 重新启动 WebSphere Application Server。

为 SSO 用户配置角色

在 WebSphere Commerce 5.5 中，安全性角色是作为注册过程的一部分进行指定的。在单一注册时，如果用户已成功地向协作系统认证，那么他们可以绕过站点的注册步骤。如果用户只是简单地面临被拒绝访问他们想要使用的设备（例如，在商店购物），那么隐式地认证到 WebSphere Commerce 5.5 站点的能力没有什么价值。

因此，发生在用户注册时的同样的自动角色指定功能也会发生在会话管理代码中。在此例中，您需要使用 “SSO” 注册类型来配置 SSO 购物者角色。这样，当客户认证到系统时，WebSphere Commerce 5.5 会自动提供他们在该站点上应该拥有的所有角色。记住，SSO 角色指定发生在站点级，而不是商店级（如典型用户注册那样）。因此，您应该确保指定的 StoreAncestor 属性确实是站点（商店 0）的上级。

例如:

```
<User registrationType="SSO" memberAncestor="o=Default Organization,o=Root Organization" storeAncestor="o=Root Organization"><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="o=Reseller Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="o=Seller Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="o=Supplier Organization,o=Root Organization"/><BR>
    <Role name="Registered Customer" roleContext="explicit" DN="ou=Supplier Hub Organization,o=Business Indirect Supplier Organization,
          o=Root Organization"/><BR>
  </User>
```

该示例会向任何从 SSO 进入系统的购物者提供四个角色

第 8 章 管理 X.509 证书

WebSphere Commerce 支持作为安全性机制的客户机证书登录，从而保护了站点和客户。X.509 证书为客户进入站点增补了基本的认证。持有此证书的客户可以访问受保护的且已启用客户机证书认证的 WebSphere Commerce 站点。

当创建 WebSphere Commerce 实例时，选择“认证方式”。认证方式可以是“基本”或“X.509”。缺省值是基本认证方式，它是使用登录标识和密码的登录认证。要激活使用 X.509 证书的登录认证，请选择 X.509 认证。

在可以开始使用 X.509 证书之前，必须安排同外部认证中心的信任关系，以便处理 X.509 证书的电子认证。如果正使用 Netscape Enterprise 作为 Web 服务器，将需要遵循附加的步骤在您的 Web 服务器上启用 X.509 证书。关于更多信息和完整的指示信息，请参阅 Netscape Enterprise Server 文档。

通过 WebSphere 贸易加速器，可以访问 X.509 用户。在启用 X.509 证书认证之前，管理员必须确保有客户机证书（它是由服务器证书识别出并且是安装在浏览器上的）。否则，管理员将无法登录。当管理员第一次访问 WebSphere Commerce 管理控制台登录窗口时，会创建一个认证购物者记录并发出一个购物者 cookie，这类似于当普通购物者访问安全 URL 的时候。在管理员使用正确的标识和密码登录到 WebSphere Commerce 管理控制台的时候，会发出一个管理员 cookie 来替换购物者 cookie。然后管理员将有两条用户记录：管理员用户和先前的购物者用户。

当发生以下情况时会显示错误消息:

- 站点已取消了用户的 X.509 证书
- 客户机证书不包含这么一种必要信息，即保证购物者在 WebSphere Commerce 中是唯一的。

X.509 错误视图任务是作为 `VIEWREG` 数据库表中的 `X509 ErrorView` 注册的。

启用 X.509 证书

当创建 WebSphere Commerce 实例时，使用配置管理器选择基本认证方式或 X.509 认证方式。缺省值是基本认证方式，它是使用登录标识和密码的认证。

要使用 X.509 证书启用认证，请执行以下操作:

1. 安装 IBM HTTP Web 服务器 SSL 证书。SSL 服务器证书包括一个用于信任关系的客户机权限列表。您可能需要添加其它的客户机认证中心。
2. 启动 WebSphere Commerce 配置管理器。
3. 选择**实例属性 -> Web 服务器**。
4. 针对“认证方式”选中 **X.509** 框。单击**应用**。现在将接受 X.509 客户机证书用户。当选择 X.509 认证方式时，将为证书支持自动启用 IBM HTTP Server。
5. 启动并停止 WebSphere Commerce 服务器。直到重新启动了服务器时，WebSphere Commerce 才会在 `CERT_X509` 表中注册 X.509 用户。

注: 您可以配置 IBM HTTP Server，使得 X.509 证书是可选的或者必需的。

1. 打开配置文件 `httpd.conf` 并找到 `SSLClientAuth` 伪指令。将该伪指令设置为 1（可选的）或 2（必需的）。建议的参数是*必需的*。
2. 因为 WebSphere Commerce Payments 客户机不支持 SSL 客户机认证，所以必须禁用 WebSphere Commerce Payments 客户机和 Web 服务器之间的 SSL。
   a. 在文本编辑器中打开 `PaymentServlet.properties` 文件。该文件在 WebSphere Commerce Payments 安装目录中。
      - 找到 `UseNonSSLWCSClient` 属性。将该属性设置为值 “1”。
      - 如果在文件中找不到 `UseNonSSLWCSClient` 属性，则添加行:

        ```
        UseNonSSLWCSClient=1
        ```
   b. 保存文件，并退出编辑器。
3. 如果 WebSphere Commerce Payments 安装在 WebSphere Commerce 的同一台机器上:
   a. 启动配置管理器。
   b. 选择实例；然后选择 **Payments**。
   c. 选中**使用非 SSL WebSphere Commerce Payments 客户机**。这使得 WebSphere Commerce Server 客户机能够在不使用 SSL 的情况下同 WebSphere Commerce Payments 通信。
   d. 单击**应用**。
   e. 关闭配置管理器。
4. 从 WebSphere 管理控制台重新启动 WebSphere Commerce Payments 应用程序服务器。
5. 从 WebSphere 管理控制台重新启动 WebSphere Commerce 应用程序服务器。

关于为证书设置限制和过滤参数的更多信息和进一步的选项，请参阅 IBM HTTP Server 文档。

更新 X.509 证书用户的状态

使用 WebSphere 贸易加速器，站点管理员可以将 X.509 证书用户的状态更新为以下三个状态值中的一个:

有效 用户可以使用他们的证书访问受保护的 WebSphere Commerce 站点。

已取消 用户无法访问 WebSphere Commerce 站点。当证书已取消的用户尝试登录时，他们将得到一个 X.509 证书错误页面。

已失效 用户无法访问 WebSphere Commerce 站点。当证书已失效的用户尝试登录时，他们将得到一个 X.509 证书错误页面。

当管理 X.509 证书时，也可能希望对证书持有者设置限制和过滤参数。例如，也可能希望通过修改 `httpd.conf` 配置文件允许某些类型的证书持有者访问受保护的站点。

关于更多信息和指示信息，请参阅 Web 服务器文档。

典型的认证方案

下面的步骤显示了 X.509 证书的典型认证方案:

1. 购物者访问:
   - 通过 http:// 的非安全 URL

     不执行任何认证。
   - 通过 https:// 的安全 URL

     提示购物者选择客户机证书。
   - 一条 URL 命令并重定向到 https://，因为这是 URL 命令的访问方式

     提示购物者选择客户机证书。
2. WebSphere Commerce 服务器使用来自客户机证书的信息确定购物者是否已存在于 WebSphere Commerce SHOPPER 表中:
   - 如果购物者存在并具有有效的证书状态，则认证该购物者并继续购物流程。
   - 如果购物者不存在:
     - 自动将购物者注册到 WebSphere Commerce 数据库中，并继续购物流程。

注: 从证书只能得到 CERT_X509 表中找到的信息。但是，可从 X.509 客户机证书得到购物者地址信息（如果有）。

第 3 部分 管理安全性授权

本部分描述可由 WebSphere Commerce 站点管理员执行的安全性授权任务。

第 9 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客户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客户，以及为渴望从因特网的能力和增加的效率中得益的新客户铺平道路来说，Web 是关键因素。当获得在 Web 上做生意的明显优势和增加客户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客户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 而开始的客户关系的影响。

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
客户可以自注册。	只有卖方管理员才可以注册新客户。
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，则只有客户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供货中心。	具有“后勤部经理”角色的雇员可以创建但是不能修改供货中心。

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 10 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 WebSphere Commerce 5.5 中，引进了业务模型。创建实例之后，管理员可以发布一些样本业务模型，这些模型将建立组织结构。关于业务模型的更多信息，请参阅第 15 页的『业务模型』。

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”关系的客户注册到站点。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。如果正在使用提供的样本业务模型，则可向前跳至关于访问控制的下一节。如果想要定义自己的组织结构，请继续以下步骤。

要找到关于创建组织、用户和角色的详细信息，请参阅可从以下技术库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

我们还建议您查看《*WebSphere Commerce 基础*》。要全面了解业务模型，请分别参阅《*WebSphere Commerce 商店开发指南*》和《*WebSphere Commerce 样本商店指南*》。

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，将为该组织创建概要文件，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。由于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和销售员等等。请参阅第 25 页的『角色』以获取缺省角色列表。
4. 创建用户。与组织相似，将为每个用户创建概要文件，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。
5. 将策略组指定给新组织，这样客户就可以在由该组织管理的商店中购物了。必需的典型策略组是: 管理和经营策略组、公共购物策略组、B2C 策略组或 B2B 策略组。关于策略组的更多信息，请参阅第 185 页的『缺省访问控制策略和组』。

上面概述的所有步骤都可由站点管理员通过组织管理控制台中的“访问管理”菜单执行。

注: 在 WebSphere Commerce Professional Edition 中，您不能创建任何组织。已经为您创建了卖方组织。

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。

注: 在正常情况下，买方组织不需要预订任何策略组，因为它们将继承根组织预定的策略组。

再次说明，上面概述的所有步骤均可通过组织管理控制台中的“访问管理”菜单执行。

注: 在 WebSphere Commerce Professional Edition 中，所有客户都属于“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从注册到管理拍卖、到更新产品目录和核准订单，以及运作和维护电子交易站点所需的所有其它数百种活动。

策略的作用是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。

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。

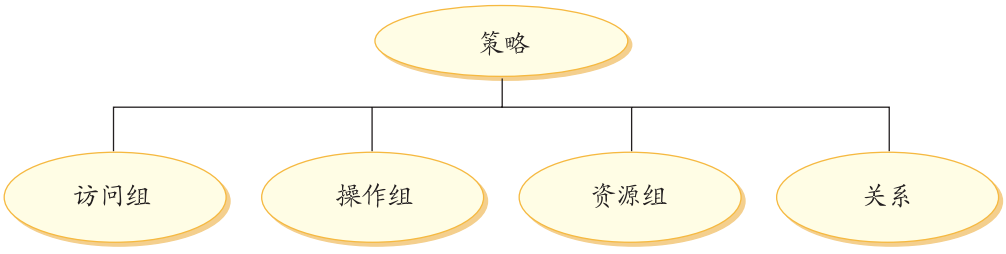
*访问组*是对站点上的一组功能共享公共访问权的一组用户。访问组通常包含共享公共属性（例如同一角色、部门或技能集）的用户。

*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 4. 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 15 页的第 3 章，『授权概念』。

如何着手使用访问控制?

在一些情况下，您什么也不用做！业务模型的简介有助于在系统中提供基本访问控制结构，而且 WebSphere Commerce 中的缺省策略设计为基于系统中的典型用户，以及他们执行的与他们在组织中的角色相关联的活动，来提供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 36 页的『详细探讨一个策略』。

第 11 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 15 页的第 3 章，『授权概念』以获取更多信息。

识别受更改影响的策略

在第 15 页的第 3 章，『授权概念』，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

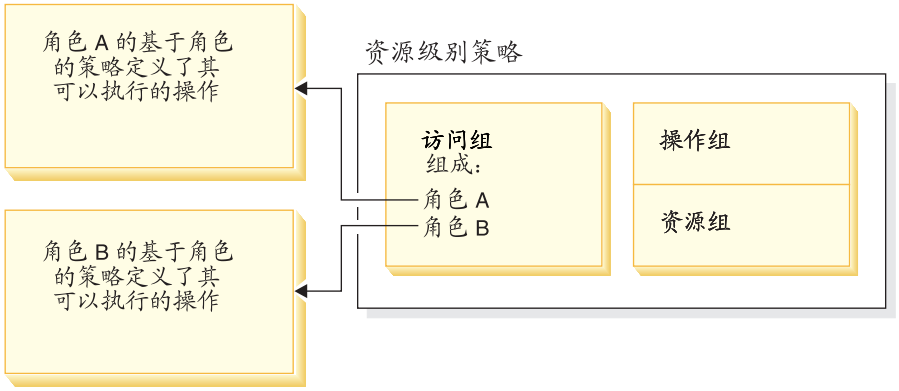
在 WebSphere Commerce 中，如下使用基于角色的策略，将可由用户执行的每个操作指定给一个或多个角色:

- 每个缺省角色都具有对应的访问组。例如，“卖方”角色的访问组是卖方。
- 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，OperationalReportsHomeRHSView 将显示带有卖方可以访问的运营报表的列表的 Web 页面。

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。

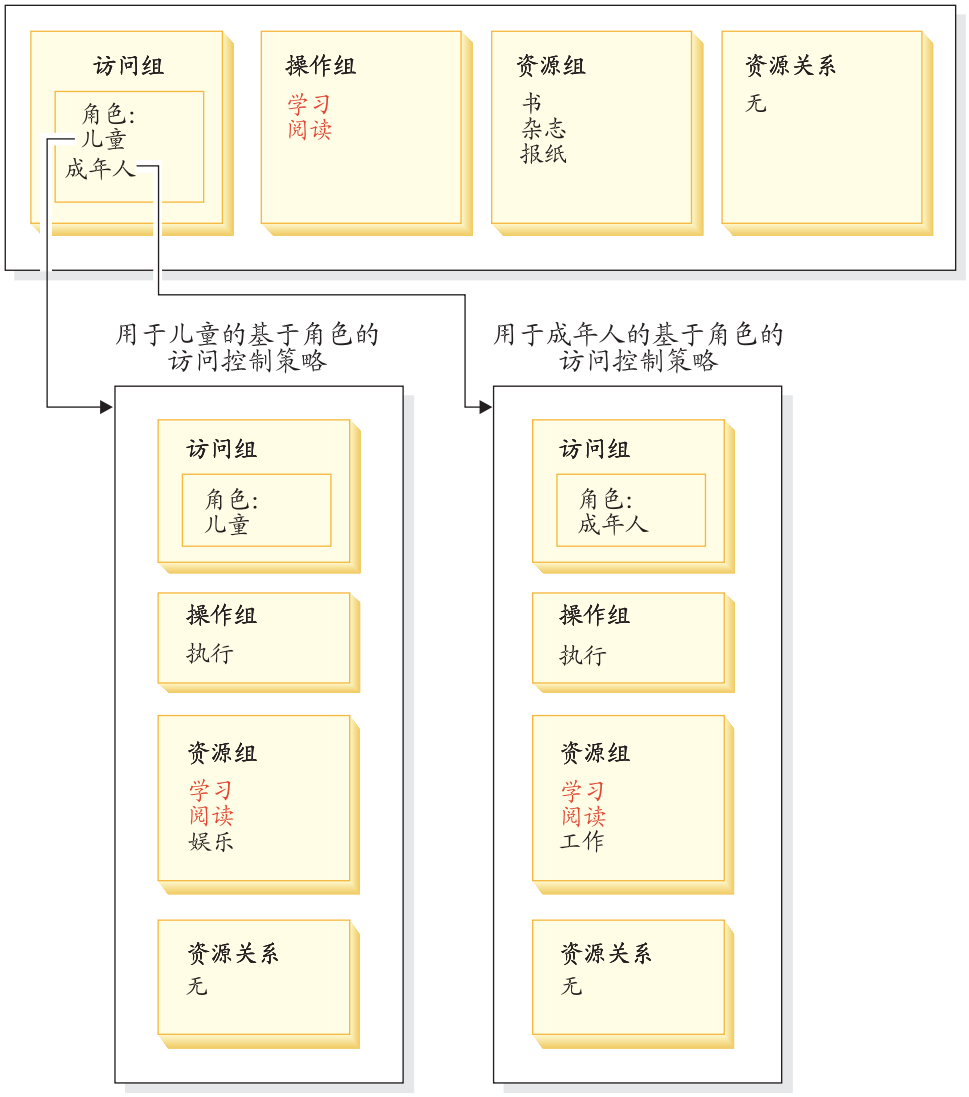
图 5. 资源级别的策略及其关联的基于角色的策略之间的关系



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 6. 资源级别的策略以及影响它的基于角色的策略。

各类用户的资源级别访问控制策略



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。可通过从组织管理控制台选择“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。

下表总结了在创建、删除或更改资源级别的策略时需要进行的附加更改。

表 9. 更改使用角色的资源级别的策略时需要的附加更改。

切换至资源级别策略	在资源级别访问组使用角色的情况下所必需的更改
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。
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。

表 9. 更改使用角色的资源级别的策略时需要的附加更改。 (续)

切换至资源级别策略	在资源级别访问组使用角色的情况下所必需的更改
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: `SalesManagersExecuteSalesManagersViews`。

资源组包含称为 `com.ibm.commerce.command.ViewCommand` 的单个资源。

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，在商店环境中创建拍卖，在组织环境中创建用户。大多数资源都是在商店环境中创建的。因此，这些策略具有如下的名称:

<AccessGroupXYZs> Execute <XYZCommands> On <StoreEntityResource>

例如:

`AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource`

.

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（例如买方或产品经理）定义的。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 25 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。要做到这点，从组织管理控制台选择**访问管理 > 访问组**。
- 根据对视图选择的值，“策略”页面列出了选定的组织所拥有的策略。它不区分站点级别的策略和特定于特殊组织的策略。
- 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: 访问控制策略菜单被移到了组织管理控制台。组织管理控制台仅可以对访问控制策略定义和访问组定义做简单的修改。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。
3. 将新策略指定给策略组。

更改策略之后

创建新策略后，在它生效之前必须先分配给策略组。应该将新策略分配给为策略提供服务的组。关于策略组名称的更多信息，请参阅第 185 页的『缺省访问控制策略和组』。

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。关于与访问控制策略和访问组相关的不同 XML 文件的描述，请参阅第 119 页的第 13 章，『使用 XML 定制访问控制策略』。还包含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的说明。

第 12 章 使用 GUI 定制访问控制策略

下面展示的方案让您能应用所学到的关于访问控制策略的知识来使用 GUI 对缺省策略进行各种基本更改。如果要进行复杂的更改，您将不得不使用 XML。请参阅第 119 页的第 13 章，『使用 XML 定制访问控制策略』。

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 10. 方案目录

业务区域	起始页
拍卖	第 92 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 95 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 97 页的『订单方案 1: 仅允许买方创建订单』
成员资格	第 103 页的『成员资格方案 1: 除去用户自注册能力』
赠券	第 107 页的『赠券方案 1: 仅允许买方兑换赠券』
采购	第 110 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 113 页的『库存方案 1: 允许供货中心经理更新供货中心但是不能删除它们』
商务智能	第 114 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，请参阅表 11，它按说明的定制类型交叉引用了这些方案。

表 11. 按定制类型组织的定制方案

定制	请参阅页
将角色添加到策略的访问组	108
更改策略的操作组	111,113
更改策略的资源关系	99,110
将策略更改为使用另一访问组	93,97,99,103,107,109
创建新访问组并将它用于策略	101,104
创建新操作组并将它用于策略	104,111
创建新的资源级别的策略	96,111
创建新的基于角色的策略	104,114

表 11. 按定制类型组织的定制方案 (续)

定制	请参阅页
创建新角色并将它用于资源级别的策略	104,114
删除策略	93,103
从策略的操作组中除去操作	3,95

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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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“更改操作组”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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 单击**更新**。

拍卖方案 2: 除去拍卖经理撤销投标的能力

缺省情况下，商店的拍卖经理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』查找资源级别的策略，该策略包含由拍卖经理执行的拍卖投标的撤回。
- 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:

   `AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
2. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
4. 从策略列表中，选择以下策略:

   AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
5. 单击**删除**。

使用更改更新策略注册表

1. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 单击**更新**。
5. 对**访问控制策略组注册表**重复步骤 3 和 4。

拍卖方案 3: 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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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(buy-side)CommandsResourceGroup.
2. 单击**访问管理 > 策略**。
3. 对于视图，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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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:
   `ContractManagersForOrgExecuteContractManageCommandsOnContractResource`
2. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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”，用本地语言指定策略的简短描述。

4. 对于“描述”，用本地语言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**成组模板策略**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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 单击**更新**。

注: 此新策略在生效之前必须先分配给策略组。策略的分配必须通过 XML 来完成。请参阅更多信息。

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用户，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。

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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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
   com.ibm.commerce.orderitems.commands.OrderItemAddCmd
   com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
   ```

   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(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup。
2. 单击**访问管理 > 策略**。
3. 对于视图，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(buy-side)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(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
   com.ibm.commerce.orderitems.commands.OrderItemAddCmd
   com.ibm.commerce.orderquotation.commands.OrderQuotationCreateCmd
   ```

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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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 Professional Edition。

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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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. 对于“关系”，选择**无**。
5. 更新策略的名称、显示名称和描述以反映对访问组的更改。
6. 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
   com.ibm.commerce.orderquotation.commands.OrderItemSelectCmd
   ```

   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: 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. 对于视图，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
   com.ibm.commerce.orderquotation.commands.OrderItemSelectCmd
   ```

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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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”，用本地语言指定策略的简短描述。
5. 对于“描述”，用本地语言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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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 Professional Edition 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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 单击**更新**。
5. 对**访问控制策略组注册表**重复步骤 3 和 4。

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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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，在对于操作的基于角色的策略中，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 UserAdminRegistrationCommands 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. 从组织管理控制台，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**来指定必须在用户自己的组织或上级中担任角色。
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:

   ```
   CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOn
   OrganizationResource
   ```

2. 单击**访问管理 > 策略**。
3. 对于视图，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”，用本地语言指定资源组的描述。
5. 对于“描述”，用本地语言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”，用本地语言指定策略的描述。
5. 对于“描述”，用本地语言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**。

注: 创建此新策略之后，在它生效之前必须先分配给策略组。这必须通过 XML 来完成。关于更多信息，请参阅第 119 页的第 13 章，『使用 XML 定制访问控制策略』。

修改资源级别的策略以使用新访问组

修改了资源级别策略之后，只允许那些在与该资源相同的组织中担任成员注册员角色的用户注册用户。在任何其他组织中担任角色的用户不具备此功能。

1. 从策略列表中，选择以下策略:

   CSAMembershipAdministratorsForOrgExecuteUserAdmin
   RegistrationCommandsOnOrganizationResource

   .
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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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:

   ```
   AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
   ```

2. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
4. 从策略列表中，选择以下策略:

   AllUsersExecuteCouponRedemptionCommandsOnCoupon WalletResource

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(buy-side)CommandsResourceGroup
   ```

2. 单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
4. 在列表中查找策略。
5. 记下资源组的名称: `Buyers(buy-side)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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 单击**更新**。

赠券方案 2: 允许赠券管理员和业务经理创建电子赠券促销

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，您可能希望也将此权限授予业务经理。

访问控制策略的灵活设计提供了实现此更改的若干方法:

- 可将业务经理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，该策略允许业务经理创建电子赠券促销。

此方案说明了第一种方法。它显示了如何将业务经理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业务经理角色的用户。
- 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』查找用于业务经理的基于角色的策略。此策略定义了具有业务经理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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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**业务经理**。
6. 单击**对于组织**来指定必须在资源自己的组织或其上级中担任角色。
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业务经理可执行命令列表的资源组中。

识别业务经理的基于角色的策略

1. 查看『附录』的“基于角色的策略”下的内容，查找出用于业务经理的基于角色的策略。策略是：OperationsManagersExecuteOperations ManagersCmdResourceGroup。
2. 单击**访问管理 > 策略**。
3. 对于视图，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 — OperationsManagersCmdResourceGroup。 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 **OperationsManagersCmdResourceGroup**。
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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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 Professional Edition。

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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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 Professional Edition。

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供货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. 从组织管理控制台，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”，用本地语言指定操作组的简短描述。
5. 对于“描述”，用本地语言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. 对于视图，单击**根组织**来显示其拥有的策略。
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”，用本地语言指定策略的简短描述。
6. 对于“描述”，用本地语言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**成组模板策略**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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 单击**更新**。

注: 创建此新策略之后，在它生效之前必须先分配给策略组。这是通过使用 XML 完成的。关于更多信息，请参阅第 119 页的第 13 章，『使用 XML 定制访问控制策略』。

库存方案 1: 允许供货中心经理更新供货中心但是不能删除它们

缺省情况下，授权供货中心经理更新或删除与其商店关联的供货中心。在一些情况下，您可能希望允许供货中心经理更新供货中心，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』查找授权供货中心经理管理供货中心的资源级别的策略。
- 从策略的操作组中除去用于删除供货中心的操作。

要执行的步骤

除去用于删除供货中心的操作

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. 从组织管理控制台，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供货中心的操作。
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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 单击**更新**。

库存方案 2: 仅允许后勤部经理、业务经理和客户代表创建、更新或删除供货中心

缺省情况下，授权供货中心经理创建、更新或删除与其商店关联的供货中心。供货中心经理的访问组包含以下角色: 卖方、后勤部经理、业务经理和客户代表。在一些情况下，您可能不希望将卖方授权为供货中心经理。

要进行此更改，需要执行以下操作:

- 使用『附录』查找授权供货中心经理管理供货中心的资源级别的策略。
- 从供货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. 从组织管理控制台，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. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. 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（审计员），并为其创建新访问组（审计员）、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。

- 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，在对于操作的基于角色的策略中，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. 从组织管理控制台，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. 从组织管理控制台，单击**访问管理 > 策略**。
3. 对于视图，选择**根组织**来显示其拥有的策略。
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**，用本地语言指定资源组的描述。
5. 对于**描述**，用本地语言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”，用本地语言指定策略的描述。
5. 对于“描述”，用本地语言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**来指定必须在资源自己的组织或其上级中担任角色。
7. 单击**添加**。

8. 单击**确定**。

使用更改更新策略注册表

1. 登录至管理控制台。
2. 单击**配置 > 注册表**。
3. 从注册表列表中，选择**访问控制策略**。
4. **单击“更新”。**

第 13 章 使用 XML 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，需要直接编辑 XML 文件,并将它们装入数据库。

在开始对用于访问控制的 XML 文件作更改之前，应当阅读《*WebSphere Commerce 编程指南和教程*》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《*WebSphere Commerce 编程指南和教程*》中所提供的指示信息完成了代码定制，就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:

- 创建或修改操作
- 创建或修改关系
- 创建或修改关系组
- 创建或修改资源
- 创建或修改属性
- 使用复杂条件创建或修改访问组
- 使用复杂条件创建或修改资源组
- 创建视图的基于角色的策略
- 更改视图的基于角色的策略中的操作组
- 创建或修改策略组
- 将策略和策略组关联起来

关于访问控制的 XML 文件

下表显示了 WebSphere Commerce 的 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 12. 用于访问控制的 WebSphere Commerce XML 文件

文件名	描述
ACUserGroups_de_DE.xml 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	用于从数据库抽取所有访问控制信息的过滤文件。
OrganizationPoliciesFilter.xml	用于抽取特定组织所拥有的所有与策略相关的访问控制信息的过滤文件。
ACUserGroupsFilter.xml	用于抽取所有访问组信息的过滤文件。
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。

表 12. 用于访问控制的 WebSphere Commerce XML 文件 (续)

文件名	描述
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。
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。

更改 XML 文件

您可以控制 XML 文件来执行以下授权任务:

- 保护视图
- 保护控制器命令
- 实现资源级别的访问控制
- 保护数据 bean
- 按属性将资源分组
- 定义关系
- 定义关系组

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"
   PolicyType="groupableStandard">
</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。同样地，对于大多数角色，每个角色都有一个对应的操作组将该角色可以访问的视图归类成一组，例如卖方角色 -> Sellers 访问组-> SellersViews 操作组。

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 列中。Name 和 CommandName 属性无需是相同的。

使用现有策略添加新视图

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，请创建一个与显示的相似的 XML 文件，然后执行以下操作:

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

 <Action Name="MyNewView"
          CommandName="MyNewView">
 </Action>
  <ActionGroup Name="ProductManagersViews" OwnerID="RootOrganization">
              <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>
 </Policies>
```

1. 在具有视图名称 *MyNewView* 的 XML 文件中创建新操作定义。这可以是您选择的任何名称。

   ```
   <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，如下面的示例所示:

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

  <ActionGroupAction Name="MyNewView"/>

 </ActionGroup>
```

已有基于角色的策略（ProductManagersExecuteProductManagersViews）包含了此操作组，因此没有必要创建新策略。同样，缺省的属于 ManagementAndAdministrationPolicyGroup 策略组的基于角色的策略适用于站点上的大多数（如果不是全部）组织，因此不需要更多的策略组预订。

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 149 页的『将更改装入数据库』。
4. 通过执行以下操作在管理控制台中更新访问控制策略注册表:
   a. 作为站点管理员登录到管理控制台。
   b. 单击**配置 > 注册表**。
   c. 从注册表列表中，选择**访问控制策略**。
   d. 单击**更新**。

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角色来访问的新视图，请创建一个与显示的相似的 XML 文件，然后执行以下操作:

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>

 <Action Name="MyNewView"
          CommandName="MyNewView">
 </Action>
  <ActionGroup Name="XYZViews" OwnerID="RootOrganization">
              <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>
 <Policy Name="XYZExecuteXYZViews"
   OwnerID="RootOrganization"
UserGroup="XYZ"
   ActionGroupName="XYZViews"
   ResourceGroupName="ViewCommandResourceGroup"
   PolicyType="groupableStandard">
 </Policy>

 <PolicyGroup Name="ManagementAndAdministrationPolicyGroup" OwnerID="RootOrganization">
  <PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization" />
 </PolicyGroup>

 </Policies>
```

1. 在具有视图名称 *MyNewView* 的 XML 文件中创建新操作定义。这可以是您选择的任何名称。

   ```
   <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>
   ```

   其中 *XYZViews* 是操作组的名称。操作组的 OwnerID 应该始终为 RootOrganization。
3. 将新操作与新操作组关联:

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

 <ActionGroupAction Name="MyNewView"/>

</ActionGroup>
```

其中 *XYZViews* 是操作组，*MyNewView* 是创建的操作。

4. 创建引用新操作组的策略:

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

其中 *XYZExecuteXYZViews* 是策略名，*XYZViews* 是操作组。在 WebSphere Commerce 5.5 中，由于策略预订模型的原因，并不使用可分组标准和可分组模板策略的 OwnerID 来确定策略将应用哪些资源。OwnerID 值当前仅由管理控制台在按组织（所有者）查看策略时使用。如果某项策略适用于多个组织，则建议将 OwnerID 设置为公共的上级组织，例如根组织。如果某项策略仅适用于一个特定的组织，则建议将 OwnerID 设置为该组织的 orgentity_id。

5. 将新的策略包含在适当的策略组中。缺省情况下，大多数基于角色的策略均放置到 ManagementAndAdministrationPolicyGroup 中，它们应适用于所有组织。

```
<PolicyGroupName="ManagementAndAdministrationPolicyGroup"
OwnerID="RootOrganization">
<PolicyGroupPolicy Name="XYZExecuteXYZViews" PolicyOwnerId="RootOrganization"/>
</PolicyGroup>
```

其中 PolicyOwnerId 值必须与用在策略定义中的 OwnerID 值相同。

6. 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 149 页的『将更改装入数据库』。
7. 通过执行以下操作在管理控制台中更新访问控制策略注册表:
   a. 作为站点管理员登录到管理控制台。
   b. 单击**配置 > 注册表**。
   c. 从注册表列表中，选择**访问控制策略**。
   d. 单击**更新**。

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 130 页的『保护资源』。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"
   PolicyType="groupableStandard">
</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 的值存储于 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，后者依次扩展 Protectable 接口。关于这些接口的更多信息，请参阅《*WebSphere Commerce 编程指南和教程*》。

使用现有策略添加新的控制器命令

要添加由新角色访问的且具有现有基于角色的策略的新控制器命令，请创建类似于以下所示的 XML 文件。随后列出了特定步骤。

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">

<Policies>
```

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

  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>
<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
    ResourceGroupResource Name="com.xyz.commands.MyNewControllerCmdResource
    Category"/>
 </ResourceGroup>
 </Policies>
```

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，如下面的示例所示:

```
 <ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
  <ResourceGroupResource Name="com.xyz.commands.
MyNewControllerCmdResourceCategory"/>

 </ResourceGroup>
```

   根据要使用的角色，您可以更改资源组。关于基于角色的策略的更多信息，请参阅第 186 页的『基于角色的策略』。

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 149 页的『将更改装入数据库』。
4. 通过执行以下操作在管理控制台中更新访问控制策略注册表:
   a. 作为站点管理员登录到管理控制台。
   b. 单击**配置 > 注册表**。
   c. 从注册表列表中，选择**访问控制策略**。
   d. 单击**更新**。

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）。关于资源级别的检查和命令的信息，请参阅第 128 页的『修改现有策略的资源级别访问控制』。

添加使用新策略的新控制器命令

要添加可由新角色访问的且不具有现有基于角色的策略的新控制器命令，请创建类似于以下所示的 XML 文件。随后列出了特定步骤。

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
<Policies>

  < ResourceCategory  Name="com.xyz.commands.MyNewControllerCmdResourceCategory"
    <ResourceBeanClass="com.xyz.commands.MyNewControllerCmd">

  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>
       <ResourceGroup Name="XYZCmdResourceGroup"  OwnerID="RootOrganization"
    <ResourceGroupResource Name="com.xyz.commands.MyNewController
    CmdResourceCategory"/>
 </ResourceGroup>
```

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

  <PolicyGroup Name="ManagementAndAdministrationPolicyGroup"
   OwnerID="RootOrganization">
  <PolicyGroupPolicy  Name="XYZExecuteXYZsCmdResourceGroup"
   PolicyOwnerId="RootOrganization" />
 </PolicyGroup>

 </Policies>
```

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。请参阅第 125 页的『使用现有策略添加新的控制器命令』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">
      PolicyType="groupableStandard">
   </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 149 页的『将更改装入数据库』。
6. 通过执行以下操作在管理控制台中更新访问控制策略注册表:
   a. 作为站点管理员登录到管理控制台。
   b. 单击**配置 > 注册表**。
   c. 从注册表列表中，选择**访问控制策略**。
   d. 单击**更新**。

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）。关于资源级别的检查和命令的信息，请参阅第 128 页的『修改现有策略的资源级别访问控制』。

为控制器命令修改命令级别访问控制

基于缺省访问控制策略，UserRegistrationAdminAddCmd 命令不能由那些仅拥有市场部经理角色的用户运行。以下方案描述修改现有策略，以使得这些用户能执行该命令所需的步骤。您可以使用此方案中的步骤，并定制它们以满足您自己的需求。

所有的控制器命令都需要一个命令级别的访问控制策略，它有 ActionGroupName = ExecuteCommandActionGroup。它还必须有一个包含控制器命令的接口名称的资源组。这些策略通常应用于一个特定角色，例如 MarketingManagersExecuteMarketingManagerCmdResourceGroup。

```
<Policy Name="MarketingManagersExecuteMarketingManagerCmdResourceGroup"
   OwnerID="RootOrganization"
   UserGroup="MarketingManagers"
   ActionGroupName="ExecuteCommandActionGroup"
   ResourceGroupName="MarketingManagerCmdResourceGroup"
   PolicyType="groupableStandard">

</Policy>
```

注: 以上策略是在实例创建期间，装入到数据库的缺省策略之一。关于缺省策略的更多信息，请参阅第 185 页的『缺省访问控制策略和组』。

在此情况下，如果想要具有市场部经理角色的用户能够执行 UserRegistrationAdminAddCmd，您必须通过创建自己的 XML 文件来将此命令添加到用于策略中的现有资源组，并执行以下操作:

1. 重新定义 ExecuteCommand 操作
2. 将 com.ibm.commerce.usermanagement.commands.UserRegistrationAddCmd 重新定义为一个资源类别。
3. 将资源类别与必需的资源组相关联，在此情况下是 MarketingManagerCmdResourceGroup。
4. 将 XML 文件复制到 *WC_installdir*/xml/policies/xml。以下是 XML 的样式示例:

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE Policies SYSTEM "../dtd/accesscontrolpolicies.dtd">
<Policies>

 <Action Name="ExecuteCommand"
   CommandName="Execute">
  </Action>

 <ResourceCategory
      Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdmin
AddCmdResourceCategory"
   ResourceBeanClass="com.ibm.commerce.usermanagement.commands.
UserRegistrationAdminAddCmd">
  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

 <ResourceGroup Name="MarketingManagerCmdResourceGroup"  OwnerID="RootOrganization"
  ResourceGroupResource
      Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmdResourceCategory"/>
 </ResourceGroup>

 </Policies>
```

5. 使用 *WC_installdir*/bin/acpload 脚本，将 XML 文件装入到数据库中。关于装入 XML 文件的更多信息，请参阅第 149 页的『将更改装入数据库』。
6. 通过执行以下操作，在 WebSphere Commerce 管理控制台中更新访问控制策略注册表:
   a. 作为站点管理员登录到管理控制台。
   b. 单击**配置 > 注册表**。
   c. 从注册表列表中，选择**访问控制策略**。
   d. 单击**更新**。

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）。如果正在执行资源级别的检查，请参阅『修改现有策略的资源级别访问控制』。

修改现有策略的资源级别访问控制: 对于需要资源级别访问控制的命令，它们会返回那些将在命令的 getResources() 方法中访问的受保护资源。这会触发由 WebSphere Commerce 访问控制框架执行的资源级别访问控制检查。在此示例 com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd 中，

WebSphere Commerce 将在带有操作组的系统中搜索访问控制策略，该操作组包含等同于当前命令的操作。策略的资源组还必须包括以 getResources() 方法返回的资源。在此情况下，UserRegistrationAdminAddCmd 命令确实实现 getResources() 方法，并返回新用户将要在上面注册的组织。

在 defaultAccessControlPolicies.xml 中的方框之外，com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd 已定义为一个操作:

```
<Action Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"
   CommandName="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd">
 </Action>
```

它还包含于一个定义在 defaultAccessControlPolicies.xml XML 文件中的操作组中。

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

  <ActionGroupAction
        Name="com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd"/>
 </ActionGroup>
```

此操作组已在现有的引导策略中使用:

```
<Policy
   Name="MembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOnOrganizationResource"
   OwnerID="RootOrganization"
   UserGroup="MembershipAdministratorsForOrg"
   ActionGroupName="UserAdminRegistration"
   ResourceGroupName="OrganizationDataResourceGroup"
   PolicyType="groupableTemplate">

</Policy>
```

注: 许多策略是缺省策略，并在创建实例期间装入到数据库中。关于缺省策略的更多信息，请参阅第 185 页的『缺省访问控制策略和组』。

要将必需的角色添加到 UserRegistrationAdminAddCmd 中，请执行以下操作:

1. 将必需的角色添加到由策略使用的访问组。在本例中是 MembershipAdministratorsForOrg。

   此访问组是在 *WC_installdir*/xml/policies/xml/ACUserGroup_en_US.xml 中定义的，具体如下:

   ```
   <UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
      Description="Administrators of membership for the organization" MemberGroupID="-97"

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

   在上面的 XML 中，至少具有一个指定角色的用户被包括在内，这些指定的角色是 getResources() 返回的资源（组织）的所有者的上级组织的“买方管理员”或“卖方管理员”。如果想添加市场部经理角色，则必须增强它使其也包含新角色。

2. 将 XML 文件复制到 *WC_installdir*/xml/policies/xml。以下是 XML 的样式示例:

```
?xml version="1.0" encoding="UTF-8"?
<!DOCTYPE UserGroups SYSTEM "../dtd/ACUserGroups_en_US.dtd">

<UserGroups>

<UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
    Description="Administrators of membership for the organization" MemberGroupID="-97">

  <UserCondition><![CDATA[
     <profile>
    <orListConditio>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Buyer Administrator"/>
     <qualifier name="org" data="?"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Seller Administrator"/>
     <qualifier name="org" data="?"/>
      </simpleCondition>
      <simpleCondition>
        <variable name="role"/>
        <operator name="="/>
        <value data="Marketing Manager"/>
     <qualifier name="org" data="?"/>
      </simpleCondition>
   </orListCondition>
    </profile>
 ]]></UserCondition>
</UserGroup>

</UserGroups>
```

3. 使用 *WC_installdir*/bin/acpload 脚本，将 XML 文件装入到数据库中。关于装入 XML 文件的更多信息，请参阅第 149 页的『将更改装入数据库』。
4. 通过执行以下操作，在 WebSphere Commerce 管理控制台中更新访问控制策略注册表:
   a. 作为站点管理员登录到管理控制台。
   b. 单击**配置 > 注册表**。
   c. 从注册表列表中，选择**访问控制策略**。
   d. 单击**更新**。

保护资源

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 null 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:

- 新命令是从执行资源级别检查的基本 WebSphere Commerce 命令扩展而来的，并拥有资源级别策略，而且新命令与基本命令实现的界面不同。
- 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="groupableTemplate">
</Policy>
```

其中:

Name: 策略的名称。

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

OwnerID: 拥有策略的成员。

UserGroup: 策略适用于该组的用户。对于其中角色的作用域可动态地到达拥有资源的组织的访问组，其命名约定会将 ForOrg 附加到组名中

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 编程指南和教程*》。

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 null 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 编程指南和教程*》。

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"
   PolicyType="groupableStandard">
  </Policy>
```

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 表中的 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《*WebSphere Commerce 编程指南和教程*》。

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: 存储于 ACRESGRP 表的 GRPNAME 列中的资源组名称。

OwnerID: 资源组的所有者。它必须是根组织。

<ResourceCondition>: 指定将装入 ACRESGRP 表的 CONDITIONS 列的数据，以定义资源组。

<![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。在此例中则是，(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: 存储属性的资源表中的列名。

ResourceKeyColumnName: 存储主键的资源表中的列名。

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="Root Organization">
  <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:

aValue: 一个代表用户和资源之间的关系的字符串。该字符串应该是在资源的 fulfills 方法中检查过的关系之一。

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 aValue2 可能的值将包括 child，该值返回在成员层次结构中用户是其直接子女的组织实体。如果 aValue1 的值是 ROLE，则 aValue2 可能的值将包含 ROLE 表的 NAME 列中的任何有效条目，这些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，则这一部分的 RELATIONSHIP_CHAIN 得到满足。

注: 关于定义关系组的更多信息，请参阅第 135 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

如果需要构成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

作为 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_installdir*/xml/policies/xml/ACUserGroups_locale.xml。此文件遵循由 *WC_installdir*/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 表的 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 13. 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。 • OrgAndAncestorOrgs: 当它用在可分组的模板策略中时。这将检查该用户在拥有资源的组织或者其任何上级组织中是否具有指定的角色。

表 13. 支持的简单条件名称 (续)

变量名	描述	支持的运算符	支持的值	限定符	限定符值
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	指定用户是指定组织的子女。此信息是基于存储在 MBRREL 表中的数据的。	= !=	• ORGENTITY 表中 ORGENTITY_ID 列的任意值。 • ?: 它是否为可分组模板策略。这将检查该用户是否为拥有资源的组织的子女。它还将检查用户是否为任何资源所有者的上级的子女，一直到正在预定策略组的最近的上级并且包含该上级。	无	n/a

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，用户必须对于 ORGENTITY_ID = 100 的组织实体具有销售员角色。

```
<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特殊数据值 OrgAndAncestorOrgs 的角色 simpleCondition。此限定的数据值 OrgAndAncestorOrgs 仅工作于可分组的模板策略中。在此示例中，用户在拥有资源的组织或其任何上级中，必须具有销售经理、财务经理或销售员角色。

```
<UserCondition><!CDATA[
  <profile>
   <orListCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Sales Manager"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Account Representative"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Seller"/>
       <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </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，必须存在一条记录，其中用户是具有 ANCESTOR_ID = 100 和 SEQUENCE = 1 的组织的子代。

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

策略

WC_installdir/xml/policies/xml/defaultAccessControlPolicies.xml文件定义直接提供的缺省访问控制策略。此文件遵循由 *WC_installdir*/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 表的 POLICYNAME 列中。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 列中。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 表的 MBRGRPNAME 列中指定的访问组的名称。它装入到 ACPOLICY 表的 mbrgrp_id 列中。缺省的访问组定义在 *WC_installdir*/xml/policies/xml/ACUserGroups_language.xml 文件中。

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 表的 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 表的 GRPNAME 列中指定的资源组名称。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 groupableStandard 和 groupableTemplate。为了实现向后兼容性，也支持值 standard 和 template。如果装入新的策略时还未指定此属性，则将使用空值。如果更新现有策略时还未指定此属性，则其值保持不变。下表显示了字符串值到存储于 ACPOLICY 表的 POLICYTYPE 列的数据库值的映射。

表 14. 字符串值到数据库值的映射

String	ACPOLICY.POLICYTYPE
groupableTemplate	3
groupableStandard	2
template	1
standard	0 或空

关于策略类型的更多信息，请参阅第 15 页的第 3 章，『授权概念』。

RelationName（可选）: 在 ACRELATION 表的 RELATIONNAME 列中所指定的关系名称。如果指定了它，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 表的 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属于 AllUserCmdResourceGroup 资源组的一部分的控制器命令。

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

资源级别的策略:

对于命令: 在此示例中，属于 AllUsers 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="AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource"
   OwnerID="RootOrganization"
   UserGroup="AllUsers"
   ActionGroupName="CouponRedemption"
   ResourceGroupName="CouponWalletResourceGroup"
   RelationName="creator"
   PolicyType="groupableStandard">
</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"
   PolicyType="groupableStandard">
</Policy>
```

可分组模板策略: 在此示例中，属于

```
OrgAdminConsoleMembershipAdministratorsForOrg
```

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="OrgAdminConsoleMembershipAdministratorsForOrgExecuteApprove
GroupUpdateCommandsOnOrganizationResource"
   OwnerID="RootOrganization"
   UserGroup="OrgAdminConsoleMembershipAdministratorsForOrg"
   ActionGroupName="ApproveGroupUpdate"
   ResourceGroupName="OrganizationDataResourceGroup"
   PolicyType="groupableTemplate">
</Policy>
```

检查 OrgAdminConsoleMembershipAdministratorsForOrg 访问组的定义将显示以下成员资格条件:

```
<UserCondition>

 <profile>
    <orListCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Buyer Administrator"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
```

```
      <value data="Seller Administrator"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
     <simpleCondition>
      <variable name="role"/>
      <operator name="="/>
      <value data="Channel Manager"/>
      <qualifier name="org" data="OrgAndAncestorOrgs"/>
     </simpleCondition>
    </orListCondition>
   </profile>
  UserCondition>
```

注: role 的 simpleCondition 由 org = **OrgAndAncestorOrgs** 限定。OrgAndAncestorOrgs 是一个仅在可分组模板策略中可用的关键字。它动态地使得角色的作用域可达到当前资源的所有者的上下文。在此示例中，用户必须在拥有资源的组织或该组织的任何上级中具有指定的角色之一。

定义策略组

基于商务和访问控制要求，策略组创建到组策略中。一些缺省策略组创建于框外；关于更多信息，请参阅第 185 页的『缺省访问控制策略和组』。在发布商店或业务模型时，根据需要创建其它策略组。在大多数情况下，您可以简单地将任何您创建的新策略添加到现有策略组。如果需要创建新的策略组，您应该在类似 defaultAccessControlPolicies.xml 的 XML 文件中对其进行定义，然后将其装入到数据库。这里是样本定义:

```
<PolicyGroup Name="aValue" OwnerID="aValue">
 </PolicyGroup>
```

其中:

Name: 策略组的名称。

OwnerID: 拥有策略组的组织实体的成员标识。它将装入到 ACPOLGRP 表的 member_id 列中。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。

将策略与策略组进行关联

策略可以属于多个策略组。不过，为了便于对策略进行管理，建议一个策略仅属于一个策略组。此关联应定义于类似 defaultAccessControlPolicies.xml 的 XML 文件中，然后装入到数据库。这里是样本定义:

```
<PolicyGroup Name="aValue" OwnerID="aValue">
  <PolicyGroupPolicy  Name="aValue" PolicyOwnerID="aValue" />
</PolicyGroup>
```

其中:

PolicyGroupPolicy Name: 先前定义的与指定策略组相关联的策略的名称。此策略必须具有以下策略类型之一: groupableStandard 或 groupableTemplate。

PolicyGroupPolicy PolicyOwnerID（可选）: 拥有指定策略的组织实体的成员标识。如果未指定此参数，则缺省值为该策略组的 OwnerID。有两个特殊的值可以由转换程序工具来识别，它们是 RootOrganization: -2001 和 DefaultOrganization: -2000。

预订策略组

组织预订的策略组中的策略会保护该组织的资源。如果该组织未预订任何策略组，则应用该组织最近的上级预订的策略组。关于组织应预订哪些策略组的更多信息，请参阅第 185 页的『缺省访问控制策略和组』。

策略组预订可以在组织管理控制台中进行，但也可以定义于类似 defaultAccessControlPolicies.xml 的 XML 文件中，然后装入到数据库。这里是样本定义:

```
<PolicyGroup Name="aValue" OwnerID="aValue">
  <PolicyGroupSubscription OrganizationID="aValue"/>
 </PolicyGroup>
```

其中:

OrganizationID: 预订此策略组的组织实体的成员标识。有两个特殊的值可以由转换程序工具来识别，它们是 RootOrganization: -2001 和 DefaultOrganization: -2000。

可转换的策略数据

以下是可用来定义可转换策略数据的定制策略文件的模板:

```
 <?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>
 <PolicyGroup_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>
 <PolicyGroup>-->
<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_installdir\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。此值存储于 ACATTR 表的 ATTRNAME 列中。

DisplayName_nls: 属性的显示名称。此值存储于 ACATTRDESC 表的 DISPLAYNAME 列中。

Description_nls: 属性的可选描述。此值存储于 ACATTRDESC 表的 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。此值存储于 ACACTION 表的 ACTION 列中。

DisplayName_nls: 操作的显示名称。此值存储于 ACACTDESC 表的 DISPLAYNAME 列中。

Description_nls: 操作的可选描述。此值存储于 ACACTDESC 表的 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。此值存储于 ACRELATION 表的 RELATIONNAME 列中。

DisplayName_nls: 关系的显示名称。此值存储于 ACRELDESC 表的 DISPLAYNAME 列中。

Description_nls: 关系的可选描述。此值存储于 ACRELDESC 表的 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。此值存储于 ACRESCGRY 表的 RESCLASSNAME 列中。

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

Description_nls: 资源类别的可选描述。此值存储于 ACRSCGDES 表的 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。此值存储于 ACACTGRP 表的 GROUPNAME 列中。

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

Description_nls: 操作组的可选描述。此值存储于 ACACGPDESC 表的 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。此值存储于 ACRESGRP 表的 GRPNAME 列中。

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

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

策略: 以下示例定义了附加的策略信息:

```
<Policy_nls PolicyName="SiteAdministratorsCanDoEverything"
OwnerID="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。此值存储于 ACPOLICY 表的 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。此值存储于 ACPOLDESC 表的 DISPLAYNAME 列中。

Description_nls: 策略的可选描述。此值存储于 ACPOLDESC 表的 DESCRIPTION 列中。

策略组: 以下示例定义了附加的策略组信息:

```
<PolicyGroup_nls PolicyGroupName="B2CPolicyGroup" OwnerID="RootOrganization"
  DisplayName_nls="B2C Policy Group"
  Description_nls="This policy group contains all the B2C specific policies."
 />
```

其中:

PolicyGroupName: 正要向其添加附加信息的访问控制策略组的名称。此值可在 ACPOLGRP 表的 NAME 列中找到。

OwnerID: 拥有此策略组的组织实体的成员标识。

DisplayName_nls: 策略组的显示名称。此值存储于 ACPLGPDESC 表的 DISPLAYNAME 列中。

Description_nls: 策略组的可选描述。此值存储于 ACPLGPDESC 表的 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 88 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:

1. 如果创建已定制的 XML 文件，则需要将它们复制到 *<WC_installdir>*/xml/policies/xml 目录中，以将它们装入数据库。
2. 在装入脚本中有一项设置，该设置在解析标识和将数据装入到数据库中时，指定以下参数设置: "-maxerror 100000"。这意味着如果在装入数据时，发生的外键违例多达 100000 次将忽略它们，而不是异常中止。此值可根据需要增大或减小。例如，如果想要在发生一次这样的错误就停止，可将该值更改为 1。

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 *WC_installdir*/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 2000

1. 从目录 *<WC_installdir>*\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>*[*schema name*] **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>*[*schema name*] **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>*[*schema name*] **例如**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_zh_CN.xml
2. 检查 *<WC_installdir>*\logs 中的日志文件 **acugload.log**、**acpload.log** 和 **acpnlsload.log**，看是否存在任何错误。

对于 400 AIX Solaris Linux

该数据库用户标识必须拥有以下许可权，以继续执行以下步骤:

- 对 *WC_installdir*/xml/policies 和 *WC_installdir*/logs 的目录、子目录和文件的读 / 写 / 执行权限。
- 对 *WC_installdir*/bin 目录和其文件的读 / 执行权限。

如果数据库用户标识不具有以上必需的权限，则您需要使用 chmod 命令对他授予此权限。

1. 使用数据库用户标识登录。
2. 从目录 <*WC_installdir*>/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*>[*schema name*] **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*>[*schema name*] **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*>[*schema name*] **例如**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_zh_CN.xml

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

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

注: 对于 400 日志文件位于 *WC_userdir*/instances。

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。抽取实用程序使用输入过滤器 XML 文件来指定从数据库中抽取哪些数据。提供了以下过滤器文件:

- ACPoliciesfilter.xml: 用来抽取所有访问组和策略数据。
- ACUserGroupsFilter.xml: 用来抽取所有访问组数据。
- OrganizationPoliciesFilter.xml: 用来抽取特定组织的所有访问组和策略数据。在使用此文件之前，应该对其进行编辑，以指定必需的组织标识。将抽取此组织标识所拥有的策略数据。

对于 NT 2000

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

```
acpextract.cmd <database name> <database user> <database user password>
<input xml filter file> [schema name]
```

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_installdir>*\logs\acpextract.log 是否存在任何可能已发生的处理错误。

对于 400 AIX Solaris Linux

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

```
acpextract.sh <database name> <database user>
<database user password> <input xml filter file> [schema name]
```

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_installdir>*\logs\acpextract.log 是否存在任何可能已发生的处理错误。

对于 400

1. 以下文件通过使用 OUTDIR 参数创建于 *WC_installdir*/xml/policies/xml 目录中:
   - 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。

第 4 部分 支付安全性

本部分描述支付安全性管理任务。

第 14 章 WebSphere Commerce Payments 访问

WebSphere Commerce Payments 通过使用域认证用户。域是用户的注册表以及用于认证那些用户的一个方法（如用户名和密码）。每个 WebSphere Commerce Payments 安装一次只可以使用一个域。域类型的示例包括 LDAP 域和操作系统域。在授予用户访问资源的权限之前，必须将该用户定义在域中。因此，当且仅当用户满足以下两个条件，该用户才是有效 WebSphere Commerce Payments 用户:

- 在域中
- 在 WebSphere Commerce Payments 中分配了角色

WebSphere Commerce Payments 使用基于角色的访问控制方案，该方案定义了四个 WebSphere Commerce Payments 角色:

1. 支付管理员
2. 商家管理员
3. 主管
4. 职员

支付管理员可以使用 WebSphere Commerce Payments 用户界面“用户”窗口将访问权（基于角色）分配给域中定义的用户。WCSRealm 随 WebSphere Commerce Payments 提供。WCSRealm 类是为您的系统自动配置的。此域允许 WebSphere Commerce Payments Servlet 使用已在 WebSphere Commerce 用户表中注册的管理员信息。此管理员信息供支付管理员使用，因此您不必定义另一套管理员标识来使用 WebSphere Commerce Payments 用户界面。

第 15 章 维护 WebSphere Commerce Payments 安全性

WebSphere Commerce Payments 安全性是构建在几个关键安全性元素上的。这些元素组合在一起创建了一个可在 Web 上安全地部署服务的环境。

注: IBM WebSphere Commerce Payments（以下称为 WebSphere Commerce Payments）先前称为 Payment Manager。从版本 3.1.3 开始，已将支付应用程序重命名为 WebSphere Commerce Payments，并且在该文档中通篇更改了对该产品的引用。

保护 WebSphere Commerce Payments

WebSphere Commerce Payments 的中心是 Payment Servlet。几种辅助产品、配置了 WebSphere Application Server 的 Web 服务器、数据库和用户界面一起构成了整个 WebSphere Commerce Payments 框架。本章讨论保护各种 WebSphere Commerce Payments 组件的方法。

保护敏感数据

对于每个查询命令，该框架会对照该最小角色来验证用户的角色，并由此在 QueryRequest 对象中设置指示符，以指示是应以全视图方式返回诸如信用卡号码或开票地址之类的敏感数据还是应屏蔽掉敏感数据。WebSphere Commerce Payments 框架不维护可通过查询命令返回的任何敏感数据。但是，向卡匣记录器提供了用于检查该指示符的值以及以标准化方式屏蔽敏感数据的一些新方法。每个卡匣都必须将敏感数据与已存储数据的其余部分区分开来。通常，敏感数据就是卡匣在将数据存储到 WebSphere Commerce Payments 数据库之前加密的一组数据。

JVM 系统参数 `wpm.MinSensitiveAccessRole={clerk|supervisor|madmin|psadmin|none}` 指定了允许用户访问敏感数据所必须具备的最小角色。该值是区分大小写的。如果没有指定这个属性，则假定值 clerk，允许所有用户看到敏感数据。如果指定了无效值，则 Payment Servlet 无法初始化。

注意此参数可以在 Payments 实例创建期间设置，并可以使用 WebSphere Commerce 配置管理器在任何时候更新。配置管理器中的参数名称是 Payments 实例面板中的最小访问角色。关于配置管理器的面板的更多信息，请参阅针对您的平台的*《WebSphere Commerce 安装指南》*，或参阅配置管理器中 Payments 实例面板的联机帮助。

下表描述了支持的值（以权限的递增顺序列出）：

表 15. Payments 用户角色权限

用户	描述
clerk	具有职员（clerk）或更高角色的用户可以看到敏感数据。
supervisor	具有主管（supervisor）或更高角色的用户可以看到敏感数据。
madmin	具有商家管理员或更高角色的用户可以看到敏感数据。
psadmin	仅支付管理员可以看到敏感数据。

表 15. Payments 用户角色权限 (续)

none	不允许任何人看到敏感数据。

可以通过 WebSphere Commerce 配置管理器指定 `wpm.MinSensitiveAccessRole` 参数。

保护数据库

WebSphere Commerce Payments 数据库存储敏感数据，并要求受到不被未授权的源读和写的保护。WebSphere Commerce Payments 支持对存储在数据库中的敏感数据（如密码和持卡人信息）进行加密。

交易数据

下面是一些关于处理交易数据的准则。

- 敏感的交易信息存储在实例库的数据库表中。在“支付实例创建向导”中将这个库指定为“实例模式名称”。
- 应当保持所有备份的安全。
- 实例库中的数据库表包含关键的配置和交易信息，应当作为系统备份战略的一部分将其包含进来。您还应当备份以下内容:
  - `/QIBM/UserData/CommercePayments/V55/`*`instance`* 目录中的文件，其中 Instance 是 WebSphere Commerce Payments 实例的名称
  - 为 WebSphere Commerce Payments 配置的 HTTP 服务器实例。在“支付实例创建向导”中将这个 HTTP 服务器指定为 Web 服务器。
  - 本地机器上实例库中的对象以及使用远程数据库存储时远程机器上的数据库集合。

第 5 部分 各种安全性主题

本部分描述可由 WebSphere Commerce 系统管理员执行的各种安全性任务。

第 16 章 启用 WebSphere Application Server 安全性

本章描述了如何启用 WebSphere Application Server 的安全性。启用 WebSphere Application Server 安全性可防止任何人对任何 Enterprise JavaBeans 组件进行远程调用。

注:

1. Windows 如果 WebSphere Application Server 全局安全性是按本章的步骤中所概述的那样启用的，您将无法从 Windows 2000 “服务”面板正确地停止 WebSphere Application Server 服务器（例如，server1）。要在安全性启用时停止服务，请在命令提示符处使用 WAS_*installdir*\bin 目录下的 stopserver 命令。

   ```
   stopserver server -username user_id -password password
   ```

   其中 *server* 是您想要停止的服务器的 WebSphere Application Server 配置目录的名称（例如 server1），如果在服务器中启用了安全性，则 *user_id* 是要认证的用户名，*password* 是要认证的密码。

   当试图从“服务”面板停止服务器时，属性中将不包括用户标识和密码。启用全局安全性之后，在停止服务器时，用户标识和密码对于认证是必需的。服务继续运行（尽管“服务”面板显示它已停止）。注意，从“服务”面板启动服务时不需要用户标识和密码。

2. 在启用了 WebSphere Application Server 安全性的情况下，如果需要停止应用程序服务器，则在命令提示符中使用来自 WAS_*installdir*/bin 目录的 stopserver 命令，如下:

   AIX Linux Solaris

   ```
   stopserver server -username user_id -password password
   ```

   其中 *server* 是您想要停止的 WebSphere Application Server 应用程序服务器的名称（例如 server1），*user_id* 是要认证的用户名，*password* 是要认证的密码。

   400

   ```
   stopserver -instance WAS_instancename server -username user_id
      -password password
   ```

   其中 *WAS_instancename* 是 WebSphere Application Server 实例的名称，*server* 是您想要停止的 WebSphere Application Server 应用程序服务器的名称（例如 server1），*user_id* 是要认证的用户名，*password* 是要认证的密码。

3. AIX Linux Solaris Windows 启用 WebSphere Application Server 安全性时，强烈建议您的机器满足以下要求:

   - 机器内存至少为 1 GB。
   - 至少 384 MB 堆大小用于 WebSphere Commerce 应用程序。

开始之前

开始启用安全性之前，需要了解将启用安全性的 WebSphere Application Server 如何验证用户标识。WebSphere Application Server 可以使用 LDAP 或操作系统的用户注册表作为 WebSphere Application Server 用户注册表。

使用 LDAP 用户注册表时启用安全性

AIX Solaris Linux 要在将 LDAP 用作 WebSphere Application Server 用户注册表时启用 WebSphere Application Server 安全性，请作为 `wasuser` 标识登录到系统，并执行以下步骤。

400 要在将 LDAP 用作 WebSphere Application Server 用户注册表时启用 WebSphere Application Server 安全性，请登录到系统，并执行以下步骤。

Windows 要在将 LDAP 用作 WebSphere Application Server 用户注册表时启用 WebSphere Application Server 安全性，请作为具备管理权限的用户登录到系统，并执行以下步骤。

1. 启动 WebSphere Application Server 并打开 WebSphere Application Server 管理控制台。
2. 在管理控制台中，如下修改全局安全性设置:
   a. 在**安全性**下，展开**用户注册表**并单击 **LDAP**。根据正在使用的目录服务器的类型，如下填写**配置**选项卡中的字段:

表 16. IBM Directory Server 用户. AIX 400 Linux Solaris Windows

字段名	定义	样本值	注解
服务器用户标识	用户标识	*user_ID*	• 它不能是 LDAP 管理员。 • 请勿使用指定为 cn=xxx 的用户。 • 请确保此用户的对象类与 “LDAP 高级特性” 窗口中 “用户过滤器” 字段中指定的对象类兼容。
服务器用户密码	用户密码	*password*	
类型	LDAP 服务器类型	SecureWay	
主机	LDAP 服务器主机名	*hostname.domain.com*	
端口	LDAP 服务器正在使用的端口		此字段不是必需的。
基本专有名称	搜索所用的专有名称	o=ibm,c=us	
绑定专有名称	搜索时绑定到目录的专有名称		此字段不是必需的。
绑定密码	“绑定专有名称” 的密码		此字段不是必需的。

表 17. *Netscape 用户.* Windows

字段名	定义	样本值	注解
服务器用户标识	用户标识	*user_ID*	• 它不能是 LDAP 管理员。 • 请勿使用指定为 cn=xxx 的用户。 • 请确保此用户的对象类与“LDAP 高级特性”窗口中“用户过滤器”字段中指定的对象类兼容。
服务器用户密码	用户密码	*password*	
类型	LDAP 服务器类型	Netscape	
主机	LDAP 服务器主机名	*hostname.domain.com*	
端口	LDAP 服务器正在使用的端口		此字段不是必需的。
基本专有名称	搜索所用的专有名称	o=ibm	
绑定专有名称	搜索时绑定到目录的专有名称		此字段不是必需的。
绑定密码	“绑定专有名称”的密码		此字段不是必需的。

表 18. *Domino™ 用户.* Windows

字段名	定义	样本值	注解
服务器用户标识	简短名称 / 用户标识	*user_ID*	请确保此用户的对象类与“LDAP 高级特性”窗口中“用户过滤器”字段中指定的对象类兼容。
服务器用户密码	用户密码	*password*	
类型	LDAP 服务器类型	Domino 5.0	
主机	LDAP 服务器主机名	*hostname.domain.com*	
端口	LDAP 服务器正在使用的端口		此字段不是必需的。
基本专有名称	搜索所用的专有名称		此字段不是必需的。
绑定专有名称	搜索时绑定到目录的专有名称		此字段不是必需的。
绑定密码	“绑定专有名称”的密码		此字段不是必需的。

表 19. 活动目录（Active Directory）用户. Windows

字段名	定义	样本值	注解
服务器用户标识	sAMAccountName	*user_ID*	• 任意普通用户的用户登录名。 • 请勿使用指定为 cn=xxx 的用户。 • 请确保此用户的对象类与 “LDAP 高级特性” 窗口中 “用户过滤器” 字段中指定的对象类兼容。
服务器用户密码	用户密码	*password*	
类型	LDAP 服务器类型	Active Directory	
主机	LDAP 服务器主机名	*hostname.domain.com*	
端口	LDAP 服务器正在使用的端口		此字段不是必需的。
基本专有名称	搜索所用的专有名称	CN=users, DC=domain1, DC=domain2, DC=com	
绑定专有名称	搜索时绑定到目录的专有名称	CN=*user_ID*, CN=users, DC=domain1, DC=domain2, DC=com	*user_ID* 的值是显示名称。它并非必须与 “用户登录名” 相同。
绑定密码	“绑定专有名称” 的密码	*bind_password*	它应当与 “安全性服务器密码” 相同。

单击**应用**，然后单击**保存**。

b. 在管理控制台中，展开**安全性**并单击**全局安全性**。
   1) 在 “全局安全性配置” 选项卡中，选择**启用**并且不选择**强制 Java 2 安全性**。

      注: WebSphere Commerce 5.5 不支持 Java 2 安全性。
   2) 在 “活动的认证机制” 字段中，选择**轻量级第三方认证（LTPA）**。
   3) 在 “活动的用户注册表” 字段中，选择 **LDAP**。
   4) 单击**应用**，然后单击**保存**。

c. 在管理控制台中，展开**安全性**，然后展开**认证机制**并单击 **LTPA**。
   1) 在 “LPTA 配置” 选项卡中，按照需要填写 LTPA 设置。
   2) 如果不想使用此功能，则在 “附加属性” 下单击**单一注册（SSO）**，并且不选择**启用**复选框。
   3) 单击**应用**，然后单击**保存**。

d. 在管理控制台中，展开**应用程序**并单击**企业应用程序**。
   1) 在 “企业应用程序” 窗口中，单击您的 Commerce 应用程序 **WC**_*instance_name*（如 WC_demo）。

2) 在“附加属性”下，单击**映射安全性角色至用户 / 组**。

3) 单击**查找用户**，找到您要映射其角色的用户。

4) 针对该用户，选择 **WCSecurityRole** 并单击**确定**。

3. 关闭管理控制台，然后停止并重新启动 WebSphere Application Server 管理控制台。从现在开始，每当打开 WebSphere Application Server 管理控制台时，将提示您输入安全性服务器标识和密码。
4. 打开 WebSphere Commerce 配置管理器并选择**实例 > *instance_name* > 实例属性 > 安全性**并单击**启用**复选框。系统提示您输入在 第 164 页的2b 中输入的用户名和密码。单击**应用**，然后退出配置管理器。
5. 停止并重新启动 WebSphere Application Server 管理控制台。

使用操作系统用户注册表时启用安全性

AIX Linux Solaris 要将操作系统用作用户注册表，需要以 `root` 标识运行 WebSphere Application Server。作为 `root` 用户运行 WebSphere Application Server，并执行以下步骤。

400 Windows 要在将操作系统用户验证用作 WebSphere Application Server 用户注册表时启用 WebSphere Application Server 安全性，请作为具备管理权限的用户登录，并执行以下步骤。

1. AIX Linux Solaris 作为 root 用户登录。
2. AIX Linux Solaris 作为 `root` 用户登录时，启动 WebSphere Application Server 并启动 WebSphere Application Server 管理控制台。要启动服务器:

   ```
   cd WAS_installdir/bin
   ./startServer server
   ```

   其中 *server* 是 WebSphere Application Server 应用程序服务器的名称，例如 `server1`。
3. 在 WebSphere Application Server 管理控制台中，如下修改全局安全性设置:
   a. 在管理控制台中，展开**安全性**，然后展开**用户注册表**并单击**本地 OS**。针对您的安全注册表服务器，如下填写**配置**选项卡中的各字段:

字段名	样本值	注解
服务器用户标识	*wcsuser*	400 iSeries 上的用户标识应当具有 *SECOFR 权限。 AIX Solaris Linux 是 root 用户或拥有 root 权限的用户标识。 Windows 登录时使用的具备操作系统管理特权的用户标识。如果此机器属于某个域，请使用全限定用户标识。例如: *DomainXYZ\user_id*。请确保域服务器中存在此帐户，并且它是管理员组的成员。
安全性服务器密码	*password*	这是属于具有登录时所用的操作系统管理特权的用户的密码。

单击**应用**，然后单击**保存**。

b. 在管理控制台中，展开**安全性**并单击**全局安全性**。

1) 在“全局安全性配置”选项卡中，选择**启用**并不选择**强制 Java 2 安全性**。

2) 在“活动的认证机制”字段中，选择 **SWAM（简单 WebSphere 认证机制）**。

3) 在“活动的用户注册表”字段中，选择**本地 OS**。

4) 单击**应用**，然后单击**保存**。

4. 在管理控制台中，展开**应用程序**并单击**企业应用程序**。

a. 在“企业应用程序”窗口中，单击您的 Commerce 应用程序 **WC**_*instance_name*（如 WC_demo）。

b. 在“附加属性”下，单击**映射安全性角色至用户／组**。

c. 单击**查找用户**，找到您要映射其角色的用户。

d. 针对该用户，选择 **WCSecurityRole** 并单击**确定**。

5. 打开 WebSphere Commerce 配置管理器并选择**实例列表 → *instance_name* → 实例属性 → 安全性**并选择**启用安全性**复选框。选择**操作系统用户注册表**作为认证方式，并输入在步骤 第 165 页的 3a 中所输入的用户名和密码。单击**应用**，然后退出配置管理器。

6. 停止并重新启动 WebSphere Application Server 管理服务器。从现在开始，每当打开 WebSphere Application Server 管理控制台时，将提示您输入安全性服务器标识和密码。

禁用 WebSphere Commerce EJB 安全性

WebSphere Commerce Business Edition 允许禁用 EJB 安全性。要禁用 WebSphere Commerce EJB 安全性，请执行以下操作:

1. 启动 WebSphere Application Server 管理控制台。

2. 在管理控制台中，展开**安全性**并单击**全局安全性**。在“全局安全性配置”选项卡中，清除**启用**复选框。
3. 打开 WebSphere Commerce 配置管理器，并选择**实例列表 → *instance_name* → 实例属性 → 安全性**并清除**启用安全性**复选框。
4. 退出 WebSphere Application Server 管理控制台。
5. 停止并重新启动 WebSphere Application Server 管理服务器。

WebSphere Commerce 安全性部署选项

WebSphere Commerce 支持各种安全性部署配置。下表列举了对您可用的安全性部署选项。

表 20. 单机安全性方案

WebSphere Application Server 安全性已启用。	• 使用操作系统作为 WebSphere Application Server 注册表。 • 使用数据库作为 WebSphere Commerce 注册表。
	• 使用 LDAP 作为 WebSphere Application Server 注册表。 • 使用 LDAP 作为 WebSphere Commerce 注册表。
	• 使用 LDAP 作为 WebSphere Application Server 注册表。
WebSphere Application Server 安全性已禁用，WebSphere Commerce 站点位于防火墙后。	• WebSphere Application Server 注册表不是必需的。 • 使用数据库作为 WebSphere Commerce 注册表。
	• WebSphere Application Server 注册表不是必需的。 • 使用 LDAP 作为 WebSphere Commerce 注册表。

表 21. 多机安全性方案

WebSphere Application Server 安全性已启用。LDAP 始终是部署的。	• 使用 LDAP 作为 WebSphere Application Server 注册表。 • 使用 LDAP 作为 WebSphere Commerce 注册表。
	• 使用 LDAP 作为 WebSphere Application Server 注册表。 • 使用数据库作为 WebSphere Commerce 注册表。 • 您将需要设置 LDAP，并将一个管理条目放入 LDAP 注册表。

表 21. 多机安全性方案 (续)

WebSphere Application Server 安全性已禁用，WebSphere Commerce 站点位于防火墙后。	• 使用数据库作为 WebSphere Commerce 注册表。 • WebSphere Application Server 注册表不是必需的。 • 不支持单一注册。
	• 使用 LDAP 作为 WebSphere Application Server 注册表。 • WebSphere Application Server 注册表不是必需的。

注: 如果从防火墙后操作 WebSphere Commerce 站点，则可以禁用 WebSphere Application Server 安全性。如果您确定防火墙后没有运行任何恶意的应用程序，则应当只禁用 WebSphere Application Server 安全性。

动态高速缓存监视器的安全性配置

如果正在使用 WebSphere Application Server 动态高速缓存监视器来进行监视，且如果正在监视的应用程序的部署描述符中定义了安全性角色，则您需要执行以下操作:

浏览到 WebSphere Application Server 管理控制台中的“步骤: 映射安全性角色到用户／组”面板，单击**应用程序 —> 安装新的应用程序**，并完成必需的步骤（与非安全性相关）。（关于更多信息，请参阅 WebSphere Application Server 信息中心（`http://www.ibm.com/software/webservers/appserv/infocenter.html`）中的“Deploying secured applications”和“Assigning users and groups to roles”主题。在“步骤: 映射安全性角色到用户／组”面板中:

1. 指定映射到每个安全性角色的用户和组。
2. 按需要选择**角色**旁边的复选框，以选择所有角色或选择个别角色。对于每个角色，您可以指定预定义的用户（例如 Everyone 或 All Authenticated 用户）是否映射到该角色。要从用户注册表选择特定的用户或组:
   a. 选择一个角色，并单击**查找用户**或**查找组**。
   b. 在显示的**查找用户**或**查找组**面板上，输入搜索条件以从用户注册表中抽取一列用户或组。
   c. 从显示的结果中选择个别的用户或组。
   d. 单击**确定**将选择的用户或组映射到在“步骤: 映射安全性角色到用户／组”面板上选择的角色。

当前有一个已定义的角色，该角色提供对所有高速缓存监视器功能的访问权。这意味着这一页可用来指定哪些用户可以访问动态高速缓存监视器。

通过配置管理器管理 WebSphere Commerce 实例

如果启用了 WebSphere Application Server 全局安全性，您应该执行以下步骤，以便能使用配置管理器正确地停止、启动、创建或删除 WebSphere Commerce 或 WebSphere Commerce Payments 实例。

1. 在 *WAS_installdir*`/properties` 目录中，将以下文件和属性更新为以下值:

- sas.client.props

  com.ibm.CORBA.securityEnabled=true

  com.ibm.CORBA.loginSource=properties

  com.ibm.CORBA.LoginUserid=validUser

  com.ibm.CORBA.LoginPassword=validPassword

- soap.client.props

  com.ibm.SOAP.loginUserid=validUser

  com.ibm.SOAP.loginPassword=validPassword

  com.ibm.SOAP.secrityEnabled=true

2. 从 *WAS_installdir*/bin 目录运行 PropFilePasswordEncoder 命令（在一行上），以对 sas.client.props 和 soap.client.props 文件中的密码进行编码。

   AIX Linux Solaris

   ```
   PropFilePasswordEncoder.sh WAS_installdir/properties/
      sas.client.props com.ibm.CORBA.LoginPassword

   PropFilePasswordEncoder.sh WAS_installdir/properties/
      soap.client.props com.ibm.SOAP.loginPassword
   ```

   400

   ```
   PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
      sas.client.props com.ibm.CORBA.LoginPassword

   PropFilePasswordEncoder.sh WAS_userdir/WAS_instance/properties/
      soap.client.props com.ibm.SOAP.loginPassword
   ```

   Windows

   ```
   PropFilePasswordEncoder.bat WAS_installdir\properties\
      sas.client.props com.ibm.CORBA.LoginPassword

   PropFilePasswordEncoder.bat WAS_installdir\properties\
      soap.client.props com.ibm.SOAP.loginPassword
   ```

3. 更新 config_client 脚本:

   AIX 400 Linux Solaris 将 $CLIENTSOAP $CLIENTSAS 添加到 Java 参数列表中。例如:

   ```
   ${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
   -Djava.security.policy="config.policy" -Djava.version="1.3"
   -Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
   -Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME" $CLIENTSOAP $CLIENTSAS
   $PM_ARGS -Xmx128m com.ibm.commerce.config.client.CMClient "$@"
   ```

   Windows 将 %CLIENTSOAP% %CLIENTSAS% 添加到 Java 参数列表中。例如:

   ```
   "%JAVA_HOME%\bin\java" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS% "
   -Dwas.install.root=%WAS_HOME%" "-Dwas.repository.root=%CONFIG_ROOT%"
   -Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%
   -Djava.security.policy="config.policy"
   com.ibm.commerce.config.client.CMClient %*
   ```

4. 更新 config_server 脚本:

   AIX 400 Linux Solaris 将 $CLIENTSOAP $CLIENTSAS 添加到 Java 参数列表中。例如:

```
${JAVA_EXE?} -classpath $CLASSPATH -DIDIR="$WPMDIR"
-Djava.security.policy="config.policy"
-Dwas.install.root="$WAS_HOME " -Dwas.repository.root="$CONFIG_ROOT"
-Dws.ext.dirs="$WAS_EXT_DIRS" -Dcom.ibm.CORBA.BootstrapHost="$COMPUTERNAME"
$CLIENTSOAP $CLIENTSAS $PM_ARGS $MAX_HEAP
com.ibm.commerce.config.server.CMServerImpl "$@"
```

Windows 将 %CLIENTSOAP% %CLIENTSAS% 添加到 Java 参数列表中。例如:

```
"%JAVA_HOME%\bin\java.exe" %CLIENTSOAP% %CLIENTSAS% %PM_ARGS%
"-Dwas.install.root=%WAS_HOME%" "-Dwas.repository.root=%CONFIG_ROOT%"
"-Dws.ext.dirs=%WAS_EXT_DIRS%" -Dcom.ibm.CORBA.BootstrapHost=%COMPUTERNAME%
-Djava.security.policy="config.policy"
com.ibm.commerce.config.server.CMServerImpl %*
```

第 17 章 为 IBM HTTP Server 的生产启用 SSL

400 本部分不适用于 iSeries 平台。关于 iSeries 信息，请参阅第 177 页的『在 IBM HTTP Server（iSeries）上启用 SSL』。

用 IBM HTTP Server 创建 WebSphere Commerce 实例后，出于测试目的已启用了安全套接字层（SSL）。在对购物者开放站点之前，必须遵循本章中的步骤为生产启用 SSL。

关于安全性

IBM HTTP Server 通过使用加密技术，为业务交易提供一个安全的环境。加密是因特网上信息交易的编码，这样信息在由接收方解码前是无法读取的。发送方使用算法模式或者密钥对交易进行编码（加密），接收方使用解密密钥对交易解码。这些密钥由安全套接字层（SSL）协议使用。

Web 服务器使用认证过程来验证业务经营对象的身份，即确保他们符合自称的身份。认证包括：获取可信第三方（称为认证中心（CA））签署的证书。对于 IBM HTTP Server 用户，CA 可能是 Equifax® 或 VeriSign® Inc。也可用其它 CA。

要创建生产密钥文件，请完成以下步骤:

1. 配置用于生产的安全性密钥文件
2. 从认证中心请求安全证书。
3. 将生产密钥文件设置为当前密钥文件。
4. 接收证书并测试生产密钥文件。

下面将对这些步骤作详细描述。

注:

1. 如果已经在使用由认证中心签署的生产密钥文件，就可能可以跳过这些步骤。请阅读本章后再作决定。
2. 在执行这些步骤时，浏览器可能会显示安全性消息。请仔细复查每条消息中的信息并决定如何继续执行。

配置用于生产的安全性密钥文件

要配置用于生产的安全性密钥文件，请在 Web 服务器上执行以下操作:

1. 停止 IBM HTTP Server。
2. 将目录切换到机器的 IBM HTTP Server 安装目录下的 `conf` 子目录。
3. 创建 `httpd.conf` 的备份副本，并将文件的备份副本重命名为 `httpd.conf.backup`。
4. 在文本编辑器中打开 `httpd.conf`。
5. 请确保对端口 443 取消以下各行的注释（通过除去行首的 “#” ）:
   - Windows
     a. `LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll`

b. Listen 443

c. <VirtualHost *host.some_domain*.com:443>（您还必须在此行中替换全限定主机名。）

d. SSLEnable

e. </VirtualHost>

f. Keyfile "*HTTPServer_installdir*/ssl/keyfile.kdb"

- AIX Linux Solaris

a. LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so

b. AddModule mod_ibm_ssl.c

c. Listen 443

d. <VirtualHost *host.some_domain*.com:443>（您还必须在此行中替换全限定主机名。）

e. SSLEnable

f. </VirtualHost>

g. SSLDisable

h. 密钥文件 "*HTTPServer_installdir*/ssl/keyfile.kdb"

i. SSLV2Timeout 100

j. SSLV3Timeout 1000

6. 请确保取消以下各行的注释（通过除去行首的 "#" ）。

a. 对于 WebSphere Commerce 管理工具，需要端口 8000、8002 和 8004:

```
Listen 8000
Listen 8002
Listen 8004
```

如果正在使用 WebSphere Commerce Payments，则还需要端口 5432 和 5433:

```
Listen 5432
Listen 5433
```

b. 请确保还取消了对上述端口的虚拟主机部分的注释（通过除去行首的 "#" ，如果它们存在）。您必须在这些部分中适当地替换全限定主机名。关于下面示例中缺省路径名变量的列表，请参阅第 ix 页的『路径变量』。

下面的示例是从 Windows 系统的 httpd.conf 文件中取消注释的虚拟主机部分得到的；在其它操作系统上这些部分是相似的。

```
########## IBM WebSphere Payments (Do not edit this section) #################
Listen 5432
Listen 5433
########## End of IBM WebSphere Payments (Do not edit this section) ##########

...

########## IBM WebSphere Commerce (Do not edit this section) #################
Listen 8000
Listen 8002
Listen 8004
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
```

图 7. httpd.conf 文件的 “Listen” 部分的示例

```
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
## VirtualHost: Allows the daemon to respond to requests for more than one
## server address, if your server machine is configured to accept IP packets
## for multiple addresses. This can be accomplished with the ifconfig
## alias flag, or through kernel patches like VIF.
#
## Any httpd.conf or srm.conf directive may go into a VirtualHost command.
## See also the BindAddress entry.
#
#<VirtualHost host.some_domain.com:443>
```

图 8. httpd.conf 文件的虚拟主机头部分的示例

```
########## IBM WebSphere Payments (Do not edit this section) #################
<VirtualHost host.some_domain.com:5433>
SSLEnable
SSLClientAuth 0
ServerName wordsworth.torolab.ibm.com
DocumentRoot "HTTPServer_installdir\htdocs\en_US"
</VirtualHost>
########## End of IBM WebSphere Payments (Do not edit this section) ##########
```

图 9. Payments 的 httpd.conf 文件的虚拟主机部分的示例

```
########## IBM WebSphere Commerce (Do not edit this section) #################
#Instance name : instance_name
<VirtualHost host.some_domain.com:80>
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wcsstore  "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /wcs   "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
</VirtualHost>
```

图 10. 用于 WebSphere Commerce 端口 80 的 httpd.conf 文件的虚拟主机部分的示例. （未受保护的端口）

```
<VirtualHost host.some_domain.com:443>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wcsstore  "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /wcs   "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
</VirtualHost>
```

图 11. 用于 WebSphere Commerce 端口 443 的 httpd.conf 文件的虚拟主机部分的示例. （受保护的端口）

```
<VirtualHost host.some_domain.com:8000>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

图 12. 用于 WebSphere Commerce 端口 8000 的 httpd.conf 文件的虚拟主机部分的示例. （Websphere 贸易加速器）

```
<VirtualHost host.some_domain.com:8002>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

图 13. 用于 WebSphere Commerce 端口 8002 的 httpd.conf 文件的虚拟主机部分的示例. WebSphere Commerce管理控制台

```
<VirtualHost host.some_domain.com:8004>
SSLEnable
SSLClientAuth 0
ServerName host.some_domain.com
DocumentRoot "HTTPServer_installdir/htdocs/en_US"
Alias /wcsdoc   "WC_installdir/web/doc"
Alias /wchelp   "WC_installdir/web/doc/en_US"
Alias /adminconsole  "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "WAS_installdir\installedApps\host\WC_instance_name.ear/Stores.war"
Alias /accelerator  "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "WAS_installdir\installedApps\host\WC_instance_name.ear/CommerceAccelerator.war"
Alias /wcadmin  "WAS_installdir\installedApps\host\WC_instance_name.ear/SiteAdministration.war"
Alias /wcorgadmin  "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war"
Alias /orgadminconsole "WAS_installdir\installedApps\host\WC_instance_name.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
########## End of IBM WebSphere Commerce (Do not edit this section) ##########
```

图 14. 用于 WebSphere Commerce 端口 8004 的 httpd.conf 文件的虚拟主机部分的示例. WebSphere Commerce组织管理控制台

注: 建议防火墙软件阻拦对已为 WebSphere Commerce 工具配置的端口（缺省情况下是端口 8000、8002 和 8004）的外部访问。关于如何执行此操作的信息，请参阅正在站点上使用的防火墙软件的文档。

7. 保存更改。
8. 要确保 `httpd.conf` 文件不包含语法错误:

   AIX Linux Solaris 切换至机器的 IBM HTTP Server 安装目录下的 `bin` 子目录，并运行以下命令: `./httpd -t`

   Windows 切换至机器上的 IBM HTTP Server 安装目录，并运行以下命令:

   ```
   apache -t
   ```
9. 启动 IBM HTTP Server。

从认证中心请求安全证书

要验证您刚在前一步骤中创建的安全性密钥文件，需要来自认证中心（CA）（例如 Equifax 或 VeriSign）的证书。这一证书包含服务器的公用密钥、与服务器的证书相关联的专有名称，以及证书的序列号和失效日期。

如果希望使用另一个 CA，可直接与之联系，了解有关应当遵循的过程的信息。

Equifax 用户

要从 Equifax 请求安全服务器证书，请参阅以下 Web 地址并遵循提供的指示信息:

`http://www.equifax.com`

您应当在 2 到 4 个营业日内通过电子邮件接收到 Equifax 安全服务器证书。

VeriSign 用户

要从 VeriSign 请求安全服务器证书，请参阅以下 URL 并遵循提供的指示信息:

`http://www.verisign.com`

AIX 尽管您正在使用适用于 IBM HTTP Server 的过程，但还是请指向至**因特网连接安全服务器**（ICSS）的链接。遵循提供的指示信息。接收到证书时，请如前一部分中所述创建生产密钥文件（如果还未这样做的话）。

Solaris 尽管您正在使用适用于 IBM HTTP Server 的过程，但还是请指向至**因特网连接安全服务器**（ICSS）的链接。后面的页面将指出这些步骤适用于 OS/2® 和 AIX 平台。这些指示信息也适用于 Solaris 软件。

遵循提供的指示信息。提交请求后，您的证书就将在 3 至 5 个工作日内到达。当接收到证书时，请如前一部分中所述创建生产密钥文件（如果还未这样做的话）。

接收生产密钥文件并将其设置为当前密钥文件

从 CA 处得到证书之后，您必须让 Web 服务器使用您的生产密钥文件。请执行以下操作:

1. 将从认证中心接收到的 *certificatename*.kdb、*certificatename*.rdb 和 *certificatename*.sth 文件复制到机器的 IBM HTTP Server 安装路径下的 ssl 子目录中，其中 *certificatename* 是您随同证书请求提供的证书名称。
2. 停止 IBM HTTP Server。
3. AIX Solaris 通过运行以下命令导出 JAVA_HOME:

   ```
   DISPLAY=host_name:0.0
   export DISPLAY
   JAVA_HOME=java_home
   export JAVA_HOME
   ```

   其中 *host_name* 是当前使用的机器的全限定主机名，*java_home* 是:

   - AIX /usr/java130
   - Solaris /opt/WebSphere/AppServer/java131
4. 打开密钥管理实用程序（ikeyman）。
5. 打开 *certificatename*.kdb 文件，并在得到提示时输入密码。
6. 选择**个人证书**，并单击**接收**。
7. 单击**浏览**。
8. 选择存储从认证中心接收的文件的文件夹。选择 *certificatename*.txt 文件并单击**确定**。
9. **个人证书**列表框现在应当列出 VeriSign *certificatename* 证书或者 Equifax *certificatename* 证书。
10. 退出密钥管理实用程序。
11. 将目录切换至机器的 IBM HTTP Server 安装路径下的 conf 子目录。
12. 创建 httpd.conf 的备份副本。
13. 在文本编辑器中打开 httpd.conf。
14. 确保在第 171 页的 5中列出的行没有注释掉。
15. 搜索 Keyfile "*keyfile_path_name*/keyfile.kdb" 伪指令，并更改路径名称，使之指向在上述步骤中创建的文件。
16. 重新启动 IBM HTTP Server。

测试生产密钥文件

要测试生产密钥，请执行以下操作:

1. 在浏览器中转至以下 URL:

   `https://host_name`

   注:

   a. 如果您已经定制过 Web 服务器，则可能需要在主机名后面输入 Web 服务器首页的名字。

   b. 务必输入 `https`，*而不是* `http`。

   如果密钥是正确定义的，您将看到关于新证书的几条消息。

2. 如果希望接受此证书，则在**新建站点证书**面板上选择**永远接受此证书（直至过期）**单选按钮。

3. 从 Web 浏览器中将高速缓存和代理（或 socks）服务器设置恢复至原始状态。

现在，您已经在服务器上启用了 SSL。

用于 WebSphere Commerce Payments 的 SSL 注意事项

缺省情况下，WebSphere Commerce 和 WebSphere Commerce Payments 之间是通过 SSL 进行通信的。然而，如果如下直接启动 WebSphere Commerce Payments 用户界面，则正在使用非 SSL 通信调用 WebSphere Commerce Payments:

http://*host_name*:*port_number*/webapp/PaymentManager

其中 *host_name* 是 Payments 服务器名称，且 *port_number* 是 5432（缺省情况下）。

要确保通过 SSL 进行通信，使用以下 URL:

https://*host_name*:*port_number*/webapp/PaymentManager

其中 *host_name* 是 Payments 服务器名称，*port_number* 是 5433（缺省情况下）。

增强机密性

当 WebSphere Commerce 接收 URL 请求时，Web 控制器会检索请求的控制器命令的接口名称，并使用该名称从 CMDREG 表查找实现类名。它还会通过检查 URLREG 表中的 HTTPS 列确定 HTTPS（受保护的）协议对于该 URL 请求是否是必需的。

显示敏感信息的任何命令应当在 URLREG 表中将 HTTPS 值设置为值“1”（一）。例如，包含客户订单详细信息的 OrderProcessView 视图命令应当只在 HTTPS 协议上进行传送，因此 URLREG 表中的 OrderProcessView 条目在 HTTPS 列的值为“1”（一）。

在 IBM HTTP Server（iSeries）上启用 SSL

400 这一部分适用于 iSeries 平台。

SSL 是一个安全性协议。SSL 确保客户机和服务器之间传送的数据保持隐秘性。它让客户机能够认证服务器的身份，而让服务器能够认证客户机的身份。

数字证书是电子文档，它们认证因特网上的安全事务中所涉及的服务器和客户机。数字证书的发行者称为认证中心（CA）。iSeries 系统可在内部网环境中执行签发服务器和客户机证书的 CA 角色，并同时作为经过服务器证书（由 iSeries CA 或诸如 VeriSign 的因特网 CA 签发）认证的服务器运行。作为 Web 服务器，IBM HTTP Server for iSeries 也可配置为请求客户机证书以认证启用了 SSL 的客户机。

关于如何在 IBM HTTP Server for iSeries 上启用 SSL 的详细信息，请参阅 iSeries 信息中心（http://publib.boulder.ibm.com/html/as400/infocenter.html）。一旦登录该站点，请选择操作系统版本和语言，然后单击 **Go**。要获得关于如何启用 SSL 的指示信息，请搜索主题 “Securing applications with SSL”。

对 WebSphere Commerce Payments 使用 SSL

如果在创建 WebSphere Commerce 实例之后创建系统证书存储，则必须同时授予 WebSphere Commerce Payments 实例和 WebSphere Commerce 实例对系统证书存储的访问权。例如，以下命令将授予 WebSphere Commerce Payments 实例对 V5R1 系统的必要访问权:

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QPYMSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QPYMSVR) DTAAUT(*R)
```

而以下命令将授予 WebSphere Commerce 对 V5R1 系统的必要访问权:

```
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server') USER(QEJBSVR) DTAAUT(*RX)
CHGAUT OBJ('/QIBM/UserData/ICSS/Cert/Server/DEFAULT.KDB') USER(QEJBSVR) DTAAUT(*R)
```

如果选择使用远程 WebSphere Commerce Payments 实例，则必须同时将 WebSphere Commerce 实例和 WebSphere Commerce Payments 实例配置为信任签发数字证书的远程认证中心。要在两个远程应用程序之间建立信任关系，请参阅以下高级过程:

1. 在 WebSphere Commerce 机器上，使用 “数字证书管理器” 导出服务器的认证中心。
2. 将证书文件传送到 WebSphere Commerce Payments 机器。
3. 在 WebSphere Commerce Payments 机器上，使用 “数字证书管理器” 导入 WebSphere Commerce 服务器的认证中心。
4. 将 WebSphere Commerce Payments 应用程序服务器配置为信任导入的 WebSphere Commerce 服务器的认证中心。
5. 在 WebSphere Commerce Payments 机器上，使用 “数字证书管理器” 导出服务器的认证中心。
6. 将证书文件传送到 WebSphere Commerce 机器。
7. 在 WebSphere Commerce 机器上，使用 “数字证书管理器” 导入 WebSphere Commerce Payments 服务器的认证中心。
8. 将 WebSphere Commerce 应用程序服务器配置为信任导入的 WebSphere Commerce Payments 服务器的认证中心。

关于详细信息，请参阅以下 Web 地址，并查找
Hints and Tips: WebSphere Commerce 技术库 Web 页面
（http://www.software.ibm.com/software/commerce/wscom/library/lit-tech.html）

第 18 章 为 IBM Directory Server（LDAP）启用 SSL

以下是为 IBM Directory Server 和 WebSphere Commerce 配置 SSL 安全性的步骤。

设置 IBM Directory Server

400 本部分不适用于 iSeries 平台。关于 iSeries 信息，请参阅『在 iSeries 平台上安装 IBM OS/400 目录服务』。

要设置 IBM 目录服务器:

1. 按照 IBM Directory Server 安装说明来安装 IBM Directory Server。确保安装 GSKit 组件。
2. 安装完成后，运行 gsk5ikm 可执行文件调用 IBM 密钥管理器。
3. 创建新的 CMS 密钥数据库文件。确保选中了**将密码隐藏到文件中**（例如 `ldap_key.kdb`）。
4. 使用 X.509 版本和 1024 密钥大小来创建自签署证书。（您可以为证书指定有意义的标签，例如，您的名字。）
5. 使用 `Base64-encoded ASCII data` 数据类型抽取证书为证书文件（例如，`cert.arm`）。
6. 打开浏览器访问以下地址: `http://host_name/ldap` 其中 *host_name* 是 LDAP 服务器的名称。
7. 单击**安全性 —> SSL —> 设置**并作以下更改:
   - SSL 状态: SSL 打开或仅 SSL
   - 认证方法: 服务器认证
   - 安全端口: 636
   - 密钥数据库路径和文件名:

     AIX Linux Solaris `/Keys/ldap_key.kdb`

     Windows `drive:\Keys\ldap_key.kdb`
   - 密钥标号: *your_label*（证书的标号。）
   - 密钥密码: *xxxxx*（CMS 密钥数据库文件的密码）。如果选择“**将密码隐藏到文件**”，则不需要输入密码。）
8. 单击**更新**并重新启动 SecureWay。

在 iSeries 平台上安装 IBM OS/400 目录服务

400 要在 iSeries 上安装 IBM OS/400 目录服务:

1. 安装 IBM iSeries Access for Windows。
2. 通过选择**开始 —> 程序 —> IBM iSeries Access for Windows —> iSeries 导航器**，在 Windows 机器上启动 iSeries 导航器。
3. 如果不存在到目标 iSeries 机器的连接，则创建一个这样的连接。
4. 在左边面板扩展目标机器，然后扩展在左边面板的**网络 —>服务器**。

5. 单击在左边面板的 **TCP/IP**。
6. 用鼠标右键单击右边面板上的**目录**，并从弹出菜单中选择**属性**。
7. 在“目录属性”窗口，单击**网络**选项卡。
8. 单击**数字证书管理器**来启动数字证书管理器并把证书指定给“Directory Services 服务器”应用程序。
9. 在把证书指定给 Directory Services 服务器后，单击**确定**来关闭“目录属性”窗口
10. 重新打开“目录属性”窗口，您会看见安全套接字层（SSL）已启用。您可以接受缺省设置:
    - SSL 状态:
    - 认证方法: 服务器认证
    - 安全端口: 636
11. 重新启动 Directory Services 服务器。

将自签署证书指定并导入至 WebSphere Application Server

400 如果认证中心（CA），例如 VeriSign 或 Thwate 还没有向您发出 SSL 证书，那么您应该从 iSeries 机器导出本地 CA 并把它导入到 WebSphere Commerce 机器上的缺省信任 Keystore 中。要用 iSeries 本地证书启用 SSL 并将本地 CA 从 iSeries 机器导出，请执行以下操作:

1. 请确证 HTTP *Admin 服务器已启动。如果还未启动，请运行:

   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```

2. 通过启动浏览器使其指向以下地址: http://host name:2001/ 来打开“iSeries 任务”页面。
3. 选择**数字证书管理器**。
4. 单击**选择证书商店**。
5. 从证书商店，选择 ***System**。
6. 如果您没有看到**在您的 PC 上安装本地 CA 证书**链接，则您需要创建一个本地 CA:
   a. 单击“创建认证中心（CA）”。
   b. 在 iSeries 上重新启动 *Admin HTTP Server。
   c. 将新证书创建为客户机或服务器类型。
   d. 选择新创建的本地认证中心。
   e. 把该证书指定到 Directory Services 服务器。
7. 在您的 PC 上单击**安装本地 CA 证书**。
8. 单击“安装证书”。然后将证书（.cer 文件）保存在临时文件夹中。
9. 把认证中心（.cer 文件）导入 Microsoft Internet Explorer，然后再把认证中心导出到在临时目录下的 .cer 文件（二进制 64 位编码）中。
10. 把证书（二进制 64 编码）导入 WebSphere Application Server 信任 Keystore。例如:

    ```
    keytool -import -alias nck -file /temp_dir/nck.cer
            -keystore /qibm/proddata/java400/jdk13/lib/security/cacerts
    ```

WebSphere Application Server

在 WebSphere Application Server 中:

1. 启动随 WebSphere Application Server 提供的 IKeyMan（IBM 密钥管理器）。（您可以从 WebSphere Application Server 菜单或者直接在命令窗口输入 ikeyman 来找到它。）

   注: 此 IBM 密钥管理器与 SecureWay 提供的不同缺省密码是 “changeit”。

2. 打开 WebSphere Application Server carcerts Keystore（例如 Windows 上的 *WAS_installdir*\AppServer\java\jre\lib\security\cacerts）
3. 遍历到**签发者证书**，然后单击**添加**。使用 “**基于 64 位编码的 ASCII 数据**” 数据类型，然后选择您想要在步骤 第 179 页的 5 中创建的证书文件。
4. 输入证书名称。
5. 关闭 IKeyMan。

WebSphere Commerce

用设置 WebSphere Commerce 与 SecureWay Directory Server 一起工作，需要修改 *instance*.xml 文件:

1. 添加新 JNDI 环境变量:

   ```
   java.naming.security.protocol = ssl
   ```

2. 更改 LdapPort 为 “636”:

   ```
   LdapPort = 636
   ```

3. 重新启动 WebSphere Commerce。

以下是一个示例:

```
<MemberSubSystem name="Member SubSystem"
          AuthenticationMode="LDAP"
                     ProfileDataStorage="LDAP"

  <Directory LdapAdminDN="cn=root"
                 LdapAuthenticationMode="SIMPLE"
                 LdapTimeOut="0"
                 LdapVersion="3"
                 EntryFileName="E:/WebSphere/WPS/xml/ldap/attributeMap.xml"
                 LdapPort="636"
                 LdapAdminPW="<adminpassword>"
                 LdapHost="<hostname>"
                 MigrateUsersFromWCSdb="OFF"
                 JNDIEnvPropName1="java.naming.security.protocol"
                 JNDIEnvPropValue1="ssl"
                 display="false"
                 LdapType="SECUREWAY"

   . . . .

  />


</MemberSubSystem>
```

第 6 部分 附录

附录. 缺省访问控制策略和组

『附录』列出了随 WebSphere Commerce 提供的缺省策略和组。

缺省访问控制策略

缺省访问控制策略分组为以下类别:

- **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**: 根据业务区域分组的资源级别的策略。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** — 包含关于业务对象的信息。数据 bean 用于在 Web 页面上显示对象信息。

表 22. 何处找到关于策略的信息

策略	起始页
基于角色的策略	第 186 页的『基于角色的策略』
不同业务区域的资源级别策略	第 189 页的『不同业务区域的资源级别的策略』
订单	第 189 页的『订单』
贸易（合同）	第 190 页的『贸易（合同）』
核准	第 191 页的『核准』
拍卖	第 191 页的『拍卖』
商务智能	第 191 页的『商务智能』
成员资格	第 191 页的『成员资格』
市场营销	第 193 页的『市场营销』
产品目录	第 193 页的『产品目录』
连通性和通知	第 194 页的『连接性和通知』
采购	第 194 页的『采购』
赠券	第 194 页的『赠券』
客户概要信息	第 194 页的『客户概要文件』
折扣	第 194 页的『折扣』
已调度库存	
库存管理	
订单管理	第 195 页的『订单管理』
支付	第 196 页的『支付』
策略编辑器	第 196 页的『策略编辑器』
产品顾问	第 196 页的『产品顾问』
RFQ	第 196 页的『RFQ』
规则	第 197 页的『规则』
调度程序	第 197 页的『调度程序』
贸易加速器	第 197 页的『贸易加速器』

表 22. 何处找到关于策略的信息 (续)

策略	起始页
装运	第 197 页的『装运』
税务	第 198 页的『税务』
实时帮助 / 协作工作空间 / 客户关心	第 198 页的『实时帮助 / 协作工作空间 / 客户关心』
商店状态	第 198 页的『商店状态』
商店管理	

基于角色的策略

- SiteAdministratorsCanDoEverything
- BuyerAdministratorsExecuteBuyersAdministratorsCommands
- BuyerApproversExecuteBuyerApproversCmdResourceGroup
- GuestsExecuteGuestUsersCmdResourceGroup
- BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepCmdResourceGroup
- MarketingManagersExecuteMarketingManagerCmdResourceGroup
- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorCmdResourceGroup
- AccountRepresentativesExecuteAccountRepresentativesCmdResourceGroup
- SalesManagersExecuteSalesManagersCmdResourceGroup
- ProductManagersExecuteProductManagersCmdResourceGroup
- SellerAdministratorsExecuteSellerAdministratorsCommands
- SellersExecuteSellersCmdResourceGroup
- CategoryManagersExecuteCategoryManagersCmdResourceGroup
- Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup
- Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup
- PickPackersExecutePickPackersCmdResourceGroup
- ReceiversExecuteReceiversCmdResourceGroup
- ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
- OperationsManagersExecuteOperationsManagersCmdResourceGroup
- LogisticsManagersExecuteLogisticsManagersCmdResourceGroup
- ProcurementBuyersExecuteProcurementBuyersCmdResourceGroup
- CustomerServiceRepresentativesExecuteCustomerServiceRepresentativeViews
- BuyerAdministratorsExecuteBuyerAdministratorsViews
- BuyerApproversExecuteBuyerApproversViews
- MarketingManagersExecuteMarketingManagersViews
- CustomerServiceSupervisorsExecuteCustomerServiceSupervisorViews
- SalesManagersExecuteSalesManagersViews
- AccountRepresentativesExecuteAccountRepresentativesViews
- Buyers(buy-side)ExecuteBuyers(buy-side)Views

- Buyers(sell-side)ExecuteBuyers(sell-side)Views
- CategoryManagersExecuteCategoryManagersViews
- CustomersExecuteCustomersViews
- ProductManagersExecuteProductManagersViews
- PickPackersExecutePickPackersViews
- ReceiversExecuteReceiversViews
- ReturnsAdministratorsExecuteReturnsAdministratorsViews
- OperationsManagersExecuteOperationsManagersViews
- LogisticsManagersExecuteLogisticsManagersViews
- SellerAdministratorsExecuteSellerAdministratorsViews
- SellersExecuteSellersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersViews
- NonRejectedUsersExecuteNonRejectedUsersViews
- GuestUsersExecuteGuestUsersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersCommandsResourceGroup
- ChannelManagersExecuteChannelManagersCommands
- AllUsersExecuteAllSiteUserCmdResourceGroup
- AllUsersExecuteAllSiteUsersViews
- RegisteredCustomersForOrgExecuteRegisteredUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredUserViews
- ChannelManagersExecuteChannelManagersViews
- AllUsersExecuteResellerUserCmdResourceGroup
- AllUsersExecuteResellerUserViews
- RegisteredCustomersForOrgExecuteRegisteredResellerUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredResellerUserViews

下表按角色、访问组、资源组和视图显示基于角色的策略。

注:

1. 除**角色**列以外，由于表中的大多数项都很长，因此为便于显示而在每个单元格中将其分开。
2. 并不是所有下面的角色均是 WebSphere Commerce 中的已定义角色。关于定义的 WebSphere Commerce 角色的更多信息，请参阅第 25 页的『角色』。

表 23. 按角色、访问组、资源组和视图显示的基于角色的策略

角色	用于基于角色的策略中的访问组	用于控制器命令的基于角色的策略中的资源组	用于视图的基于角色的策略中的操作组
站点管理员	SiteAdministrators	n/a	n/a
买方管理员	BuyerAdministrators	BuyerAdministrators CommandsResource Group	BuyerAdministrators Views
买方核准员	BuyerApprovers	BuyerApproversCmd ResourceGroup	BuyerApproversViews

表 23. 按角色、访问组、资源组和视图显示的基于角色的策略 (续)

角色	用于基于角色的策略中的访问组	用于控制器命令的基于角色的策略中的资源组	用于视图的基于角色的策略中的操作组
来宾 [1]	Guests	GuestUsersCmd ResourceGroup	GuestUsersViews
客户服务代表	CustomerService Representatives	CustomerService RepCmdResourceGroup	CustomerService Representative Views
市场部经理	MarketingManagers	MarketingManager CmdResourceGroup	MarketingManagersViews
客户服务主管	CustomerService Supervisors	CustomerService Supervisor CmdResourceGroup	CustomerService SupervisorViews
客户代表	Account Representatives	AccountRepresentativesCmd ResourceGroup	AccountRepresentatives Views
销售经理	SalesManagers	SalesManagersCmd ResourceGroup	SalesManagersViews
产品经理	ProductManagers	ProductManagers CmdResourceGroup	ProductManagersViews
卖方管理员	Seller Administrators	SellerAdministrators CommandsResourceGroup	SellerAdministrators Views
卖方	Sellers	SellersCmdResourceGroup	SellersViews
类别经理	CategoryManagers	CategoryManagers CmdResourceGroup	CategoryManagersViews
买方（购买方）	Buyers(buy-side)	Buyers(buy-side) CommandsResourceGroup	Buyers(buy-side)Views
买方（销售方）	Buyers(sell-side)	Buyers(sell-side) CommandsResourceGroup	Buyers (sell-side)Views
提货装货员	PickPackers	PickPackersCmd ResourceGroup	PickPackersViews
收货员	Receivers	ReceiversCmdResourceGroup	ReceiversViews
退货管理员	ReturnsAdministrators	ReturnsAdministratorsCmd ResourceGroup	ReturnsAdministrators Views
业务经理	OperationsManagers	OperationsManagersCmd ResourceGroup	OperationsManagersViews
后勤部经理	LogisticsManagers	LogisticsManagersCmd ResourceGroup	LogisticsManagersViews
采购买方	ProcurementBuyers	ProcurementBuyersCmd ResourceGroup	n/a
注册核准用户 [2]	RegisteredApproved Users	RegisteredApprovedUsers CommandsResourceGroup	RegisteredApproved UsersViews
非拒绝用户 [3]	NonRejectedUsers	NonRejectedUserCommands ResourceGroup	NonRejectedUsersViews
渠道经理	ChannelManagers	ChannelManagersCmd ResourceGroup	ChannelManagersViews

表 23. 按角色、访问组、资源组和视图显示的基于角色的策略 (续)

角色	用于基于角色的策略中的访问组	用于控制器命令的基于角色的策略中的资源组	用于视图的基于角色的策略中的操作组
所有用户 [4]	AllUsers	ResellerUserCmd ResourceGroup[5]	ResellerUserViews[5]
		AllSiteUserCmd ResourceGroup[6]	AllSiteUsersViews[6]
注册客户（带有 OrgandAncestorOrgs 角色限定符）	Registered CustomersForOrg	RegisteredUserCmd ResourceGroup	RegisteredUserViews
		RegisteredResellerUser CmdResourceGroup	RegisteredReseller UserViews

注意:

1. “来宾”不是真正的角色。注册状态设置为 “G”（USER.REGISTERTYPE 列设置为 “G”）的用户隐式地属于 Guests 访问组。
2. “注册核准用户”不是真正的角色。注册状态设置为 “R”（USER.REGISTERTYPE 列设置为 “R”），且状态已核准（MEMBER.STATE 列设置为 1）的用户隐式地属于 RegisteredApprovedUsers 访问组。
3. “非拒绝用户”不是真正的角色。注册状态为非拒绝（MEMBER.STATE 列不是设置为 2）的用户隐式地属于 NonRejectedUsers 访问组。
4. “所有用户”不是真正的角色。系统中的所有用户均隐式地属于 AllUsers 访问组。
5. 这些操作组和资源组属于那些是 B2CPolicyGroup 的一部分的策略。此策略组很可能仅适用于遵循 B2C 业务模型的组织。
6. 这些操作组和资源组属于那些是 ManagementAndAdministrationPolicyGroup 的一部分的资源。此策略组很可能适用于所有组织。

不同业务区域的资源级别的策略

订单

数据资源: 订单:

- AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
- AllUsersExecuteOrderCreateCommandsOnStoreResource
- AllUsersExecuteOrderReadCommandsOnOrderResource
- AllUsersExecuteOrderPrepareCommandsOnOrderResource
- AllUsersExecuteOrderWriteCommandsOnOrderResource
- AllUsersExecuteScheduledOrderCancelOnOrderResource
- AllUsersExecuteReturnAgainstOrderOnOrderResource
- AllUsersExecuteOrderProcessOnOrderResource
- OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
- CustomerOrderManagersForOrgExecuteOrderProcessOnOrderResource
- ResellerAdministratorsForOrgExecuteOrderReadCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderPrepareCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteOrderWriteCommandsOnOrderDataResourceGroup
- ResellerAdministratorsForOrgExecuteScheduledOrderCancelOnOrderDataResourceGroup

- ResellerAdministratorsForOrgExecuteOrderProcessOnOrderDataResourceGroup
- EmailOrderNotificationManagersForOrgExecuteCustomerServiceEmailOrderOnOrderResource

数据资源: 需求列表:

- AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
- AllUsersExecuteRequisitionListSharedReadCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveReadCommandsOnPrivateRequisitionListResource
- AllUsersExecuteRequisitionListWriteCommandsOnRequisitionListResource
- AllUsersExecuteRequisitionListSharedProcessCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveProcessCommandsOnPrivateRequisitionListResource

数据资源: 兴趣商品:

- AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
- AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource

*数据资源: **RMA**:*

- AllUsersExecuteRMACreateCommandsOnStoreResource
- AllUsersExecuteRMAReadCommandsOnRMAResource
- AllUsersExecuteRMAPrepareOnRMAResource
- AllUsersExecuteRMAWriteCommandsOnRMAResource
- AllUsersExecuteRMAProcessCommandsOnRMAResource
- RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
- RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
- RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
- RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
- StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource

*数据 **bean**: 订单:*

- AllUsersDisplayOrderDatabeanResourceGroup
- AllUsersDisplayApprovalsOrderDataBeansResourceGroup
- AccountRepresentativesForOrgDisplayOrderDatabeanOnlyResourceGroup

*数据 **bean**: 需求列表:* AllUsersDisplaySharedRequisitionListDataBeansIfSameOrganizationalEntityAsCreator

*数据 **bean**: 兴趣商品:* AllUsersDisplayInterestItemDatabeanResourceGroup

*数据 **bean**: **RMA**:* AllUsersDisplayRMADatabeanResourceGroup

贸易（合同）

数据资源: 合同:

- ContractCreatorsForOrgExecuteContractCreateCommandsOnMemberResource
- ContractManagersForOrgExecuteContractManageCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource
- ContractViewersExecuteContractDisplayCommandsOnContractResource

- ContractOperatorsForOrgExecuteContractSubmitCommandsOnContractResource
- ContractManagersForOrgExecuteContractAccountManageCommandsOnAccountResource

数据资源: 业务策略:

- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyCreateCommandsOnStoreResource
- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyManageCommandsOnBusinessPolicyResource

数据资源: 商店创建: StoreCreatorsForOrgExecuteStoreCreationCommandsOnOrganizationResource

*数据 **bean**:* AccountHandlersForOrgDisplayTradingDatabeanResourceGroup

核准

数据资源:

- AllUsersExecuteApproveCommandsOnApprovalResource
- FlowAdministratorExecutesFlowAdminCreateCommandsOnStoreEntityResource
- FlowAdministratorExecutesFlowadminDeleteCommandsOnFlowadminResource

*数据 **bean**:* FlowAdministratorsForOrgDisplayFlowadminDatabean

拍卖

数据资源:

- AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
- AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
- AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionStyleManageCommandsOnAuctionStyleResource
- AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteBidControlRuleManageCommandsOnBidControlRuleResource
- RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteBidManageCommandsOnBidResources
- RegisteredApprovedUsersExecuteAutoBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteAutoBidManageCommandsOnAutoBidResources

*数据 **bean**:* AuctionDatabeanOwnersDisplayAuctionDatabeans

商务智能

数据资源:

- BusinessAnalystsForOrgExecuteViewContextListCommandsOnStoreEntityResource
- IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReportCommands OnStoreEntityResource

成员资格

数据资源: 用户:

- MembershipAdministratorsForOrgExecuteUserAdminUpdateCommandsOnUserResource

- GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteUserSelfRegistrationContinuationCommandsOnUserResource
- NonRejectedUsersExecuteNonRejectedUserCommands
- AllUsersDisplayUserDatabeanResourceGroup
- NonRejectedDisplayUserDatabeanResourceGroup

数据资源: 组织:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrgEntityPolicySubscription UpdateCommandsOnOrganizationResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteOrganizationManageActions OnOrganiztionResource
- CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommands OnOrganizationResource
- CSAMembershipAdministratorsExecuteUserAdminRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityRegistrationCommands OnOrganizationResource
- MembershipAdministratorsForOrgExecuteOrgEntityUpdateCommandsOnOrganizationResource GuestsExecuteResellerSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteResellerSelfRegistrationContinuationCommandsOnOrganizationResource
- ChannelManagersExecuteOrgEntityLockCommandsOnOrgResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteApproveGroupUpdateCommands OnOrganizationResource

数据资源: 成员组:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnUserResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnMemberGroupResource
- MemberGroupAdministratorsForOrgExecuteMemberGroupCreateCommandsOnMemberResource
- MemberGroupManagersForOrgExecuteMemberGroupManageCommandsOnMemberGroupResource

数据资源: 地址:

- NonRejectedUsersExecuteAddressManageCommandsOnUserResource
- MembershipAdministratorsForOrgExecuteAddressManageCommandsOnMemberResource

数据资源: 角色:

- MembershipAdministratorsForOrgExecuteRoleUnassignCommandsOnUserResource
- OrganizationRoleAdministratorsExecuteRoleManageCommandsOnOrganizationResource
- MembershipAdministratorsForOrgExecuteUserRoleAssignCommandsOnOrganizationResource

数据资源: 成员属性:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberAttributeCommands OnOrgResource
- AllUsersExecuteMemberAttributeCommandsOnUserResource

*数据 **bean**:*

- MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayOrganizationDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayUserDatabeanResourceGroup
- EmployeesDisplayOrganizationSpecificDatabeanResourceGroup

市场营销

数据资源: 竞销:

- CampaignManagersForOrgExecuteCampaignRelatedCreateCommandsOnStoreEntityResource
- CampaignManagersForOrgExecuteCampaignUpdateCommandsOnCampaignResource
- CampaignManagersForOrgExecuteInitiativeUpdateCommandsOnInitiativeResource
- CampaignManagersForOrgExecuteEMarketingSpotUpdateCommandsOnEMarketingSpotResource
- CampaignManagersForOrgExecuteCollateralUpdateCommandsOnCollateralResource

数据资源: 电子邮件活动:

- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnEmailActivity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivityDeleteCommandsOnEmailActivity DataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivityConfigurationSaveCommandsOnEmailActivityDataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroupAllUsersExecuteEmailOptOutDataResourceGroup

*数据 **bean**: 竞销:* CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

*数据 **bean**: 电子邮件活动:*

- EmailUserReceiveDataBeanPolicy
- EmailActivityDataBeanPolicy
- EmailConfigurationDataBeanPolicy

*数据 **bean**: 电子促销:* EpromotionDisplayDataBeanPolicy

产品目录

数据资源:

- CatalogManagersForOrgExecuteStoreCategoryManageCommandsOnCatalogResource
- CatalogManagersForOrgExecuteCatalogManageCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteCatalogGroupManageCommandsOnCatalogGroupResource
- CatalogEntryManagersForOrgExecuteStoreCatalogEntryManageCommandsOnStoreEntityResource
- CatalogGroupManagersForOrgExecuteProductSetAddCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteProductSetManageCommandsOnProductSetResource
- CatalogEntryManagersForOrgExecuteCatalogEntryManageCommandsOnCatalogEntryResource
- CatalogEntryManagersForOrgExecuteCatalogEntryRelationManageCommandsOnCatalogResource
- CatalogEntryManagersForOrgExecuteCatalogStoreManageCommandsOnStoreEntityResource

*数据 **bean**:*

- ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup
- CatalogGroupViewersForOrgDisplayCatalogGroupDataBeansResourceGroup
- CatalogListViewersForOrgDisplayCatalogListDataBeansResourceGroup

连接性和通知

数据资源:

- BackendOrderAdministratorsForOrgExecuteBackendOrderStatusCreateCommandsOnOrderDataResource
- BackendPickPackersForOrgExecuteBackendPickPackListCommandsOnFulfillmentCenterDataResource
- MessagingUpdateAdministratorsForOrgExecuteMessagingUpdateCommandsOnStoreEntityResource

采购

数据资源:

- ProcurementAdministratorsForOrgExecuteProcurementAuthenticationAndRegistration OnOrganizationResource
- ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource

赠券

数据资源:

- CouponAdministratorsForOrgExecuteCouponPromotionCreateCommandsOnStoreEntityResource
- CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommandsOnCouponPromotionResource
- AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
- AllUsersExecuteCouponDeleteCommandsOnCouponWalletResource
- CouponAdministratorsForOrgExecuteCouponPromotionUpdateCommandsOnStoreEntityResource
- AllUsersExecuteCouponSaveCommandsOnCouponWalletResource

*数据 **bean**:* CouponAdministratorsForOrgDisplayECouponPromotionBeans

客户概要文件

数据资源: CustomerProfileEditorsForOrgExecuteSegmentManageCommandsOnStoreEntityResource

*数据 **bean**:* CustomerProfileEditorsForOrgDisplaySegmentationDatabeansResourceGroup

折扣

数据资源:

- DiscountAdministratorsForOrgExecuteDiscountCreateCommandsOnStoreEntityResource
- DiscountAdministratorsForOrgExecuteDiscountDeployCommandsOnCalculationCodeResource
- DiscountAdministratorsForOrgExecuteDiscountAssociateCommandsOnCalculationCodeResource

*数据 **bean**:* DiscountViewersForOrgDisplayDiscountDatabeans

库存管理

数据资源:

- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterCreateCommandsOn OrganizationResource

- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManageCommandsOn FulfillmentCenterResource
- PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommandsOn FulfillmentCenterResource
- VendorInventoryManagersForOrgExecuteVendorManageCommandsOnVendorResource
- VendorInventoryManagersForOrgExecuteVendorCreateCommandsOnStoreEntityResource
- ExpectedInventoryManagersForOrgExecuteInventoryManageCommandsOnStoreEntityResource
- PickPackGeneratorsForOrgExecutePickPackGenerateCommandsOnFulfillmentCenterResource
- InventoryAdjustersForOrgExecuteInventoryAdjustCommandsOnStoreEntityResource
- ReturnReasonsManagersForOrgExecuteReturnReasonsCommandsOnStoreEntityResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterReleaseOnFulfillmentCenter ReleaseDataResourceGroup
- SharedFulfillmentCenterPickBatchInventoryManagersExecuteReleaseReadyShipCommands OnFulfillmentCenterDataResource
- SharedFulfillmentCenterPickPackGeneratorsExecutePickPackGenerateCommands OnFulfillmentCenterResource
- SharedFulfillmentCenterManagersExecuteFulfillmentCenterReleaseCommandsOnFulfillment CenterReleaseDataResourceGroup

*数据 **bean**:*

- ReturnReasonsManagersForOrgDisplayReturnReasonsOrderManagementDataBeansResourceGroup
- ExpectedInventoryManagersForOrgDisplayExpectedInventoryDataBeansResourceGroup
- VendorInventoryManagersForOrgDisplayVendorInventoryDataBeansResourceGroup
- ProductFindInventoryManagersForOrgDisplayProductFindInventoryDataBeansResourceGroup
- FulfillmentCenterManagersForOrgDisplayFulfillmentCenterDataBeansResourceGroup
- PickBatchInventoryManagersForOrgDisplayPickBatchInventoryDataBeansResourceGroup
- ReceiverOrderManagersForOrgDisplayReceiverOrderManagementDataBeansResourceGroup
- ReturnsAdminOrderManagersForOrgDisplayReturnsAdminOrderManagementDataBeans ResourceGroup
- SuperUserOrderManagersForOrgDisplaySuperUserOrderManagementDataBeans ResourceGroupFulfillmentManagersForOrgDisplayReleaseOrderItemsDatabeanResourceGroup

订单管理

数据资源:

- CustomerOrderManagersForOrgExecuteCustomerServiceOrderWriteCommands OnOrderResource
- CustomerOrderManagersForOrgExecuteCustomerServiceOrderCreateCommands OnStoreEntityResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnWriteCommands OnRMAResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnCreateCommands OnStoreEntityResource
- CustomerOrderManagersExecuteCustomerWriteCommandsOnUserResource
- CustomerOrderManagersForDefaultOrgExecuteCustomerServiceCustomerWriteCommandsOn UserDataResourceGroupwithGuestRegisterType

*数据 **bean**:*

- CustomerOrderManagersForOrgDisplayCustomerOrderManagementDatabeans
- MemberOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- MemberOrderManagersDisplayOrganizationSpecificDatabeans
- MemberOrderManagersDisplayUserDatabeanResourceGroup

- UserOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- UserOrderManagersDisplayOrganizationSpecificDatabeans
- UserOrderManagersDisplayUserDatabeanResourceGroup
- LogisticsManagersForOrgDisplayOrdersAndReturnsListsDatabeans
- ReturnsManagersForOrgDisplayReturnsListsDatabeans

支付

数据资源:

- AccountManagersForOrgExecuteAccountCreateCommandsOnOrganizationResource
- AccountAdministratorsForOrgExecuteAccountManageCommandsOnAccountResource
- AccountViewersForOrgExecutePaymentSummaryGenerateCommandsOnAccountResource
- AccountViewersForOrgExecuteStorePaymentAdminCommandsOnStoreEntityResource
- AllUsersExecutePaymentOrderWriteCommandsOnOrderResource

策略编辑器

数据资源:

- StoreAdministratorsForOrgExecuteACPolicyCreateCommandsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACPolicyEditCommandsOnACPolicyResource
- StoreAdministratorsForOrgExecuteACViewPoliciesForUpdateActionsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACViewApplicablePoliciesActionsOnOrganizationResource
- DescendantStoreAdministratorsExecuteACViewPoliciesForOrgActionsOnOrganizationResource

*数据 **bean**:* StoreAdministratorsForOrgExecuteUserGroupSearchViews

产品顾问

*数据 **bean**:*

- ProductAdvisorStatisticiansForOrgDisplayProductAdvisorStatisticsDatabeans
- SalesAssistantStatisticiansForOrgDisplaySalesAssistantStatisticsDatabeans
- ProductAdvisorManagersDisplayPAWCBEDatabeanResourceGroup
- GuidedSellManagersDisplayGSWCBEDatabeanResourceGroup

RFQ

数据资源:

- RFQBuyersExecuteRFQCreateCommandsOnStoreEntityDataResourceGroup
- RFQBuyersManageRFQResourcesTheyOwn
- RFQBuyersManageRFQResponsesForRFQsTheyOwn
- RFQAdministratorsAdministerRFQs
- RFQAdministratorsManageRFQResponses
- RFQSalesManagersForOrgCreateRFQResponse
- RFQSalesManagersExecuteRFQResponseManageCommandsOnRFQResponseResource
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQWithPublicAccess TypeResourceGroup

- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQResourceGroup

*数据 **bean**:*

- RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
- RFQBuyersDisplayRFQResponseDataBeansViewabletoRFQOwnerResourceGroup
- RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup
- RFQSalesViewersDisplayRFQDataBeanWithPublicAccessTypeResourceGroup
- RFQSalesViewersDisplayRFQDataBeanResourceGroup

规则

数据资源: StoreAdministratorsForOrgExecutePersonalizationRuleServiceAdministrationCommands OnStoreEntityResource

*数据 **bean**:* StoreAdministratorsForOrgDisplayPersonalizationRuleServiceAdministrationDataBeanResourceGroup

调度程序

数据资源:

- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnStoreEntityResource
- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnUserResource

*数据 **bean**:* StoreAdministratorsForOrgDisplaySchedulerDataBeansResourceGroup

贸易加速器

数据资源:

- B2CCSAViewUsersForOrgExecuteB2CCSAViewActionsOnStoreEntityResource
- B2BCSAViewUsersForOrgExecuteB2BCSAViewActionsOnStoreEntityResource
- CHSCSAViewUsersForOrgExecuteCHSCSAViewActionsOnStoreEntityResource
- RHSCSAViewUsersForOrgExecuteRHSCSAViewActionsOnStoreEntityResource
- CPSCSAViewUsersForOrgExecuteCPSCSAViewActionsOnStoreEntityResource
- RPSCSAViewUsersForOrgExecuteRPSCSAViewActionsOnStoreEntityResource
- HCPCSAViewUsersForOrgExecuteHCPCSAViewActionsOnStoreEntityResource
- MHSCSAViewUsersForOrgExecuteMHSCSAViewActionsOnStoreEntityResource
- MPSCSAViewUsersForOrgExecuteMPSCSAViewActionsOnStoreEntityResource
- SCPCSAViewUsersForOrgExecuteSCPCSAViewActionsOnStoreEntityResource
- SHSCSAViewUsersForOrgExecuteSHSCSAViewActionsOnStoreEntityResource
- SPSCSAViewUsersForOrgExecuteSPSCSAViewActionsOnStoreEntityResource

装运

数据资源: ShippingMembershipAdministratorsForOrgExecuteShippingManageCommandsOnStore DataResourceGroup

*数据 **bean**:* ShippingMembershipAdministratorsForOrgDisplayShippingDatabeanResourceGroup

税务

数据资源: TaxationAdministratorsForOrgExecuteTaxationManageCommandsOnStoreDataResourceGroup

*数据 **bean**:* TaxationAdministratorsForOrgDisplayTaxationDatabeanResourceGroup

实时帮助 / 协作工作空间 / 客户关心

数据资源: 实时帮助:

- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnUserDataResources
- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnOrderDataResources

数据资源: 客户关心:
CustomerCareAdministratorsForOrgExecuteCustomerCareQueueManageCommandsOnStoreResource

*数据 **bean**: 实时帮助:* LiveHelpAgentsForOrgDisplayCustomerCareDatabeanResourceGroup

*数据 **bean**: 协作工作空间*
: CollaborativeWorkspaceAdministratorsForOrgDisplayCollaborativeWorkspaceDatabeanResourceGroup

商店状态

数据资源:

- ChannelManagersExecuteStoreStateChangeCommandsOnStoreResource
- AdministrativeRolesForOrgExecuteStoreStateChangeCommandsOnStoreResource
- AdministratorsForOrgAccessStoreWithCloseOrSuspendStateResourceGroup
- AllUsersAccessStoreWithOpenStateResourceGroup

商店管理

数据资源: 报表交付:
ReportDeliveryManagersForOrgExecuteSetupReportDeliveryCommandsOnStoreDataResourceGroup

数据资源: 商店:

- StoreFrontManagersForOrgExecuteStoreFrontRelatedUpdateOnStoreEntityResource
- StoreProfileManagersForOrgExecuteStoreProfileRelatedUpdateOnStoreEntityResource

---

缺省访问控制策略组

随 WebSphere Commerce 一起提供的缺省访问控制策略组如下:

- 管理和经营策略组: 此策略组包含所有成员管理和商店经营策略。
- 临时购物者管理策略组: 此策略组包含所有与临时购物者管理相关的策略。
- 公共购物策略组: 此策略组包含所有对于消费者直销和 B2B 方案而言是公共的与购物相关的策略。
- B2C 策略组: 此策略组包含所有消费者直销特定的购物策略。
- B2B 策略组: 此策略组包含所有 B2B 特定的购物策略。

注: 管理和经营策略组是核心策略组，它通常应适用于所有组织。只要组织预订任何一个策略组，它都还应预订该策略组。对于拥有商店的组织，根据商店的类型，除要预订管理和经营策略组以外，它还应预订公共购物策略组、B2C 策略组和 B2B 策略组。临时购物者管理策略组只应由拥有临时购物者的组织预订，该组织是公共方案中的缺省组织。

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 代表咨询。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。

任何对此出版物中 IBM 许可程序的引用并非意在明示或暗示只能使用 IBM 的许可程序。任何不侵犯 IBM 的知识产权的同等功能的产品、程序或服务，都可以用来代替 IBM 的产品、程序或服务。在与其它产品结合使用时，除了那些由 IBM 明确指定的产品之外，其评估和验证均是用户的责任。

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:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

本条款不适用英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 可以随时对本资料中描述的产品和／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。那些 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:

IBM 中国公司上海分公司
Office of the Lab Director
8200 Warden Avenue
Markham, Ontario
L6G 1C7
Canada

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。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其它操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

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。

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。

此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，如与实际商业企业所使用的名称和地址相似，纯属巧合。

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。

版权许可

本信息包含用源语言表示的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下作全面测试。因此 IBM 不能担保或暗示这些程序的可靠性、可服务性或功能。用户如果是为了按照 IBM 应用程序编程接口开发、使用、经销或分发应用程序，则可以任何形式复制、修改和分发这些样本程序，而无须向 IBM 付费。

商标

IBM 徽标和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:

AIX	AS/400	DB2
@server	IBM	iSeries
OS/2	OS/400	SecureWay
WebSphere	400	

Domino 是 Lotus Development Corporation 在美国和 / 或其它国家或地区的商标。

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

Java、JavaBeans 和所有基于 Java 的商标是 Sun Microsystems, Inc. 在美国和其它国家或地区的商标或注册商标。

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。

中国印刷