IBM WebSphere Commerce

安全性指南

版本 5.4

IBM WebSphere Commerce

安全性指南

版本 5.4

注意:

在使用本资料及其支持的产品之前，请务必阅读第 97 页的『声明』中的一般信息。

第一版，第一修订版（2002 年 5 月）。

本版本适用于 IBM® WebSphere Commerce 版本 5.4 以及所有后续发行版和修订版，直至在新版本中另有声明为止。确认您正在使用本产品级别的正确版本。

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

IBM 欢迎您提出宝贵意见。您可以将意见通过以下任何一种方式发送给我们:

1. 发送电子邮件到下面列出的网络地址之一。如果需要答复，请在电子邮件中提供您完整的网络地址。

   因特网: torrcf@ca.ibm.com
   IBMLink: toribm（torrcf）

2. 如果通过传真，请使用以下传真号码:

   美国和加拿大: 416-448-6161
   其它国家或地区: (+1)-416-448-6161

3. 通过将邮件邮至以下地址:

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

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

目录

前言

本文档描述了 WebSphere Commerce 5.4 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。

请注意本指南中的许多部分是从 WebSphere Commerce 5.4 信息库中的其它文档（例如 WebSphere Commerce 5.4 联机帮助、《*WebSphere Commerce 5.4 安装指南*》和《*WebSphere Commerce 5.4 程序员指南*》）中得来的。具体而言:

- 第 11 页的第 3 章，『授权（访问控制）』中的信息在《*WebSphere Commerce 5.4 访问控制指南*》中也有记载。
- 第 33 页的第 4 章，『增强站点安全性』和第 53 页的第 6 章，『会话管理』中的信息在 WebSphere Commerce 5.4 联机帮助中也有记载。第 45 页的第 5 章，『启用 WebSphere Application Server 安全性』中的信息在《*WebSphere Commerce 5.4 安装指南*》中也有记载。
- 第 57 页的第 3 部分，『系统管理员安全性任务』中的信息在《*WebSphere Commerce 5.4 安装指南*》中也有记载。
- 第 75 页的第 4 部分，『WebSphere Commerce 开发者安全性任务』中的信息在《*WebSphere Commerce 5.4 程序员指南*》中也有记载。

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。

浏览本文档

本文档分为以下部分:

- 第 1 页的第 1 部分，『WebSphere Commerce 安全性模型』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 31 页的第 2 部分，『WebSphere Commerce 站点管理员安全性任务』讨论了关于站点安全性的 WebSphere Commerce 站点管理任务。任何执行关于站点安全性的站点管理任务的人员将对该部分内容感兴趣。

- 第 57 页的第 3 部分，『系统管理员安全性任务』讨论了关于系统安全性的 WebSphere Commerce 系统管理任务。任何执行系统管理任务且关心系统安全性的人员将对该部分内容感兴趣。
- 第 75 页的第 4 部分，『WebSphere Commerce 开发者安全性任务』从开发者的立场讨论了 WebSphere Commerce 访问控制。任何想要理解访问控制概念并且用代码实现访问控制策略的人员将对该部分内容感兴趣。

进行中的安全性评估

WebSphere Commerce 产品线正在持续地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 5.4 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 的安全性增强。在 WebSphere Commerce 商务版 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 5.4 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 中已经实现了新的访问控制框架。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 77 页的第 11 章，『访问控制』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。

- **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 33 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 5.4 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 33 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 33 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 33 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 33 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 33 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 33 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 33 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 33 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 WebSphere Commerce 5.4 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 中已经实现了新的访问控制框架。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 77 页的第 11 章，『访问控制』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。

WebSphere Commerce Suite 5.1 专业版中的安全性改进

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 5.4 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。通过遵循工业标准 J2EE 规范，WebSphere Commerce Suite 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 Suite 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 Suite 服务器将不启动。

会话管理

完全重写了 WebSphere Commerce Suite 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 12 位密钥，安全地加密了 WebSphere Commerce Suite 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 Suite 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 Suite 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 Suite 日志文件中。

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。当看到任何以下名称时，如下所述替换为您的系统值:

  host_name

  WebSphere Commerce Studio 机器的全限定主机名（例如 ibm.com 是全限定的）。

  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。

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

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

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

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

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

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

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

在何处查找更多信息

关于 WebSphere Commerce 5.4 产品的信息，请参阅以下 Web 站点:

- Business

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

- Professional

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

关于 Commerce Studio，专业开发者版 5.1 或较早版本的 WebSphere Commerce Studio 的信息，请参阅以下 Web 站点:

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

第 1 部分 WebSphere Commerce 安全性模型

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 5.4 系统密码的详细信息，请参阅第 59 页的第 7 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。根据对 WebSphere Commerce 资源的访问控制策略来确定授权。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 45 页的第 5 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。在第 77 页的第 11 章，『访问控制』中讨论了此过程。

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。

访问控制策略是描述授权哪个用户或用户组在您的站点上执行特定活动的规则。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 5.4 的访问控制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，审计跟踪用于记录顾客活动。审计跟踪记录顾客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 65 页的第 8 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 53 页的第 6 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。

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

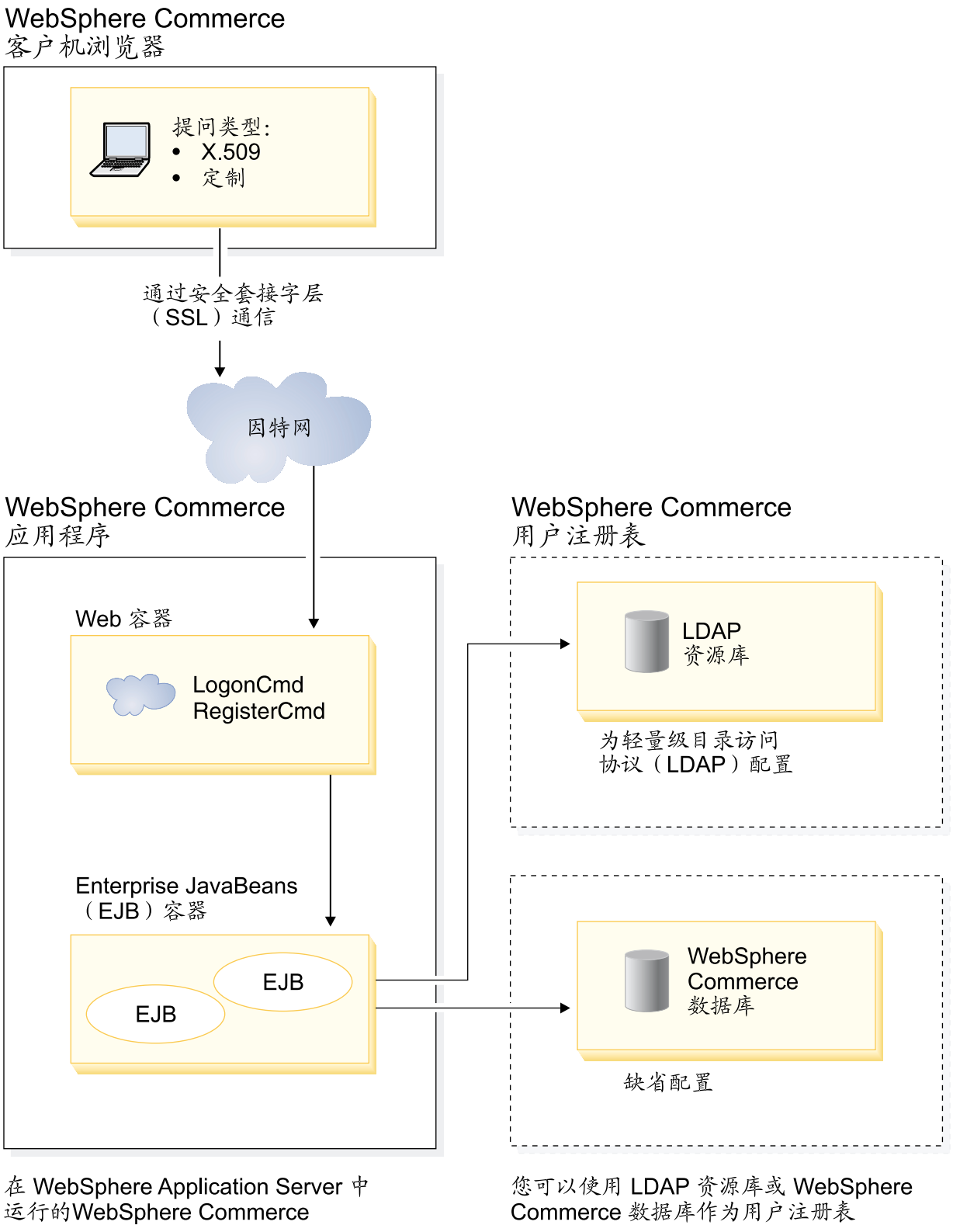


图 1. WebSphere Commerce 5.4 安全性模型

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 5.4 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 5.4 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 5.4 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 5.4 支持以下 LDAP 供应商:

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

凭证

WebSphere Commerce 5.4 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 ServerLTPA 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跨多个 HTTP 请求保留用户认证。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 73 页的第 10 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 5.4 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 41 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 43 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 42 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 36 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 37 页的『启用受密码保护的命令』。

会话策略

在 WebSphere Commerce 5.4 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 36 页的『启用登录超时』中对此作了详细描述。

第 3 章 授权（访问控制）

WebSphere Commerce 将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。为了理解 WebSphere Commerce 的访问控制组件，首先必须理解电子交易站点典型的组织层次结构。

组织层次结构

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

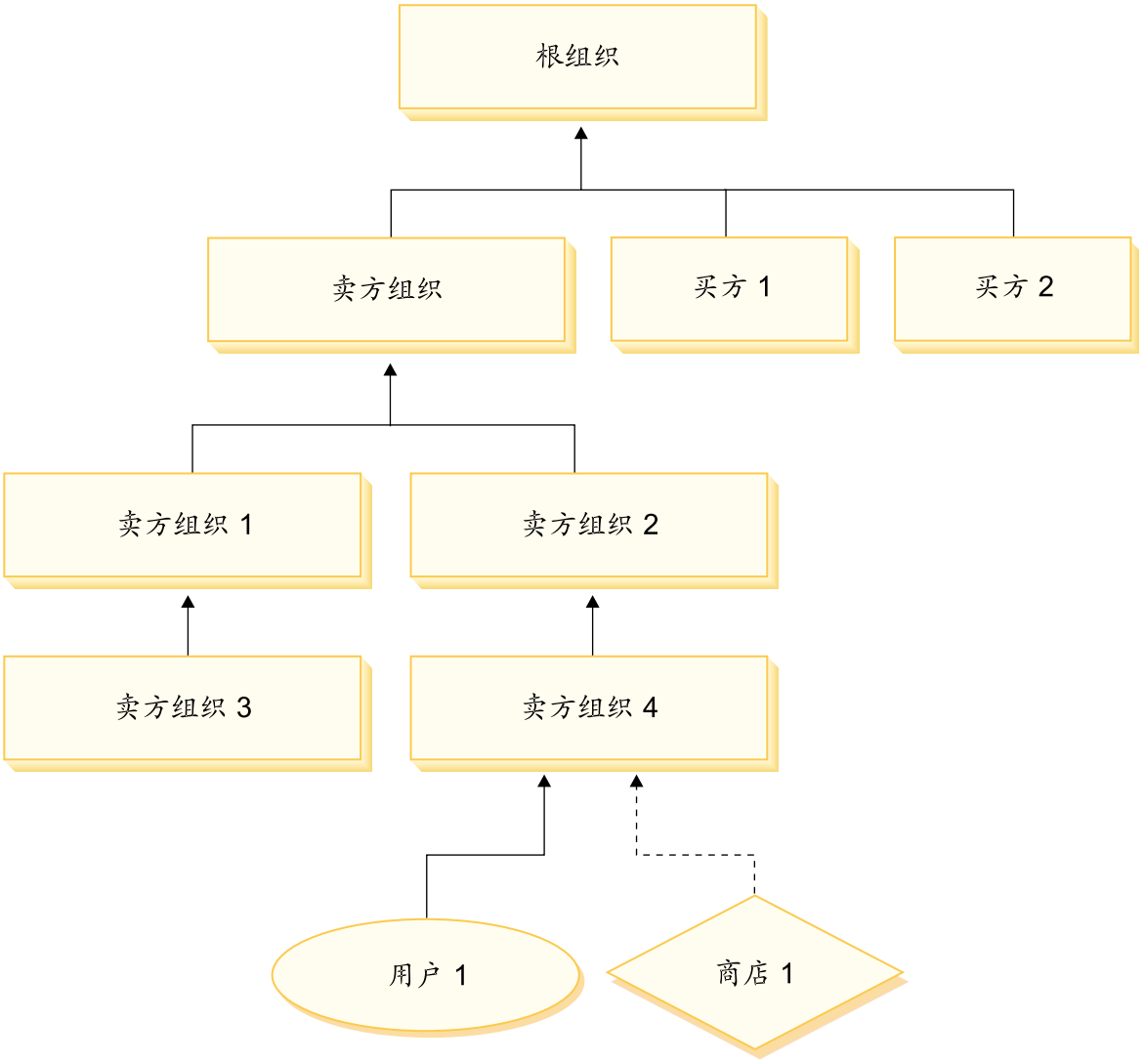


图 2. “商家到商家”站点的组织层次结构

根组织

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

注: 用户可以在其父组织之外的组织中担当角色。

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

组织（卖方）

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

卖方管理员的责任总结如下:

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

组织（买方）

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

买方管理员的责任总结如下:

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

注: 如有必要，站点管理员可修改和管理买方组织的访问控制策略。关于站点管理员任务的更多信息，请参阅第 14 页的『站点管理员』。

角色

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

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

注: 将角色指定给用户和组织是在 MBRROLE 表中完成的。

随 WebSphere Commerce 附带的缺省角色可分为以下类别:

- 站点操作
- 站点和内容开发
- 市场营销管理

- 产品管理
- 销售管理
- 后勤和运作管理
- 组织管理

站点操作

WebSphere Commerce 支持以下技术操作角色:

- 站点管理员
- 商店管理员

站点管理员

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

商店管理员

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

站点和内容开发

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

商店开发者

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

后勤和运作

WebSphere Commerce 支持以下后勤和操作管理角色:

- 后勤部经理
- 业务经理
- 收货员
- 退货管理员
- 提货装货员

后勤部经理

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

业务经理

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

提货装货员

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

收货员

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

退货管理员

退货管理员管理对退回产品的处理。

- 列出退货
- 列出退回产品
- 处理退回产品

产品管理

WebSphere Commerce 支持以下产品管理角色:

- 买方（销售方）
- 类别经理
- 产品经理或销售部经理

买方（销售方）

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

类别经理

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

产品经理 / 销售部经理

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

- 执行类别经理的所有任务
- 执行市场部经理的所有任务

销售管理

WebSphere Commerce 支持以下商务关系管理角色:

- 销售经理
- 客户代表
- 客户服务主管

- 客户服务代表

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

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

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

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

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

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

组织管理
WebSphere Commerce 支持以下组织管理角色:

- 卖方管理员
- 买方管理员
- 买方核准员

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

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

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

访问控制策略

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

访问控制策略的元素

访问控制策略由四个元素组成:

访问组 应用策略的一组用户。

操作组 由用户对资源执行的一组操作。

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

关系（可选）

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

访问控制策略概念

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

每个访问控制策略具有以下格式:

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

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

以下部分描述了与访问控制关联的概念性信息和术语。

成员组

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

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

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

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

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

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

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

操作

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

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

操作组

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

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

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

资源类别

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

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

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

资源

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

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

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

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

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

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

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

资源组

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

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

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

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

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

关系

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

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

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

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

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

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

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

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

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

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

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

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

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

注: 由带有单个参数元素的单个关系链所组成的关系组在功能上等价于简单关系。在此情况下，在策略中使用关系而不是关系组则更为方便。

资源和策略所有权

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

访问控制策略类型

有两种类型的访问控制策略:

- 标准策略
- 模板策略

标准策略

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

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

模板策略

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

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

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

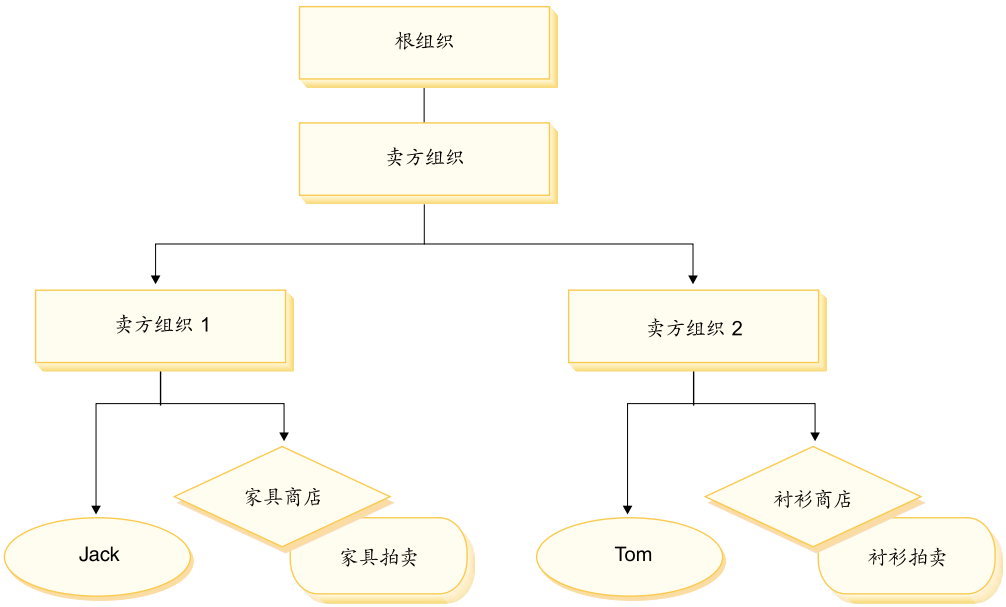
重设模板策略: 模板策略的另一个功能是: 对于指定的组织实体，他们可以重设。回到上面的示例，如果在 WebSphere Commerce 站点中添加了第 11 个组织实体，但这个最新的组织实体不希望上面的模板策略适用于它，则有一种方法可作此指定。必须在 ACORGPOL 表中添加一个条目，指定模板策略的策略标识和第 11 个组织的组织实体标识。这也可以通过 WebSphere Commerce 管理控制台，在商店管理员删除或更新模板策略时，在特定组织的上下文中完成。

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

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

访问控制级别

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



命令级别或基于角色的访问控制

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

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

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

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

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

实例级别或资源级别的访问控制

实例级别或资源级别的访问控制策略提供了细粒度的访问控制，确定了“谁可对哪些资源执行什么命令”。前面的基于角色的访问控制策略的示例允许卖方修改拍卖，可将它精细调整为资源级别的访问控制：卖方可修改对其担当该角色的组织所拥有的拍卖。在 23 中，Jack 具有卖方组织 1 的卖方角色，Tom 具有卖方组织 2 的卖方角色。Jack 在家具商店创建了家具拍卖。Tom 在衬衫商店创建衬衫拍卖。Jack 可修改家具拍卖，而*不能*修改衬衫拍卖。Tom 可修改衬衫拍卖，而*不能*修改家具拍卖。

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

资源级别访问控制适用于命令和数据 bean。

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

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

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

访问控制如何防止未授权的操作

本部分解释了基于策略的访问控制如何工作以确保用户仅可执行已授权的操作。

在执行用户启动的操作之前检查权限

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

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

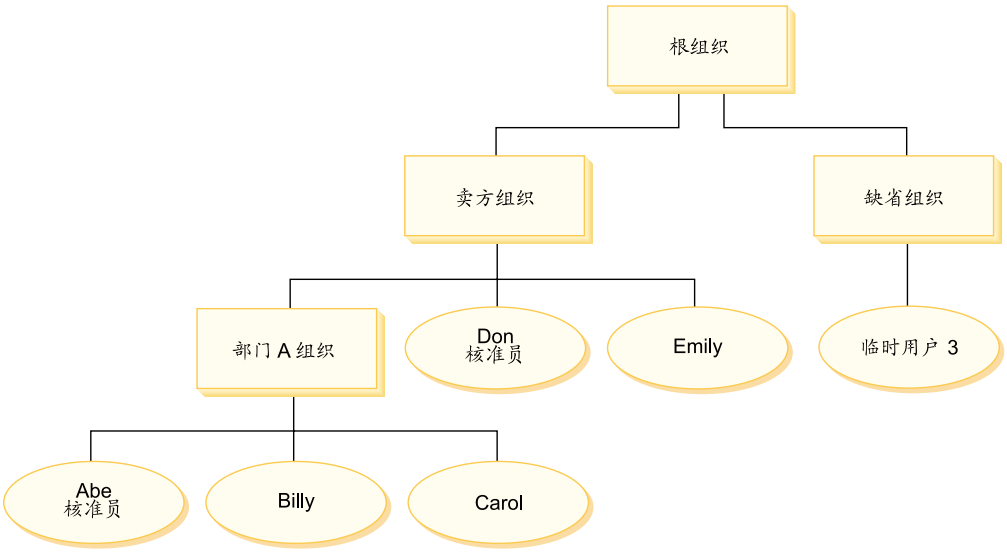
使用访问控制

关于任务（例如定制缺省访问控制策略、定制方案以及使用 XML 文件定制访问控制策略）的更多信息，请参阅《WebSphere Commerce 访问控制指南》。

评估访问控制策略

本部分可用作评估访问控制策略的指南。在本部分中，将向您展示一个方案，并通过一个如何评估标准访问控制策略和模板访问控制策略的示例对您作指导。每个部分都以对相关策略以及使用每个策略的方案的描述作为开头。关于标准策略和模板策略的更多信息，请参阅第 21 页的『访问控制策略类型』。

下图以图形方式显示了方案:



组织层次结构

从图中可看到站点中有以下四个组织:

- 根组织
- 卖方组织
- 缺省组织
- 部门 A 组织

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

用户

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

角色

Don 具有卖方组织的核准员角色。Abe 具有部门 A 组织的核准员角色。

访问组

以下访问组用于此方案:

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

文档

文档对象是受保护的资源。文档的所有者定义为在其中创建该文档的组织。

更新文档的访问控制需求

以下是更新文档的访问控制需求:

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

评估标准策略

本部分引导您完成标准策略以及评估这些策略的方案。

与更新文档相关的访问控制策略

以下是与更新文档相关的策略格式和访问控制策略:

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

策略 1:

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

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

策略 2:

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

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

策略 3:

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

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

策略 4:

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

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

方案

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

命令级别的检查:

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

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

资源级别的检查:

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

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

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

命令级别的检查:

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

资源级别的检查:

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

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

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

命令级别的检查:

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

资源级别的检查:

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

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

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

命令级别的检查:

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

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

资源级别的检查:

1. 因为命令级别的检查失败，因此根本不会执行资源级别的检查。

因为临时用户 3 未通过命令级别的检查，因此他不能更新他自己的文档。

评估模板策略

此示例基于前面的方案。

与更新文档相关的访问控制策略

当评估模板策略时，用于评估标准策略的访问控制策略 1 和 2 仍然适用，然而模板策略 5 现在取代了标准策略 3 和 4。关于策略 1 和 2 的更多信息，请参阅第 26 页的『评估标准策略』。

策略 5:

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

此策略是资源级别的模板策略。拥有文档的组织的核准员可更新文档。

还需要将用参数表示的新访问组用于此模板策略。将以下访问组添加到此方案:

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

方案

以下方案仅使用策略 1、2 和 5。

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

命令级别的检查:

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

资源级别的检查:

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

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

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

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

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

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

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

命令级别的检查:

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

资源级别的检查:

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

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

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

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

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

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

第 2 部分 WebSphere Commerce 站点管理员安全性任务

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

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 36 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 36 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 37 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 38 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 38 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 40 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 41 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 42 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 43 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 44 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

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『密码失效』）
- 受密码保护的命令（请参阅第 35 页的『受密码保护的命令』）
- 交叉站点脚本保护（请参阅第 36 页的『交叉站点脚本保护』）

关于创建视图以及开发商店前台的一般信息，请参阅《*商店开发者指南*》。

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 将用户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 1. 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 2. 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 3. 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 4. 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 5. 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 6. 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 7. 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 34 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、商店服务等），登录超时功能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. 从 WebSphere Application Server 管理控制台中，停止然后重新启动 WebSphere Commerce Server 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 34 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. 从 WebSphere Application Server 管理控制台中，停止然后重新启动 WebSphere Commerce Server 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 35 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**。所选择的命令将列出在“当前受密码保护的命令列表”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. 从 WebSphere Application Server 管理控制台中，停止然后重新启动 WebSphere Commerce Server 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”，更新给定实例的 WebSphere Commerce 数据库中的所有加密数据（例如，密码或信用卡号码）以及商家密钥。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，因此此选项不适用于 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. 从 WebSphere Application Server 管理控制台中，停止然后重新启动 WebSphere Commerce Server 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 36 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`
   - `&lt;SCRIPT`
   - `<%` 和 `&lt;%`

   .
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. 从 WebSphere Application Server 管理控制台中，停止然后重新启动 WebSphere Commerce Server 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（例如属性 txt）则不允许，则可以排除 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. 完成更新后，请保存 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。 本页列表所有现有帐户策略，包含任何缺省情况下随 WebSphere Commerce 提供的预定义帐户策略。 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。

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

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。本页列表所有现有密码策略，包含任何缺省情况下随 WebSphere Commerce 提供的预定义帐户策略。

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。

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

设置帐户锁定策略

WebSphere Commerce 管理控制台的“帐户锁定策略”允许您为 WebSphere Commerce 内的不同用户角色设置帐户锁定策略。 本页列表所有现有帐户锁定策略，包含任何缺省情况下随 WebSphere Commerce 提供的预定义帐户锁定策略。 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 iSeries 版。

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检查的安全性程序以及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 log 子目录的 sec_check.log 文件中:

NT *drive*:\WebSphere\Commerce\instances*instance_name*\log

2000 *drive*:\Program Files\WebSphere\Commerce\instances*instance_name*\log

AIX /usr/lpp/Commerce/instances/*instance_name*/log

Solaris /opt/WebSphere/Commerce/instances/*instance_name*/log

Linux /opt/WebSphere/Commerce/instances/*instance_name*/log

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 Administrators 组才对敏感文件具有读 / 写 / 执行权力:

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** 并取消选中表示“允许可继承的许可权....”的框
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。

第 5 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 安全性将使所有 Enterprise JavaBean 组件都免于受到任何人从远程调用。

注: Windows AIX Solaris Linux 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。

Windows AIX Solaris Linux 关于运行 WebSphere Application Server 安全性所必需的最新电子修订包的信息，请参考可从以下 WebSphere Commerce Web 站点获取的最新 WebSphere Commerce 5.4 自述文件文档:

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`

使用 LDAP 用户注册表时启用安全性

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。

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。

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` 登录到系统，并执行以下步骤。

1. 启动 WebSphere Application Server 管理服务器并打开 WebSphere Application Server 管理控制台。
2. 在控制台中按照如下步骤修改全局安全性设置:
   a. 从“控制台”菜单中，选择**安全性中心**。
   b. 在“常规”选项卡上，选择**启用安全性**。

c. 在**认证**选项卡上，选择“轻量级第三方认证（LTPA）”。填写 LTPA 设置，并取消选择**启用单一注册**复选框（如果您不希望使用此功能）。根据正在使用的目录服务器的类型，如下填写 **LDAP 设置**选项卡:

Windows AIX Solaris Linux 400

表 8. SecureWay 用户

字段名	定义	样本值	注解
安全性服务器标识	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。
安全性服务器密码	用户密码	*password*	
目录类型	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。

Windows

表 9. Netscape 用户

字段名	定义	样本值	注解
安全性服务器标识	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。
安全性服务器密码	用户密码	*password*	
目录类型	LDAP 服务器类型	Netscape	
主机	LDAP 服务器主机名	*hostname.domain.com*	

表 9. Netscape 用户 (续)

字段名	定义	样本值	注解
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。

Windows

表 10. Domino™ 用户

字段名	定义	样本值	注解
安全性服务器标识	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。
安全性服务器密码	用户密码	*password*	
目录类型	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。

Windows

表 11. 活动目录（Active Directory）用户

字段名	定义	样本值	注解
安全性服务器标识	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。
安全性服务器密码	用户密码	*password*	
目录类型	LDAP 服务器类型	Active Directory	

表 11. 活动目录（Active Directory）用户 (续)

字段名	定义	样本值	注解
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。

d. Windows 400 重新启动 WebSphere Application Server 管理服务器，然后重新打开 WebSphere Application Server 管理控制台。

e. 在**角色映射**选项卡上，选择 WCS 应用程序服务器并单击**编辑映射...**按钮。

1) 选择 WCSSecurityRole 并单击**选择...**按键。

2) 选中“选择用户／组”复选框并添加在第 46 页的2c中输入的用户标识。

f. 单击**完成**。

3. 关闭管理控制台，停止并重新启动 WebSphere Application Server 管理服务器。从现在开始，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 46 页的2c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 管理服务器。

使用操作系统用户注册表时启用安全性

Windows 400 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。

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

1. AIX Solaris Linux 作为 root 用户登录。

2. AIX Solaris Linux 当作为 root 用户登录时，启动 WebSphere Application Server 并启动 WebSphere Application Server 管理控制台。

```
export DISPLAY=fully_qualififed_host_name:0.0
cd WAS_HOME/bin
./startupServer.sh &
./adminclient.sh remote_WAS_host_name port
```

其中 *fully_qualififed_host_name* 是正在用来访问 WebSphere Application Server 管理控制台的计算机的名称，*remote_WAS_host_name* 是 WebSphere Application Server 的全限定主机名，port 是正在通过其访问 WebSphere Application Server 的端口（缺省端口是 2222）。

3. 在 WebSphere Application Server 管理控制台中，如下修改全局安全性设置:
   a. 从“控制台”菜单中，选择**安全性中心**。
   b. 在“常规”选项卡上，选择**启用安全性**复选框。
4. 选择**认证**选项卡并选择**本地操作系统**单选按钮。
5. 在**安全性服务器标识**字段中输入安全性服务器标识。如下输入用户名:

字段名	样本值	注解
用户标识	*user_ID*	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。 AIX Solaris Linux 系 root 用户或具备 root 用户权限的用户标识。 400 iSeries 上的用户标识应当具备 *SECOFR 权限。
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。

6. Windows 400 重新启动 WebSphere Application Server 管理服务器，然后重新打开 WebSphere Application Server 管理控制台。
7. 在**角色映射**选项卡上，选择 WC 企业应用程序并单击**编辑映射...**按钮。
   a. 选择 WCSecurityRole 并单击**选择...**按钮。
   b. 选中“选择用户/组”复选框，在“搜索”字段中输入步骤 5 中使用的用户标识，并单击**搜索**。从“可用的用户／组”列表中选择该用户并单击**添加**将其添加至“选定的用户／组”列表中。然后在每个面板上单击**确定**直到退出“安全性中心”。
8. 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 5 中所输入的用户名和密码。单击**应用**，然后退出配置管理器。
9. 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 商务版允许禁用 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. 单击**控制台 → 安全性中心...**并取消选择**常规**选项卡上的**启用安全性**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 12. 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 13. 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。
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。

第 6 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 将第一次尝试使用 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 基于小服务程序 HTTP 会话标准。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，请从位于以下地址的 WebSphere Application Server InfoCenter 中搜索“session management”：
  `http://www.ibm.com/software/webservers/appserv/infocenter.html`。

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

  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 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，顾客的浏览器是否接受 cookie。
   - Cookie 会话管理器

     选择是希望 WebSphere Commerce 还是希望 WebSphere Application Server 管理 cookie。缺省值是 WebSphere Commerce。
     - WebSphere Application Server 会话 cookie 基于小服务程序 HTTP 会话标准。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，请从位于以下地址的 WebSphere Application Server InfoCenter 中搜索“session management”：
       http://www.ibm.com/software/webservers/appserv/infocenter.html。
     - 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

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

     不能更改此字段。缺省值是当浏览器关闭时 cookie 失效。
   - Cookie 域

     通常不能更改此字段。指定一个域限制模式。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，且与 a.ibm.com 和 b.ibm.com 匹配，而不与 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. 从 WebSphere Application Server 管理控制台中，停止然后重新启动实例。

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。小服务程序引擎识别 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 高速缓存与 URL 重写不能协同工作。当 URL 重写打开时，需要禁用 WebSphere Commerce 高速缓存组件。

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. 从 WebSphere Application Server 管理控制台中，停止然后重新启动实例。

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。小服务程序引擎将 ;$jsessionid$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顾客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。如果顾客使用**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。

第 3 部分 系统管理员安全性任务

本部分描述通常可由站点的系统管理员（不必一定是 WebSphere Commerce 站点管理员）执行的安全性任务。

第 7 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。

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。

iSeries 用户简要表 400

在安装和配置 WebSphere Commerce 时经常使用和提及两个 iSeries 用户简要表:

- 您创建的用于安装 WebSphere Commerce 和访问配置管理器的用户简要表。要安装和配置 WebSphere Commerce，必须使用 USRCLS(*SECOFR) iSeries 用户简要表或使用 QSECOFR 用户简要表。如果需要创建用户简要表，请参阅 iSeries 版的《*WebSphere Commerce 5.4 安装指南*》。
- 在创建 WebSphere Commerce 实例时由配置管理器创建的用户简要表。此用户简要表也称为“实例用户简要表”。USRCLS(*USER) 用户简要表在每次创建 WebSphere Commerce 实例时由配置管理器创建。如果需要创建用户简要表，请参阅 iSeries 版的《*WebSphere Commerce 5.4 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`。

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

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

IBM HTTP Server 用户标识 Windows AIX Solaris Linux

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`*`:8000/adminconsole`

- 商店服务. 可以通过打开 Web 浏览器并输入以下 Web 地址访问您的“商店服务”页面。

  `https://`*`host_name`*`:8000/storeservices`

缺省的实例管理员用户标识是 `wcsadmin`，缺省密码是 `wcsadmin`。

注: 切勿除去 `wcsadmin` 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。

Payment Manager 管理员

当安装 Payment Manager 时，WebSphere Commerce 管理员标识 wcsadmin 自动指定为 Payment Manager 管理员角色。请遵循《*WebSphere Commerce 5.4 安装指南*》中的指导将 Payment Manager 域类切换为 WCSRealm（如果尚未完成此步骤）。

Payment Manager 管理员角色使用户标识能够控制和管理 Payment Manager 。

注意: 400

- 不要删除或重命名登录用户标识 wcsadmin，也不要更改预先指定的 wcsadmin 的 Payment Manager 角色，否则将导致与 Payment Manager 集成相关的 WebSphere Commerce 功能失效。
- 如果将 Payment Manager 角色指定给 WebSphere Commerce 管理员，而后又希望删除或重命名此管理员的登录用户标识，则必须在删除或重命名该用户标识前除去管理员的 Payment Manager 角色。

重要信息

Payment Manager 已经为其它两个管理标识预先指定 Payment Manager 管理员角色:

- ncadmin
- admin

要防止用户无意间获取此 Payment Manager 管理员角色，可以:

1. 使用 WebSphere Commerce 管理控制台在 WebSphere Commerce 中创建以上管理标识。
2. 在 Payment Manager 用户界面上，选择**用户**。
3. 除去这两个管理标识的 Payment Manager 管理员角色。

还应知道启动、停止或删除 Payment Manager 实例所需的 Payment Manager 实例密码。还需要它向 Payment Manager 实例添加卡匣。如果 Payment Manager 实例是由 WebSphere Commerce 配置管理器创建的，则 Payment Manager 实例密码与 WebSphere Commerce 实例登录密码（也称为实例用户简要表密码）相同。如果 Payment Manager 实例是从 iSeries 会话使用 **CRTPYMMGR** 命令创建的，或是从 iSeries 任务页面创建的，则将提示您提供密码。

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。

Windows AIX Solaris Linux 或者，要更改配置管理器用户标识或密码，请切换至 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:

```
config_env
java com.ibm.commerce.config.server.PasswordChecker -action [action type]
   -pwfile [password file] -userid [user ID]
   -password [userid password] [-newpassword [new userid password]]
```

其中，操作类型是 Add、Check、Delete 或 Modify。参数说明如下:

pwfile

指向存储密码的文件的路径。缺省路径是 WebSphere Commerce 安装路径下的 bin 子目录。 此参数总是必需的。

userid

输入希望添加、检查、删除或修改的用户标识。此参数总是必需的。

password

输入希望创建、检查、删除或修改的密码。此参数必须与 userid 参数一起使用。此参数总是必需的。

newpassword

使用此参数来更改特定用户标识的密码。此参数必须与 userid 和 password 参数一起使用。当指定操作类型是 Modify 时，此参数是必需的。

设置 IBM HTTP Server 管理员密码

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

1. 切换至机器上的 IBM HTTP Server 安装目录。
2. 输入以下命令:

   Windows `htpasswd -b conf\admin.passwd` *`user password`*

   AIX Solaris Linux `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。

更改 SSL 密钥文件密码

Windows AIX Solaris Linux 如果您正在使用 IBM HTTP Server，请遵循下面的步骤更改 SSL 密钥文件密码。

1. Windows 单击**开始菜单 → 程序 → IBM HTTP Server → 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 65 页的第 8 章，『为 IBM HTTP Server 的生产启用 SSL』中概括的指导创建新的密钥文件。
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 加密密码

Windows AIX Solaris Linux WebSphere Commerce 允许生成加密密码。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_password.bat` *password SALT merchant_key*

   AIX Solaris Linux `./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 命令。请参阅 F1 联机帮助以获取运行此命令的详细信息。

生成 Payment Manager 加密密码

WebSphere Commerce 允许生成 Payment Manager 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 Solaris Linux `./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。

400 对于 iSeries，要生成 Payment Manager 的加密密码，请使用 CRTWCSPMPW 命令。请参阅 F1 联机帮助以获取运行此命令的详细信息。

第 8 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 68 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. 创建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。

创建用于生产的安全性密钥文件

要创建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 安装子目录下的 `conf` 子目录。
3. 创建 `httpd.conf` 的备份副本。
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:
   - Windows

```
#LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
#Listen 443#Listen 443#<VirtualHost host.some_domain.com:443>
#SSLEnable
#</VirtualHost>
#SSLDisableKeyfile "drive:/WebSphere/HTTPServer/ssl/keyfile.kdb"
#SSLV2Timeout 100
#</VirtualHost>
#SSLDisable
```

- AIX Solaris Linux

```
#LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
#AddModule mod_ibm_ssl.c
#Listen 443#<VirtualHost host.some_domain.com:443>
#SSLEnable
#</VirtualHost>
#SSLDisableKeyfile "keyfile"
#SSLV2Timeout 100
#</VirtualHost>
#SSLDisable
```

其中 *keyfile* 是以下一项:

AIX `/usr/HTTPServer/ssl/keyfile.kdb`

Solaris `/opt/IBMHTTPD/ssl/keyfile.kdb`

Linux `/opt/IBMHTTPServer/ssl/keyfile.kdb`

6. 请确保对端口 8000 取消以下各行的注释:
   a. `#Listen 8000`
   b. `#<VirtualHost host.some_domain.com:8000>`. 您还必须在此行中替换全限定主机名。
   c. `#SSLEnable`
   d. `#</VirtualHost>`

   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）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，请切换至机器的 IBM HTTP Server 安装目录下的 `bin` 子目录，并运行以下命令:

   AIX Solaris Linux `./apachectl configtest`

   Windows `apachectl configtest`
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导:

`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 并遵循提供的指导:

`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。遵循提供的指导。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。这些指导也适用于 Solaris 软件。

遵循提供的指导。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）。

接收并设置生产密钥文件为当前密钥文件

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. 打开密钥管理实用程序。
3. 打开 *certificatename*.kdb 文件，并在得到提示时输入密码。
4. 选择**个人证书**，并单击**接收**。
5. 单击**浏览**。
6. 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**。
7. **个人证书**列表框现在应当列出 VeriSign *certificatename* 证书或者 Equifax *certificatename* 证书。
8. 退出密钥管理实用程序。
9. 将目录切换至机器的 IBM HTTP Server 安装路径下的 conf 子目录。
10. 创建 httpd.conf 的备份副本。
11. 在文本编辑器中打开 httpd.conf。
12. 确保在第 65 页的5中列出的行没有注释掉。
13. 搜索 Keyfile "*keyfile path name*" 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。
14. 停止并重新启动 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 Payment Manager 的 SSL 注意事项

缺省情况下，WebSphere Commerce 和 Payment Manager 之间是通过 SSL 进行通信的。然而，如果如下直接启动 Payment Manager 用户界面:

http://*host_name*/webapp/Paymentmanager/

则是使用非 SSL 的通信调用 Payment Manager 。要确保通过 SSL 进行通信，应当使用

https://*host_name*/webapp/Paymentmanager/

或者在以下目录中，将 `indexSSL.html` 文件重命名为 `index.html`:

- Windows *WAS_HOME*\installedApps\IBM_PaymentManager.ear\PaymentManager.war
- AIX Solaris Linux

  WAS_HOME/installedApps/IBM_PaymentManager.ear/PaymentManager.war

以此方式，可继续使用 **http**://*host_name*/webapp/Paymentmanager/ 目录，且重命名后的 `index.html` 将重定向到 `https`（SSL）。

在 IBM HTTP Server（iSeries）上启用 SSL

400 本部分适用于 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 iSeries 版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 iSeries 版上启用 SSL 的详细信息，请参阅以下 Web 地址:

```
www.ibm.com/software/webservers/commerce/servers/lit-tech-os400.html
```

特别地，请查看 **Hints and Tips** 部分。

对 Payment Manager 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 Payment Manager 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 Payment Manager 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 Payment Manager 实例，则必须同时将 WebSphere Commerce 实例和 Payment Manager 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 Payment Manager 机器上。
3. 在 Payment Manager 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 Payment Manager 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 Payment Manager 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 机器上。
7. 在 WebSphere Commerce 机器上，使用“数字证书管理器”导入 Payment Manager 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 Payment Manager 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**:

```
www.ibm.com/software/webservers/commerce/servers/lit-tech-os400.html
```

第 9 章 为 IBM SecureWay Directory Server（LDAP）启用 SSL

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

设置 SecureWay

要设置 IBM SecureWay Directory Server:

1. 按照 SecureWay Directory Server 产品安装说明，安装 IBM SecureWay Directory Server。确保安装 GSKit 组件。
2. 安装完成后，调用 IBM Key Manager（在 Windows 上是 *drive*:\Program Files\IBM\GSK4\bin\gsk4ikm.exe）。
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. 创建自签署证书
5. 将证书抽取为以 Base64 为编码的 ASCII 数据数据类型。
6. 创建新的 SSLight 密钥数据库类（例如 keyring.class）。
7. 在 **Singer 证书**部分中，添加在步骤 5 中创建的证书文件。
8. 将浏览器打开为以下地址: http://hostname/ldap
9. 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 Solaris Linux /Keys/ldap_key.kdb

     Windows *drive*:\Keys\ldap_key.kdb
   - 密钥标号: *your_label*（证书的标号）
10. 单击**更新**并重新启动 SecureWay。

WebSphere Commerce

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

```
java.naming.security.ssl.keyring = keyring
'keyring' is the name of the SSLight key database class (keyring.class)
This class file should put in the class path in WAS.

java.naming.security.ssl.authentication = ibm
'ibm' is the password specified when create the SSLight key database class.

java.naming.security.protocol = ssl
LdapPort = 636
```

```
<MemberSubSystem name="Member SubSystem"
                     ProfileDataStorage="LDAP"
                     AuthenticationMode="LDAP">
  <Directory LdapAdminDN="cn=root"
                 LdapAuthenticationMode="SIMPLE"
                 LdapTimeOut="0"
                 LdapVersion="3"
                 EntryFileName="WC_Install_Dir/xml/ldap/ldapentry.xml"
                 LdapPort="636"
                 SingleSignOn="0"
                 LdapAdminPW="EaDPFd9VAf0="
                 LdapHost="yazhuang.torolab.ibm.com"
                 MigrateUsersFromWCSdb="ON"
                 JNDIEnvPropName1="java.naming.security.ssl.keyring"
                 JNDIEnvPropValue1="keyring"
                 JNDIEnvPropName2="java.naming.security.ssl.authentication"
                 JNDIEnvPropValue2="ibm"
                 JNDIEnvPropName3="java.naming.security.protocol"
                 JNDIEnvPropValue3="ssl"
                 display="false"
                 LdapType="SECUREWAY" />
</Membersubsystem>
```

重新启动 WebSphere Commerce。

第 10 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《*IBM WebSphere Commerce 版本 5.4 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 45 页的第 5 章，『启用 WebSphere Application Server 安全性』。

启用单一注册

限制

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` 并确保在 LDAP 组件中用户的迁移状态为 “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 信息中心中搜索 “single sing-on”，可以从以下地址获得:

   ```
   http://www.ibm.com/software/webservers/appserv/doc/v40/ae
   /infocenter/index.html
   ```

   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. 展开 **WebSphere Commerce** → *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. 重新启动 WebSphere Application Server。

第 4 部分 WebSphere Commerce 开发者安全性任务

本部分描述与 WebSphere Commerce 编程相关的安全性任务。这些任务通常由 WebSphere Commerce 程序员执行。

第 11 章 访问控制

理解访问控制

WebSphere Commerce 应用程序的访问控制模型有三个主要概念: 用户、操作和资源。用户是使用系统的人。资源是在应用程序中得到维护或由应用程序维护的实体。例如，资源可以是产品、文档或订单。代表人员的用户简要表也是资源。操作是用户可对资源执行的活动。访问控制是确定给定用户是否可对给定资源执行给定操作的电子交易应用程序组件。

在 WebSphere Commerce 应用程序中，访问控制有两个主要级别。访问控制的第一个级别是由 WebSphere Application Server 执行的。对此，WebSphere Commerce 使用 WebSphere Application Server 来保护企业 bean 和小服务程序。访问控制的第二个级别是 WebSphere Commerce 细粒度访问控制系统。

WebSphere Commerce 访问控制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。该访问控制框架提供了细粒度的访问控制。它与 WebSphere Application Server 提供的访问控制一起（而并非替代）工作。

WebSphere Application Server 中资源保护概述

以下 WebSphere Commerce 资源由 WebSphere Application Server 通过访问控制保护:

- 实体 bean
  这些 bean 模拟电子交易应用程序中的对象的模型。它们是远程客户机可访问的分布式对象。
- JSP 模板
  WebSphere Commerce 将 JSP 模板用于显示页。每个 JSP 模板可包含一个或多个数据 bean，这些数据 bean 从实体 bean 检索数据。客户机可通过编写 URL 请求来请求 JSP 页面。
- 控制器和视图命令
  客户机可通过编写 URL 请求来请求控制器和视图命令。并且，一个显示页通过使用已注册在 VIEWREG 表中的 JSP 文件名或视图名称，可包含至另一页面的链接。

WebSphere Commerce Server 通常配置为使用以下 Web 路径:

- `/webapp/wcs/stores/servlet/*`
  用于对请求小服务程序的请求。
- `/webapp/wcs/stores/*.jsp`
  用于对 JSP 小服务程序的请求。

下表显示了对前面的 Web 路径配置，请求为了访问 WebSphere Commerce 资源而可能遵循的途径。

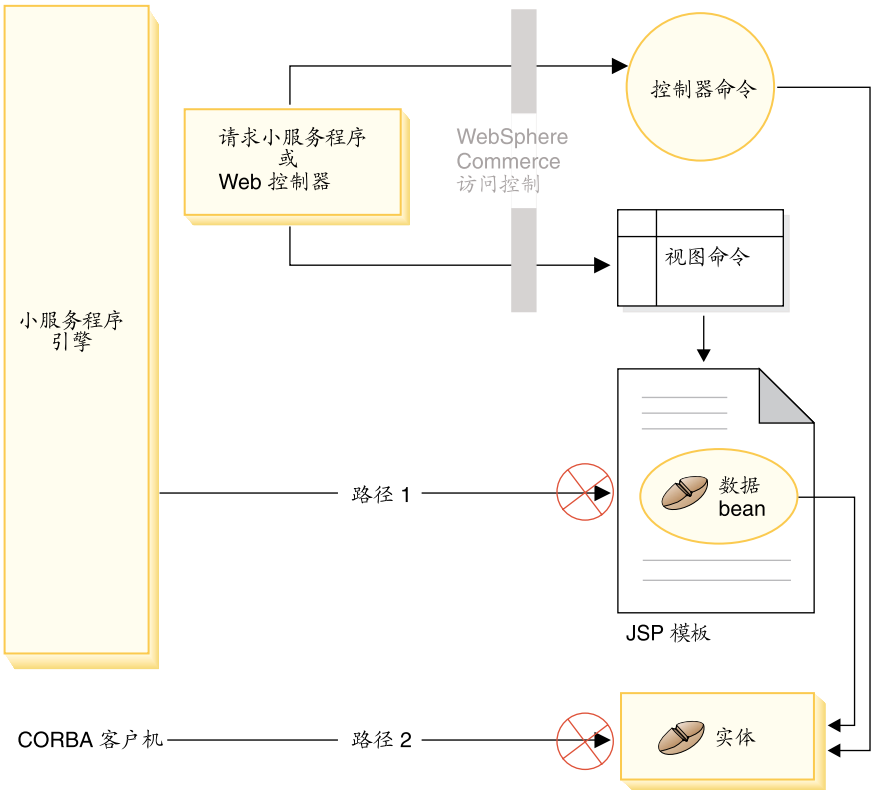


图 3.

所有合法请求都应定向到请求小服务程序，然后由该小服务程序将它们定向到 Web 控制器。Web 控制器实现对控制器命令和视图的访问控制。然而上面显示的 Web 路径使恶意用户可能直接访问 JSP 模板（路径 1）和实体 bean（路径 2）。为了防止这些恶意攻击得逞，必须在运行时拒绝它们。

可通过使用以下方法之一来防止对 JSP 模板和实体 bean 的直接访问:

WebSphere Application Server 安全性

WebSphere Application Server 提供了安全性功能。使用此方法，将所有企业 bean 方法和 JSP 模板配置为仅由“系统标识”调用。要访问这些 WebSphere Commerce 资源，必须在将 URL 请求传递到 Web 控制器之前将它路由到请求小服务程序，该小服务程序将“系统标识”设置为当前线程。然后 Web 控制器在将请求传递到相应的控制器命令或视图前，确保调用者具有必需的授权。WebSphere Application Server 安全性组件将拒绝直接访问 JSP 模板和实体 bean 的所有尝试（即不通过使用 Web 控制器）。

关于配置 WebSphere Application Server 来保护 WebSphere Commerce 资源的信息，请参阅《*WebSphere Commerce 安装指南*》。关于 WebSphere Application Server 中安全性的信息，请参阅 WebSphere Application Server 文档中的“系统管理”主题。

关于为定制企业 bean 方法配置 WebSphere Application Server 安全性的信息，请参阅《*WebSphere Commerce 5.4 程序员指南*》中的『将新的企业 bean 装配成企业应用程序』和『将修改后的企业 bean 装配成企业应用程序』部分。

防火墙保护

当 WebSphere Commerce Server 运行在防火墙后面时，因特网客户机不能直接

访问实体 bean。使用此方法，由包含在页面中的数据 bean 提供了对 JSP 模板的保护。数据 bean 由数据 bean 管理器激活。数据 bean 管理器检测 JSP 模板是否由视图命令转发。如果不是由视图命令转发，则抛出异常且拒绝对 JSP 模板的请求。

WebSphere Commerce 访问控制策略简介

WebSphere Commerce 访问控制模型基于对访问控制策略的强制。访问控制策略允许访问控制规则外部化于商务逻辑代码，因此除去了将访问控制语句硬性编码为代码的必要。例如，无需包含类似于以下的代码:

```
if (user.isAdministrator())
   then {}
```

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受保护资源所适用的访问控制策略，然后基于所适用的访问控制策略，确定是否允许用户访问请求的资源。

访问控制策略是存储在 ACPOLICY 表中的 4 元组策略。每个访问控制策略具有以下格式:

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

4 元组访问控制策略中的元素指定: 允许属于特定用户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，只要用户对正被讨论的资源满足关系或关系组中指定的条件。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。

用户组是定义在 MBRGRP 数据库表中的特定类型的成员组。用户组必须与成员组类型 `-2` 关联。值 `-2` 表示访问组，它在 MBRGRPTYPE 表中定义。用户组和成员组类型之间的关联存储在 MBRGRPUSG 表中。

可显式地或隐式地声明用户在特定用户组中的成员资格。如果 MBRGRPMBR 表声明用户属于特定成员组，则发生显式指定。如果用户满足 MBRGRPCOND 表中声明的条件（例如满足产品经理角色的所有用户），则发生隐式指定。还可以有组合条件（例如满足产品经理角色且担任该角色至少 6 个月的所有用户）和显式排除。

将用户包含在用户组中的大多数条件都是基于满足特定角色的用户。例如，可以有一个访问控制策略允许满足产品经理角色的所有用户执行产品目录管理操作。在此情况下，则将 MBRROLE 表中指定为产品经理角色的所有用户隐式地包含在用户组中。

关于成员组子系统的更多详细信息，请参阅 WebSphere Commerce 联机帮助。

ActionGroup 元素来自 ACACTGRP 表。操作组是指对操作的显式指定的组合。操作列表存储在 ACACTION 表中，且每个操作对于所在的一个或多个操作组的关系存储在 ACACTACTGP 表中。操作组的示例是 “OrderWriteCommands” 操作组。该操作组包含以下用于更新订单的操作:

- com.ibm.commerce.order.commands.OrderDeleteCmd
- com.ibm.commerce.order.commands.OrderCancelCmd
- com.ibm.commerce.order.commands.OrderProfileUpateCmd
- com.ibm.commerce.order.commands.OrderUnlockCmd
- com.ibm.commerce.order.commands.OrderScheduleCmd

- com.ibm.commerce.order.commands.ScheduledOrderCancelCmd
- com.ibm.commerce.order.commands.ScheduledOrderProcessCmd
- com.ibm.commerce.order.commands.OrderItemAddCmd
- com.ibm.commerce.order.commands.OrderItemDeleteCmd
- com.ibm.commerce.order.commands.OrderItemUpdateCmd
- com.ibm.commerce.order.commands.PayResetPMCmd

资源组是将特定类型的资源组合在一起的机制。可用以下两种方式之一来指定资源组中资源的成员资格:

- 使用 ACRESGRP 表中的 conditions 列
- 使用 ACRESGPRES 表

大多数情况下，使用 ACRESGPRES 表将资源关联到资源组已经足够了。使用此方法，用资源的 Java 类名将资源定义在 ACRESCGRY 表中。然后，使用 ACRESGPRES 关联表将这些资源与相应的资源组（ACRESGRP 表）关联。在 Java 类名本身不足以定义资源组成员的情况下（例如，如果需要基于资源的某个属性来进一步限制此类对象），则可完全使用 ACRESGRP 表的 conditions 列来定义资源组。请注意为了基于属性对资源执行此分组，资源还必须实现 Groupable 接口。

以下图表显示了资源分组指定的示例。在此示例中，资源组 10023 包含 ACRESGPRES 表中与之关联的所有资源。使用 ACRESGRP 表中的条件字段列定义了资源组 10070。此资源组包含 Order 远程接口的实例，这些实例也具有状态 “Z”（指定共享的需求列表）。

注: 可在《*WebSphere Commerce 访问控制指南*》中找到 ACRESGRP 表 Conditions 列的 XML 信息的详细内容。

ACRESGRP

AcResGrp_Id	GrpName	Conditions
10023	AccountRepresentatives CmdResourceGroup	null
10070	SharedRequisitionList ResourceGroup	<profile> <andListCondition> <simpleCondition> <variable name="Status"/> <operator name="="/> <value data="Z"/> </simpleCondition> <simpleCondition> <variable name="classname"/> <operator name="="/> <value data="com.ibm.commerce.order.objects.Order"/> </simpleCondition> </andListCondition> </profile>

ACRESGRPES

AcResGrp_Id	AcResCgry_Id
10023	10246
10023	10247
10023	10248
10023	10249
10023	10250

ACRESCGRY

AcResCgry_Id	ResClassname
10246	com.ibm.commerce.contract.commands.ContractCreateCmd
10247	com.ibm.commerce.contract.commands.ContractCreateCmd
10248	com.ibm.commerce.contract.commands.ContractCreateCmd
10249	com.ibm.commerce.contract.commands.ContractCreateCmd
10250	com.ibm.commerce.contract.commands.ContractCreateCmd

图 4.

ACACTGRP、ACRESGRP 和 ACRELGRP 表的 MEMBER_ID 列应当具有值 -2001（根组织）。

访问控制策略可以可选地将 Relationship 或 RelationshipGroup 元素包含为其第四个元素。

如果访问控制策略使用 Relationship 元素，则该元素来自 ACRELATION 表。而如果它包含 RelationshipGroup 元素，则该元素来自 ACRELGRP 表。请注意可以两个都不包含，但是如果包含了一个，则不能包含另一个。来自 ACRELGRP 表的 RelationshipGroup 指定具有比来自 ACRELATION 表的 Relationship 信息更高的优先级。

ACRELATION 表指定存在于用户和资源之间的关系的类型。关系类型的一些示例包含创建者、提交者和所有者。使用 relationship 元素的一个示例是: 使用它来确保订单的创建者始终能够更新订单。

ACRELGRP 表指定可与特定资源关联的关系组的类型。关系组是一个或多个关系链的分组。关系链是多个关系的序列。关系组的示例是指定用户必须是资源的创建者且还必须属于资源中所引用的买方组织实体。

关系组（或关系）指定是访问控制策略的可选部分。它通常用在创建了您自己的命令且未将这些命令限制于某些角色的情况下。在这些情况下，您可能希望在用户和资源之间强制一种关系。通常，如果将命令限制于某些角色，则是通过访问控制策略的 UserGroup 元素而不是使用 Relationship 元素来实现的。

与访问控制策略相关的另一个重要概念是访问控制策略*所有者*的概念。访问控制策略所有者是拥有访问控制策略的组织实体。了解访问控制策略的所有者是很重要的，因为访问控制策略仅可适用于由访问控制策略所有者所拥有的资源。

对于每个正被讨论的资源，访问控制策略管理器将应用由拥有方组织实体或成员层次结构中其上级组织实体所拥有的访问控制策略，直至找到了授予许可权的策略或已检查了所有策略但没有一个授予许可权。

请看显示了成员层次结构的以下图表。

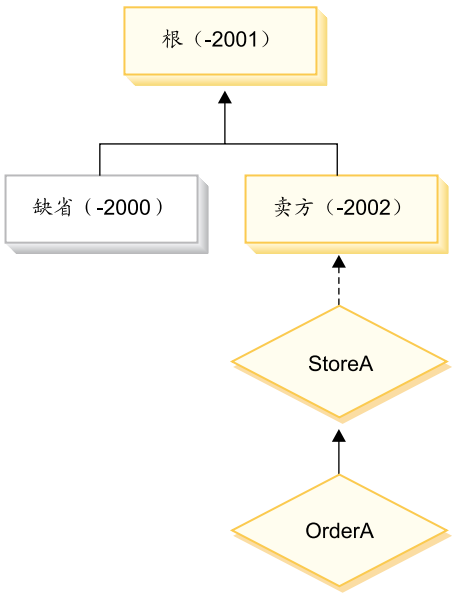


图 5.

对于资源“OrderA”，可应用由卖方或根组织所拥有的任何访问控制策略。如果访问控制策略管理器找到由这两个组织中任何一个所拥有的一个策略授予用户许可权（基于访问控制策略中的四个元素），则它立即停止搜索访问控制策略。但是，如果它未找到由这些组织所拥有的任何访问控制策略授予用户对受保护资源执行操作的许可权，则拒绝访问。

关系组

关系组允许指定多个关系。关系可以直接在用户和正在讨论的资源之间，或者可以是间接将用户关联到资源的关系链。

注: 对于与关系组相关的以下部分，意识到 WebSphere Commerce 专业版中唯一可用的组织是 RootOrganization、DefaultOrganization 和 SellerOrganization 是很重要的。引用其它组织的示例仅适用于 WebSphere Commerce 商务版。

将关系与关系组作比较: 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，指定关系应当满足应用程序的访问控制要求。但是，如果该策略是必须指定在用户和资源之间非直接的但实为一系列的关系，则必须使用关系组。

例如，如果必须在用户和买方组织之间指定关联，其中的关系要求用户对该组织扮演特定角色或用户是买方组织的成员，则必须使用关系组和关系链。

如果仅需要在用户和正被讨论的资源之间实施直接关联，则可使用简单关系。例如，可以是需要实施用户必须是资源的创建者的情况。

如果将多个简单关系组合起来，例如用户必须是创建者或提交者，则这成为关系链且必须使用关系组。此简单关系的组合可在使用 WebSphere Commerce 专业版或 WebSphere Commerce 商务版时出现。

关于关系组的一般信息: 关系链是多个关系的序列。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="aName" value="aValue" />` 元素的数目而确定。

只有最后一个 `<parameter name="Relationship" value="aValue"/>` 元素才必须由资源的 fulfills() 方法处理。其余的由访问控制策略管理器作内部处理。

当关系链的长度为 2 时，第一个 `<parameter name="aName" value="aValue" />` 元素表示用户和组织实体之间的关系。最后一个 `<parameter name="aName" value="aValue" />` 元素表示组织实体和资源之间的关系。

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。可修改 `defaultAccessControlPolicies.xml` 文件，或创建自己的 XML 文件。关于创建这些基于 XML 的信息的更多信息，请参阅《*WebSphere Commerce 访问控制指南*》。

以下部分显示了不同类型的关系组的示例。

由单一关系链组成的关系组: Business 作为访问控制策略的一部分，可能需要强制用户必须属于系资源的 BuyingOrganizationalEntity 的组织实体。这要求创建由长度为 2 的一个关系链所组成的关系组。关系链的长度为 2 是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级组织实体之间。用户是该组织的子级。对于第二个关系，访问控制策略管理器检查父级组织实体是否对资源满足 BuyingOrganizationalEntity 关系。换言之，如果它是资源的买方组织实体则返回 “true”。

以下 XML 片段是从 `defaultAccessControlPolicies.xml` 文件中取出的，它显示了如何定义此类型的关系组:

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

```
    </openCondition>
   </profile>
 ]]></RelationCondition>
</RelationGroup>
```

Business 另一示例是强制用户必须对组织实体（该组织实体系正在讨论的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。链的第一部分将查找用户对其具有客户代表角色的所有组织实体。然后对于这一组织实体的集合，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。换言之，如果其中有一个是资源的买方组织实体则返回 true。

以下 XML 片段是从 defaultAccessControlPolicies.xml 文件中取出的，它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>
```

由多个关系链组成的关系组: 为包含多个关系链，可以组成关系组。实现此操作时，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）。

Business 为了演示此类型的关系，以下 XML 片段用于强制用户必须是资源的创建者，且用户还必须属于资源中指定的 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。

```
<RelationGroup 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>
```

如果不使用 *AND* 方案，而是需要用户满足两个关系链中的任何一个，则应将 <andListCondition> 标记更改为 <orListCondition> 标记。

Professional Business 为了说明可用于 WebSphere Commerce 专业版（以及 WebSphere Commerce 商务版）中的关系组，请考虑一个用于强制用户必须是资源的创建者或提交者的关系组。这在以下 XML 片段中作了显示。

```
<RelationGroup Name="Creator_Or_Submitter"
     OwnerID="RootOrganization">
   <RelationCondition><![CDATA [
   <profile>
      <orListCondition>
    <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="creator"/>
    </openCondition>
    <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="submitter"/>
    </openCondition>
      </orListCondition>
   </profile>
 ]]></RelationCondition>
</RelationGroup>
```

访问控制的类型

有两种类型的访问控制，两者都是基于策略的：命令级访问控制和资源级访问控制。

命令级（又称为“基于角色的”）访问控制使用广泛策略类型。可指定某一特定角色的所有用户都可执行某些类型的命令。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。或者，如以下图表所描述，另一示例策略指定所有的商店管理员都可对由 StoreAdminCmdResourceGrp 指定的任何资源，执行在 ExecuteCommandAction 组中指定的任何操作。

注：当使用管理控制台设置访问组时，生成 MBRGRPCOND 表 Conditions 列的 XML 信息。关于使用管理控制台设置访问组的信息，请参阅 WebSphere Commerce 联机帮助。

ACPOLICY

PolicyName	Member_Id	MbrGrp_Id	AcActGrp_id	AcResGrp_Id	AcRelGrp_Id
StoreAdministrators ExecuteStoreAdmin CmdResourceGroup	-2001	-8	10052	10018	null

MBRGRP

MbrGrp_Id	MbrGrpName
-8	StoreAdministrators

MBRGRPCOND

MbrGrp_Id	Conditions
-8	<profile> <simpleCondition> <variable name="role"/> <operator name="="/> <value data="Store Administrator"/> </simpleCondition> </profile>

ACACTGRP

AcActGrp_Id	GroupName
10052	ExecuteCommandActionGroup

ACRESGRP

AcResGrp_Id	GrpName
10018	StoreAdminCmdResourceGroup

图 6.

命令级访问控制策略始终将 ExecuteCommandActionGroup 作为控制器命令的操作组。对于视图，资源组始终是 ViewCommandResourceGroup。

所有的控制器命令都必须受到命令级访问控制的保护。并且，可以被直接调用或可通过来自另一命令的重定向而启动（相对于通过转发给视图而启动）的任何视图，必须受到命令级访问控制的保护。

命令级访问控制不考虑命令将对其实施命令的资源。它仅确定是否允许用户执行特定命令。如果允许用户执行命令，则可应用后续的资源级访问控制策略来确定用户是否可访问正讨论的资源。

请考虑商店管理员试图执行管理任务时的情形。第一个级别的访问控制检查将是确定是否允许该用户执行特定的商店管理命令。一旦确定了实际上允许该用户执行此命令（因为允许商店管理员执行 storeAdminCmds 组中的命令），则可调用资源级访问控制策略。此策略可声明仅允许商店管理员执行该用户是其商店管理员的组织所拥有的商店的管理任务。

总之，在命令级访问控制中，“资源”即命令本身，而“操作”只是执行命令（换言之，即实例化命令对象）。访问控制检查确定是否允许用户执行命令。相反地，在资源级访问控制中，“资源”是命令或 bean 访问的任何受保护资源，而“操作”是命令本身。

访问控制交互

此部分显示一些交互图表，这些图表显示了 WebSphere Commerce 访问控制策略框架中访问控制如何工作。

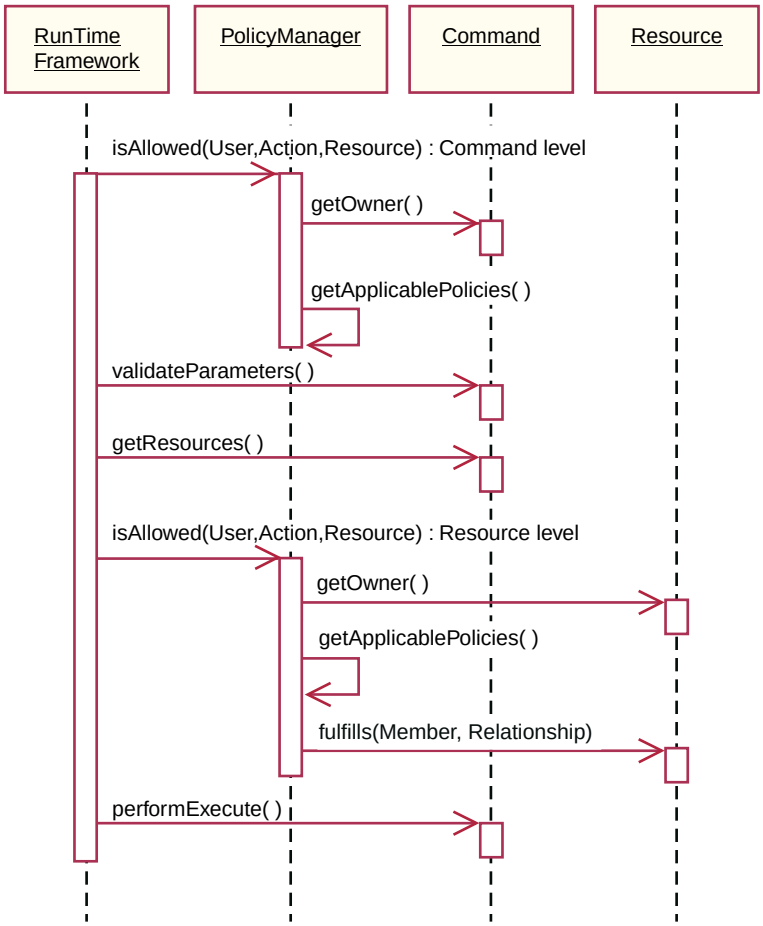


图 7.

以上图表显示了访问控制*策略管理器*执行的操作。访问控制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。它通过搜索由资源所有者及其上级组织所拥有的策略来确定。如果至少有一个策略授予访问权，则授予许可权。

以下列表描述了上面交互图表中的操作。其顺序是从图表的顶部到底部。

1. `isAllowed()`
   此运行时组件确定用户是否对控制器命令或视图具有命令级访问权。
2. `getOwner()`
   访问控制策略管理器确定命令级资源的所有者。缺省实现返回处于命令上下文中的商店（`storeId`）所有者的成员标识（`memberId`）。如果在命令上下文中没有商店标识，则返回根组织（`-2001`）。

3. getApplicablePolicies()
   访问控制策略管理器根据指定的用户、操作和资源来查找并处理可应用的策略。
4. validateParameters()
   初始参数检查和解析。
5. getResources()
   返回系“资源-操作”对的向量的访问向量。

   如果没有任何返回，则不执行资源级访问控制检查。如果存在任何应受到保护的资源，则应返回访问向量（由“资源-操作”对组成）。

   每个*资源*都是可保护对象（实现 com.ibm.commerce.security.Protectable 接口的对象）的实例。在许多情况下，资源是访问 bean。

   访问 bean 可能不实现 com.ibm.commerce.security.Protectable 接口，然而根据第 90 页的『在企业 bean 中实现访问控制』中包含的信息，只要相应的企业 bean 是受保护的，则仍可发生访问控制检查。

   *操作*是一个字符串，代表要对资源执行的操作。在大多数情况下，操作是命令的接口名称。
6. isAllowed()
   此运行时组件确定用户是否具有对 getResources() 指定的所有“资源-操作”对的资源级访问权。
7. getOwner()
   资源返回其所有者的 memberId。这确定了应用哪些策略。仅应用由资源所有者及其上级组织所拥有的策略。
8. getApplicablePolicies()
   访问控制策略管理器搜索可应用的策略，然后应用它们。如果对于每个“资源-操作”对都找到了至少一个策略授予用户访问资源的许可权，则授予访问权，否则拒绝访问。
9. fulfills()
   如果可应用的策略具有指定的关系组，则对资源执行检查以查看对于该资源而言，成员是否满足指定的一个或多个关系。
10. performExecute()
    命令的商务逻辑。

Protectable 接口

让资源受 WebSphere Commerce 访问控制策略保护的关键因素是该资源必须实现 com.ibm.commerce.security.Protectable 接口。此接口最常见地用于企业 bean 和数据 bean，但是只有那些需要保护的特定 bean 才需要实现此接口。

使用 Protectable 接口，资源必须提供两种主要方法：getOwner() 和 fulfills(Long member, String relationship)。

访问控制策略由组织或组织实体所拥有。getOwner 方法返回可保护资源的所有者的 memberId。在访问控制策略管理器确定了资源的所有者之后，它还获取成员层次结构中所有者的每个上级的 memberId。然后应用属于来自原始的 getOwner 请求的所有者的所有访问控制策略以及属于所有者的任何上级的所有访问控制策略。

将应用适用于指定所有者的访问控制策略以及适用于成员资格层次结构中所有者的任何更高级别上级的访问控制策略。

fulfills 方法仅在给定的成员对于资源满足必需的关系时返回 true。通常成员是单个用户，但也可以是组织。如果您正在访问控制策略中使用关系组，则它将是组织。

Groupable 接口

访问控制策略的应用是特定于一组资源的。可基于一些属性（例如类名、订单状态或 storeId 值）进行资源分组。

如果资源将按除其类名之外的某个属性进行分组，以用于应用访问控制策略的目的，则它必须实现 com.ibm.commerce.grouping.Groupable 接口。

以下代码片段表示了 Groupable 接口:

```
Groupable interface {
Object getGroupingAttributeValue (String attributeName, GroupContext context)
}
```

例如，要实现仅适用于处于未决状态（status = P（未决））的订单的策略，则 Order 实体 bean 的远程接口实现 Groupable 接口，且 attributeName 的值设置为“status”。

Groupable 接口的使用很少见。

查找关于访问控制的更多信息

关于 WebSphere Commerce 访问控制模型的更多信息，请参阅《*WebSphere Commerce 访问控制*》。该指南提供了对访问控制的详细概述，并描述了如何使用管理控制台创建或修改策略、操作组和资源组。

实现访问控制

本部分描述如何在定制代码中实现访问控制。

标识可保护资源

一般地，企业 bean 和数据 bean 是您可能希望保护的资源。然而，并非所有的企业 bean 和数据 bean 都应当受保护。在现有的 WebSphere Commerce 应用中，需要保护的资源已实现了 protectable 接口。在您创建新的企业 bean 和数据 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。

如果命令在 getResources 方法中返回企业 bean，则企业 bean 必须受保护，因为访问控制策略管理器将对企业 bean 调用 getOwner 方法。如果在相应的资源级访问控制策略中指定了关系，则还将调用 fulfills 方法。

如果要对您自己的所有企业 bean 和数据 bean 实现 protectable 接口（因此将资源置于保护之下），则您的应用程序可能需要许多策略。随着策略数目的增加，性能可能降级且策略管理将变得更为困难。

在主资源和从属资源之间作了理论上的区分。*主资源*可基于其自身而存在。*从属资源*仅当其相关的主资源存在时才存在。例如，在“箱外”WebSphere Commerce 应用程序代码中，Order 实体 bean 是可保护资源，而 OrderItem 实体 bean 则不是。原因是 OrderItem 的存在依赖于 Order — Order 是主资源而 OrderItem 是从属资源。如果用户应具有对 Order 的访问权，则它也应具有对该订单中的商品的访问权。

类似地，User 实体 bean 是可保护资源，而 Address 实体 bean 则不是。在此情况下，地址的存在取决于用户，因此任何对用户具有访问权的也应对地址具有访问权。

主资源应当是受保护的，而从属资源经常是不需要保护的。如果允许用户访问主资源，则有理由在缺省情况下也应允许用户访问其从属资源。

在企业 bean 中实现访问控制

如果您创建的新企业 bean 需要受到访问控制策略的保护，则必须执行以下操作:

1. 创建新的企业 bean，确保它从 com.ibm.commerce.base.objects.ECEntityBean 扩展。
2. 确保 bean 的远程接口扩展了 com.ibm.commerce.security.Protectable 接口。
3. 如果 bean 与之交互的资源按除资源的 Java 类名之外的某一属性进行分组，则该 bean 的远程接口还必须扩展 com.ibm.commerce.grouping.Groupable 接口。
4. 企业 bean 类包含以下方法的缺省实现:
   - getOwner
   - fulfills
   - getGroupingAttributeValue

   请重设所需的任何方法。至少，您必须重设 getOwner 方法。
   这些方法的缺省实现显示在以下代码片段中。

```
**************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
      return null;
}
**************************************************************************
**************************************************************************
public boolean fulfills(Long member, String relationship)
   throws Exception, java.rmi.RemoteException
{
      return false;
}
**************************************************************************
**************************************************************************
public Object getGroupingAttributeValue(String attributeName,
   GroupingContext context) throws Exception, java.rmi.RemoteException
{
      return null;
}
**************************************************************************
```

   以下是基于 OrderBean bean 的这些方法的样本实现:

```
**************************************************************************
public Long getOwner() throws Exception, java.rmi.RemoteException
{
   com.ibm.commerce.common.objects.StoreEntityAccessBean storeEntAB = new
   com.ibm.commerce.common.objects.StoreEntityAccessBean();
   storeEntAB.setInitKey_storeEntityId(getStoreEntityId().toString());
   return storeEntAB.getMemberIdInEJBType();
}
**************************************************************************
**************************************************************************
public boolean fulfills(Long member, String relationship)
   throws Exception, java.rmi.RemoteException
   {
      if (relationship.equalsIgnoreCase("creator"))
```

```
        {
           return member.equals(getMemberId());
        }
        else if (relationship.equalsIgnoreCase (
           com.ibm.commerce.base.helpers.EJBConstants.
           SAME_ORGANIZATIONAL_ENTITY_AS_CREATOR_RELATION)) {
              com.ibm.commerce.user.objects.UserAccessBean creator = new
                 com.ibm.commerce.user.objects.UserAccessBean();
              creator.setInitKey_MemberId(getMemberId().toString());
              com.ibm.commerce.user.objects.UserAccessBean ab = new
                 com.ibm.commerce.user.objects.UserAccessBean();
              ab.setInitKey_MemberId(member.toString());
              if (ab.getParentMemberId().equals(creator.getParentMemberId()))
                 return true;
            }
        return false;
    }
    ********************************************************************************
    ********************************************************************************
    public Object getGroupingAttributeValue(String attributeName,
       GroupingContext context) throws Exception
       {
          if (attributeName.equalsIgnoreCase("Status"))
             return getStatus();
          return null;
       }
    ********************************************************************************
```

5. 创建（或重新创建）企业 bean 的访问 bean 和生成的代码。

在数据 bean 中实现访问控制

如果要保护数据 bean，则它可以直接或间接地受访问控制策略的保护。如果直接保护数据 bean，则存在应用于该特定数据 bean 的访问控制策略。如果间接保护数据 bean，则将保护交托给存在访问控制策略的另一数据 bean。

如果创建的新数据 bean 直接受访问控制策略的保护，则数据 bean 必须执行以下操作:

1. 实现 com.ibm.commerce.security.Protectable 接口。因此，bean 必须提供 getOwner() 实现和 fulfills(Long member, String relationship) 方法。这些应当在 bean 的远程接口上实现。

   当数据 bean 实现 Protectable 接口时，数据 bean 管理器调用 isAllowed 方法，根据当前访问控制策略确定用户是否具有相应的访问控制特权。isAllowed 方法由以下代码片段描述:

   ```
   IsAllowed(Context, "Display", protectable_databean);
   ```

2. 如果 bean 与之交互的资源按除资源的 Java 类名之外的某一属性进行分组，则该 bean 必须实现 com.ibm.commerce.grouping.Groupable 接口。
3. 实现 com.ibm.commerce.security.Delegator 接口。此接口由以下代码片段描述:

   ```
   Interface Delegator {
   Protectable getDelegate();
   }
   ```

   注: 为了直接受保护，getDelegate 方法应返回数据 bean 本身（即数据 bean 交托给它自身以用于访问控制目的）。

数据 bean 是应受直接保护还是应受间接保护之间的区别类似于主资源和从属资源之间的区别。如果数据 bean 对象可存在于其自身之上，则应直接保护它。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。受间接保护的数据 bean 的示例是 OrderItem 数据 bean。

如果创建的新数据 bean 间接受访问控制策略的保护，则数据 bean 必须执行以下操作:

1. 实现 com.ibm.commerce.security.Delegator 接口。此接口由以下代码片段描述:

```
Interface Delegator {
Protectable getDelegate();
}
```

   注: 由 getDelegate 返回的数据 bean 必须实现 Protectable 接口。

如果数据 bean 未实现 Delegator 接口，则不受访问控制策略的保护即填充它。

在控制器命令中实现访问控制

当创建新的控制器命令时，新命令的实现类应当扩展 com.ibm.commerce.commands.ControllerCommandImpl 类，且它的接口应当扩展 com.ibm.commerce.command.ControllerCommand 接口。

对于用于控制器命令的命令级别的策略，则将该命令的接口名称指定为资源。为了让资源受到保护，它必须实现 Protectable 接口。根据 WebSphere Commerce 编程模型，这是通过让该命令的接口从 com.ibm.commerce.command.ControllerCommand 接口扩展，且让该命令的实现从 com.ibm.commerce.commands.ControllerCommandImpl 扩展而完成的。ControllerCommand 接口扩展 com.ibm.commerce.command.AccCommand 接口，后者再扩展 Protectable。AccCommand 接口是命令为了受命令级别的访问控制保护而应当实现的最小接口。

如果命令访问应受保护的资源，则创建类型 AccessVector 的专用实例变量来保存资源。然后重设 getResources 方法，因为此方法的缺省实现是返回空值，因此不发生资源检查。

在新的 getResources 方法中，应当返回命令可对其实施操作的一系列资源或“资源-操作”对。当未显式地指定操作时，操作的缺省值是正在执行的命令的接口名称。

并且，建议该方法确定它是否必须实例化资源，或它是否可以使用现有的实例变量保存对资源的引用。检查资源对象是否已经存在可有助于改进系统性能。然后可在新控制器命令的 performExecute 方法中使用同一 getResources 方法（如有必要）。

以下是 getResources 方法的示例:

```
private AccessVector resources = null;

public AccessVector getResources() throws ECException {

   if (resources == null) {
      OrderAccessBean orderAB = new OrderAccessBean();
      orderAB.setInitKey_orderId(getOrderId().toString());
      resouces = new AccessVector(orderAB);
      }
   return resources;
}
```

例如，请考虑 OrderItemUpdate 命令。此命令的 getResources 方法返回 Order 和 User 可保护对象。因为未指定操作，则它缺省使用 OrderItemUpdate 命令的接口。

getResources 方法可返回多个资源。发生此情况时，如果要执行操作，则必须找到一个策略，该策略给予用户对所有指定资源的访问权。如果用户对三个资源当中的两个具有访问权，则操作不能继续（三个当中的三个全都需要）。

如果需要执行附加参数检查或对控制器命令中的参数执行解析，可使用 validateParameters() 方法。这是可选的。

附加资源级检查

并非在调用控制器命令的 getResources 方法时总是可能确定所有需要保护的资源。

如有必要，任务命令也可实现 getResources 方法以返回命令可对其实施操作的资源的列表。

调用资源级检查的另一方法是使用 checkIsAllowed(Object resource, String action) 方法，对访问控制策略管理器作直接调用。此方法可用于从 com.ibm.commerce.command.AbstractECTargetableCommand 类扩展的任何类。例如，以下类从 AbstractECTargetableCommand 类扩展:

- com.ibm.commerce.command.ControllerCommandImpl
- com.ibm.commerce.command.DataBeanCommandImpl

checkIsAllowed 方法也可用于扩展 com.ibm.commerce.command.AbstractECCommand 类的那些类。例如，以下类从 AbstractECCommand 类扩展:

- com.ibm.commerce.command.TaskCommandImpl

以下显示了 checkIsAllowed 方法的特征符:

```
void checkIsAllowed(Object resource, String action)
   throws ECException
```

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抛出 ECApplicationException。如果授予访问权，则该方法即简单地返回。

“create”命令的访问控制

因为在命令中 getResources 方法的调用在 performExecute 方法之前，因此必须采取不同的办法用于对尚未创建的资源的访问控制。例如，如果有 WidgetAddCmd，则 getResources 方法无法返回将要创建的资源。在此情况下，getResources 方法应返回资源的创建者。例如，命令由命令工厂创建，订单在商店内创建，用户在组织内创建。

命令级访问控制的缺省实现

对于命令级访问控制，如果指定了 storeId，则 getOwner() 方法的缺省实现返回商店所有者的 memberId。如果未指定 storeId，则返回根组织的 memberId（memberId = -2001）。

getResources() 方法的缺省实现返回 null。

validateParameters() 的缺省实现什么都不返回。

在视图中实现访问控制策略

视图的资源级访问控制由数据 bean 管理器执行。在以下情况下调用数据 bean 管理器:

1. 当 JSP 模板包含 <useBean> 标记且数据 bean 不在属性列表中。

2. 当 JSP 模板包含以下激活的方法:

```
DataBeanManager.activate(xyzDatabean, request);
```

注: 要（直接或间接）保护的任何数据 bean 都必须实现 Delegator 接口。要直接保护的任何数据 bean 将交托给它自身，因此还必须实现 Protectable 接口。间接保护的数据 bean 应当交托给实现 Protectable 接口的数据 bean。

对访问控制检查的忽略（并不建议此行为）发生在以下情形中:

1. 如果 JSP 模板直接调用访问 bean，而不是使用数据 bean。
2. 如果 JSP 模板直接调用数据 bean 的 populate() 方法。

如果将控制器命令的结果转发给视图（使用 ForwardViewCommand），则不对视图执行命令级访问控制。并且，如果控制器命令将填充后的数据 bean（用于视图中）放置在响应属性的属性列表中，然后转发给视图，则 JSP 模板可访问数据而不通过数据 bean 管理器。这需要在 JSP 模板中使用 `<useBean>` 标记。这可以是使 JSP 模板更有效率的一种方法，因为它可忽略对某些资源（数据 bean）的任何多余的资源级访问控制检查，通过控制器命令已授予了用户对这些资源的访问权。

第 5 部分 附属资料

声明

本信息是为在美国提供的产品和服务编写的。

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

在本出版物中任何对 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。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 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，其评估和验证均由用户自行负责。

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

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

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

本条款不适用联合王国或任何这样的条款与当地法律不一致的国家或地区:

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

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

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

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

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

IBM Canada Ltd.
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。

此信息仅作为规划目的。其中的信息在描述的产品可用之前会得到更改。

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，仅供已由信用卡标记的所有者授予通过该信用卡接受支付的权限的商家使用。

商标

以下术语是国际商业机器公司在美国和／或其它国家或地区的商标或注册商标:

400	AIX	AS/400
DB2	IBM	iSeries
OS/2	SecureWay	WebSphere

Domino 是 Lotus Development Corporation 和／或 IBM 公司在美国和／或其它国家或地区的注册商标。

Netscape 是 Netscape Communications Corporation 在美国和／或其它国家或地区的注册商标。

Solaris、Solaris Operating Environment、Java、JavaBeans 以及所有基于 Java 的商标和徽标是 Sun Microsystems, Inc. 的商标或注册商标。

VeriSign 和 VeriSign 徽标是 VeriSign, Inc. 的商标和服务标记或注册商标和服务标记。

UNIX 是 The Open Group 在美国和其它国家或地区的注册商标。

Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和／或其它国家或地区的商标或注册商标。

其它公司、产品或服务名称可能是其它公司的商标或服务标记。

中国印刷