IBM WebSphere Commerce

Guía de seguridad

Versión 5.5

IBM WebSphere Commerce

Guía de seguridad

Versión 5.5

Nota:
Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado “Avisos” en la página 231.

Primera edición (Junio 2003)

Esta edición se aplica a IBM WebSphere Commerce Versión 5.5 (número de producto 5724-A18), así como a todos los releases y modificaciones siguientes hasta que se indique lo contrario en nuevas ediciones. Asegúrese de utilizar la edición correcta para el nivel del producto.

Puede solicitar publicaciones a través de un representante de IBM o una oficina local de IBM.

IBM agradece sus comentarios. Puede enviar sus comentarios utilizando la hoja de comentarios de la documentación de IBM WebSphere Commerce que puede encontrar en el URL siguiente:

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

Cuando envía información a IBM, otorga a IBM un derecho no exclusivo de utilizar o distribuir la información de la forma que crea apropiada sin incurrir en ninguna obligación para con su persona.

Contenido

Acerca de este manual

Este documento describe las características de seguridad de WebSphere Commerce y el modo de configurar dichas características.

Describe de forma detallada temas y características de seguridad de WebSphere Commerce tales como las políticas de autenticación, autorización y control de acceso. El objetivo de este documento es proporcionar a las personas responsables de la seguridad del sitio (entre las que probablemente se encuentran un administrador del sistema o un administrador de sitio de WebSphere Commerce) un documento completo para permitirles proteger un sitio de producción de WebSphere Commerce de forma fiable.

Este documento está destinado a las personas responsables de la seguridad o los administradores de seguridad de los sitios de WebSphere Commerce.

Importante

Este documento sólo incluye temas de seguridad de WebSphere Commerce relacionados con el despliegue de un sitio de comercio electrónico. No se incluyen temas relacionados con la vulnerabilidad del sistema operativo. Para proteger el sistema operativo, deberá consultar con el proveedor del sistema operativo a fin de determinar las medidas apropiadas que debe tomar.

Resumen de cambios

Esta Guía de seguridad y cualquier versión actualizada de esta Guía de seguridad estarán disponibles en la página Web de la biblioteca técnica de WebSphere (http://www.ibm.com/software/commerce/library/). Para obtener información adicional acerca de su edición de WebSphere Commerce, consulte las páginas de visión general.

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

Para obtener información sobre el soporte adicional, consulte la página de soporte de WebSphere Commerce (`http://www.ibm.com/software/commerce/support/`).

Para obtener información acerca de los cambios de última hora realizados en el producto, consulte el archivo README del producto actualizado que puede obtener también en el sitio Web mencionado.

Cualquier actualización realizada en este manual se resumirá en este apartado.

Cómo está organizada la información en esta publicación

Este documento se divide en las partes siguientes:

- La Parte 1, "Conceptos de seguridad en WebSphere Commerce", en la página 1, describe el modelo de seguridad de WebSphere Commerce y proporciona una visión general de los conceptos de seguridad de WebSphere Commerce. Esta

parte será de interés para cualquier persona que desee tener una visión general de la seguridad de WebSphere Commerce o planificar la seguridad en un sitio de WebSphere Commerce.

- La Parte 2, "Administración de la autenticación de seguridad", en la página 51, describe las tareas de administración de WebSphere Commerce relacionadas con la seguridad del sitio. Esta parte será de interés para cualquier persona que realice tareas de administración de sitio relacionadas con la seguridad del sitio.
- La Parte 3, "Administración de la autorización de seguridad", en la página 95 describe las tareas de autorización de WebSphere Commerce relacionadas con el control de acceso. Esta parte será de interés para cualquier persona que realice tareas de autorización del sistema relacionadas con el control de acceso en WebSphere Commerce.
- La Parte 4, "Seguridad de Payments", en la página 181, describe las tareas de administración de WebSphere Commerce relacionadas con la seguridad de WebSphere Commerce Payments. Esta parte será de interés para los administradores de WebSphere Commerce Payments.
- La Parte 5, "Diferentes temas sobre seguridad", en la página 187, describe diferentes tareas de administración del sistema WebSphere Commerce como, por ejemplo, mejorar la seguridad de WebSphere Application Server. Esta parte será de interés para los administradores del sistema responsables de la seguridad.

Convenios utilizados en este manual

Este manual utiliza los convenios de resaltado siguientes:

Negrita	Indica mandatos o controles de la interfaz gráfica de usuario, la GUI, como por ejemplo los nombres de campos, iconos u opciones de menú.
`Monoespaciado`	Indica ejemplos de texto que se han de escribir exactamente como se muestran, por ejemplo, nombres de archivos, nombres de vías de acceso a directorios y nombres.
Cursiva	Se utiliza para enfatizar palabras. La cursiva también indica nombres que se deben sustituir por los valores apropiados para el sistema.
nombre_sistema_principal	El nombre de sistema principal totalmente calificado de WebSphere Commerce Server (por ejemplo, `servidor.midominio.ibm.com` es un nombre totalmente calificado).
nombre_instancia	El nombre de la instancia de WebSphere Commerce con la que está trabajando.
Windows *unidad*	Letra que representa la unidad en la que ha instalado el producto o el componente que se está describiendo (por ejemplo `C:`).

Este icono indica un Consejo - información adicional que puede ayudarle a realizar una tarea.

Importante

En estos apartados se resalta la información que tienen una importancia especial.

Atención
En estos apartados se resalta la información destinada a proteger sus datos.

Business indica la información específica de WebSphere Commerce Business Edition.

Professional indica información específica de WebSphere Commerce Professional Edition.

AIX indica información específica de WebSphere Commerce para AIX.

400 indica información específica de WebSphere Commerce para IBM @server iSeries 400 (anteriormente se denominaba AS/400)

Linux indica información específica de WebSphere Commerce para Linux.

Solaris indica información específica de WebSphere Commerce para software del entorno operativo Solaris.

Windows indica información específica de WebSphere Commerce para Windows 2000.

Variables de vía de acceso

En esta guía se utilizan las variables siguientes para representar vías de acceso como:

dir_instalación_DB2
Esta variable representa el directorio de instalación real de DB2 Universal Database en la máquina. Los siguientes son los directorios de instalación por omisión para DB2 Universal Database en diferentes sistemas operativos:

AIX `/usr/lpp/db2_08_01`

400 No es aplicable (se instala como parte del sistema operativo)

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

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

Windows `C:\Archivos de programa\WebSphere\sqllib`

dir_instalación_HTTPServer
Esta variable representa el directorio de instalación real de IBM HTTP Server en la máquina. Los siguientes son los directorios de instalación por omisión de IBM HTTP Server en diferentes sistemas operativos:

AIX `/usr/IBMHttpServer`

400 No es aplicable (se instala como parte del sistema operativo)

Linux `/opt/IBMHttpServer`

Solaris /opt/IBMHttpServer

Windows C:\Archivos de programa\WebSphere\IBMHTTPServer

dir_instalación_Oracle
Esta variable representa el directorio de instalación real de Oracle en la máquina. Los siguientes son los directorios de instalación por omisión de Oracle en diferentes sistemas operativos:

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

400 No es aplicable para OS/400.

Linux No aplicable para Linux.

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

Windows C:\oracle\ora91

dir_instalación_WAS
Esta variable representa el directorio de instalación real de WebSphere Application Server en la máquina. Los siguientes son los directorios de instalación por omisión para WebSphere Application Server en diferentes sistemas operativos:

AIX /usr/WebSphere/AppServer

400 /QIBM/ProdData/WebAS5/Base

Linux /opt/WebSphere/AppServer

Solaris /opt/WebSphere/AppServer

Windows C:\Archivos de programa\WebSphere\AppServer

dir_usuario_WAS
400 Esta variable representa el directorio para todos los datos que utiliza WebSphere Application Server que el usuario debe configurar o que se pueden modificar, en una máquina iSeries. El valor por omisión de este directorio es:

400 /QIBM/UserData/WebAS5/Base/*nombre_instancia_WAS*

dir_instalación_WC
Esta variable representa el directorio de instalación real de WebSphere Commerce en la máquina. Los siguientes son los directorios de instalación por omisión para WebSphere Commerce en diferentes sistemas operativos:

AIX /usr/WebSphere/CommerceServer55

400 /QIBM/ProdData/CommerceServer55

Linux /opt/WebSphere/CommerceServer55

Solaris /opt/WebSphere/CommerceServer55

Windows C:\Archivos de programa\WebSphere\CommerceServer55

dir_usuario_WC

400 Esta variable representa el directorio para todos los datos que utiliza WebSphere Commerce que el usuario debe configurar o que se pueden modificar en un sistema iSeries. El valor por omisión de este directorio es:

400 `/QIBM/UserData/CommerceServer55`

Parte 1. Conceptos de seguridad en WebSphere Commerce

Esta parte proporciona una visión general de los conceptos de seguridad de WebSphere Commerce.

Capítulo 1. Introducción al modelo de seguridad de WebSphere Commerce

Este capítulo describe el modelo de seguridad de WebSphere Commerce, así como diversos conceptos de seguridad de WebSphere Commerce.

Visión general

La información de este documento describe las nociones de autenticación, autorización, políticas y confidencialidad:

¿Qué es la autenticación?

La autenticación es el proceso mediante el cual se verifica que los usuarios o las aplicaciones son quienes afirman ser. En un sistema WebSphere Commerce, la autenticación es necesaria para todos los usuarios y todas las aplicaciones que acceden al sistema, con la excepción de los usuarios invitados. El proceso de autenticación de usuario se realiza siempre bajo SSL. Esto asegura que una tercera persona que utilice programas de "fisgoneo" de la red no pueda *husmear* en la red cuando un usuario somete una contraseña. Las contraseñas no se descifran nunca durante el proceso de autenticación, como práctica de seguridad común. Todas las contraseñas de usuario se generan de forma aleatoria (hash) y unidireccional y se cifran utilizando una clave de 128 bits, conocida como la *clave de comerciante*. La clave de comerciante se especifica durante la instalación y configuración del sistema WebSphere Commerce.

El sistema WebSphere Commerce tiene sus propias contraseñas para la administración. Estas contraseñas deben cambiarse periódicamente como parte de una política de seguridad de todo el sitio de WebSphere Commerce. Para conocer los detalles de cómo cambiar las contraseñas del sistema WebSphere Commerce, consulte el Capítulo 6, “Establecimiento y cambio de contraseñas”, en la página 79.

¿Qué es la autorización?

La autorización es el proceso mediante el cual se determina si un usuario puede realizar una operación específica en un recurso. La autorización se determina a partir de las políticas de control de acceso que rigen los recursos de WebSphere Commerce. En un sistema WebSphere Commerce, el control de acceso es necesario en dos áreas:

- Para proteger los Enterprise JavaBeans (beans EJB) de WebSphere Commerce frente al acceso no autorizado. Este proceso se describe en el Capítulo 16, “Habilitación de la seguridad de WebSphere Application Server”, en la página 189.
- Para asegurar que sólo las partes autorizadas puedan ejecutar grupos diferentes de mandatos de WebSphere Commerce. Este proceso se describe en el apartado "Control de acceso" de la publicación *WebSphere Commerce, Guías de programación y aprendizaje*.

¿Qué son las políticas de control de acceso?

Suponiendo que ha terminado de definir las organizaciones y los usuarios que participarán en el sitio de comercio electrónico, ahora puede gestionar sus actividades mediante un conjunto de políticas, que es un proceso que se conoce como *control de acceso*.

Una política de control de acceso es una norma que describe qué grupo de usuarios tiene autorización para realizar determinadas actividades en el sitio. Estas actividades pueden incluir acciones que van desde el registro y la gestión de subastas hasta la actualización del catálogo de productos y la concesión de aprobaciones en los pedidos, así como cualquiera de los cientos de actividades diferentes que son necesarias para operar y mantener un sitio de comercio electrónico.

Las políticas son las que otorgan a los usuarios el acceso al sitio. A no ser que estén autorizados a ejercer sus responsabilidades mediante una o más políticas de control de acceso, los usuarios no tienen acceso a ninguna de las funciones del sitio.

El modelo de autorización para WebSphere Commerce está basado en la aplicación de políticas de control de acceso. Las políticas de control de acceso las impone el Gestor de políticas de control de acceso. En general, cuando un usuario intenta acceder a un recurso protegido, el gestor de políticas de control de acceso determina primero qué políticas de control de acceso son aplicables para dicho usuario y, a continuación, basándose en las políticas de control de acceso aplicables, determina si se permite al usuario realizar la operación solicitada en el recurso en concreto.

¿Qué es un seguimiento de comprobación?

En los sistemas informáticos, se utiliza el término *seguimiento de comprobación* para hacer referencia a las anotaciones cronológicas electrónicas o en papel que se utilizan para hacer el seguimiento de la actividad del sistema. Por ejemplo, puede que un empleado tenga acceso a una parte de una red corporativa, por ejemplo las cuentas por cobrar, pero no esté autorizado a acceder a otras partes del sistema, por ejemplo las nóminas. Si dicho empleado intenta acceder a una sección no autorizada escribiendo contraseñas, dicha actividad inadecuada se registra en el seguimiento de comprobación.

En sistemas de comercio electrónico, los seguimientos de comprobación se utilizan para registrar la actividad del cliente. Un seguimiento de comprobación registra el contacto inicial de un cliente con el sistema, así como las acciones subsiguientes, por ejemplo el pago y la entrega del producto o servicio. Las empresas pueden utilizar el seguimiento de comprobación para responder a cualquier consulta o reclamación. También pueden utilizar el seguimiento de comprobación para reconciliar cuentas, proporcionar información de análisis e histórica para la planificación y los presupuestos futuros, así como para proporcionar un registro de ventas en el caso de una auditoría fiscal.

Los seguimientos de comprobación también se pueden utilizar para investigar delitos informáticos a través del ciberespacio o Internet. Para descubrir a un individuo que realiza accesos delictivos en un sistema, los investigadores pueden consultar el seguimiento de comprobación que ha dejado el autor del delito. A veces los autores de delitos cibernéticos dejan, sin saberlo, seguimientos de

comprobación en anotaciones cronológicas de actividad de los proveedores de servicios de Internet o quizá a través de anotaciones cronológicas de salas de charla.

¿Qué es la confidencialidad?

La confidencialidad es el proceso mediante el cual se evita que la información delicada sea descifrada por personas a las que no está destinada dicha información. En el sistema WebSphere Commerce, es necesaria la confidencialidad cuando fluye información confidencial del navegador del usuario al servidor WebSphere Commerce, así como del servidor WebSphere Commerce al navegador del usuario. Tal como se describe en el Capítulo 17, "Habilitación de SSL para producción con IBM HTTP Server", en la página 201, la utilización de SSL (Secure Sockets Layer) proporciona confidencialidad para este escenario.

La confidencialidad es también un requisito importante en el área del gestión de sesiones. Puesto que el protocolo HTTP (Hypertext Transfer Protocol) no tiene estado, se utiliza normalmente un *cookie* para identificar de forma continua al usuario en el servidor WebSphere Commerce. Si se roba este cookie, la cuenta de usuario puede verse comprometida. Esto se conoce normalmente como *robo de sesión*. WebSphere Commerce evita el robo de sesiones utilizando las características exclusivas de las especificaciones de cookie que se describen en el Capítulo 5, "Gestión de sesiones", en la página 71.

Consideraciones acerca de la seguridad general

Valoración continua de la seguridad

Generalmente, las líneas del producto WebSphere Commerce se someten a un análisis de seguridad que realiza un grupo independiente de expertos de seguridad de IBM. Estos expertos realizan el análisis de la seguridad, tanto desde el punto de vista de un usuario que sólo tiene acceso a WebSphere Commerce mediante un navegador, como desde el punto de vista de los usuarios más privilegiados que tienen una cuenta en el mismo sistema en el que se ejecuta el servidor WebSphere Commerce. Los resultados del análisis de los expertos de seguridad se utilizan para mejorar continuamente la seguridad de WebSphere Commerce.

Mejoras de la seguridad en WebSphere Commerce 5.5

En WebSphere Commerce 5.5 se ha añadido la suscripción a grupos de políticas a la infraestructura de control de acceso.

En WebSphere Commerce 5.4, se ha aplicado una política a los recursos que son propiedad de los descendientes del propietario de políticas. Cuando las diferentes organizaciones de la misma jerarquía organizativa deseaban niveles de control de acceso resultaba difícil obtener niveles diferentes. Asimismo, si la jerarquía de organización era muy espesa, comprender todas las políticas que se aplicaban a una organización situada en los niveles inferiores de la jerarquía podía crear confusión.

Para simplificar las cosas y hacerlas más explícitas en WebSphere Commerce 5.5, las políticas se agrupan primero en grupos de políticas basados en requisitos de control de acceso y de negocio. Por ejemplo, un grupo de políticas puede tener las políticas necesarias para dar soporte a contratos, mientras que otro sólo permitirá que los usuarios registrados compren. De este modo, dependiendo de los requisitos de control de acceso y de negocio de una organización, la organización puede suscribir de forma más explícita a los grupos de políticas adecuados. Cuando una

organización se suscribe a grupos de políticas, solamente las políticas de dichos grupos de políticas se aplicarán a los recursos de la organización. Las políticas de las organizaciones predecesoras no se aplicarán. No obstante, si una organización no se suscribe explícitamente a grupos de políticas, heredará la suscripción a políticas de la predecesora más próxima suscrita.

Para obtener una visión general de los grupos de políticas, consulte el apartado ″Grupos de políticas″ del Capítulo 3, “Conceptos relacionados con la autorización”, en la página 19.

Mejoras de la seguridad en WebSphere Commerce 5.4

El apartado siguiente lista las mejoras de seguridad de WebSphere Commerce 5.4 con respecto a WebSphere Commerce Suite 5.1 y las que se han mantenido en WebSphere Commerce 5.5. La mayoría de estas mejoras se han realizado en el release de WebSphere Commerce Business Edition 5.1. Generalmente estas mejoras son aplicables al:

- Administrador de sitio de WebSphere Commerce
- Administrador del sistema
- Desarrollador de WebSphere Commerce

Tenga en cuenta que, a veces, estos roles son intercambiables.

Mejoras para el administrador de sitio

A continuación se indican mejoras de seguridad de WebSphere Commerce que están generalmente destinadas a un administrador de sitio:

Control de acceso

- **Infraestructura de control de acceso** — Una mejora clave es que en WebSphere Commerce 5.4 se ha implementado la nueva infraestructura de control de acceso y se ha mantenido en WebSphere Commerce 5.5 (junto con la nueva mejora de grupos de políticas de WebSphere Commerce 5.5). Esta nueva infraestructura utiliza políticas de control de acceso para determinar si a un determinado usuario se le permite realizar una acción determinada en un recurso determinado. La nueva infraestructura de control de acceso proporciona control de acceso detallado. Funciona conjuntamente con el control de acceso proporcionado por WebSphere Application Server, pero no lo sustituye. La nueva infraestructura de control de acceso se describe detalladamente en la Parte 3, “Administración de la autorización de seguridad”, en la página 95.

  La nueva infraestructura de control de acceso mejora el control de acceso anterior de los modos siguientes:

  Es expresiva...
  Captura la intención de una gran variedad de políticas de acceso. La infraestructura es genérica para que se pueda manejar en un amplio conjunto de grupos de usuarios, grupos de recursos, grupos de acciones y grupos de relaciones.

  Es jerárquica...
  Las políticas de control de acceso pertenecen a grupos de políticas. Los grupos de políticas a los que se suscribe una organización también se pueden aplicar implícitamente a sus suborganizaciones.

  Es personalizable...
  Las políticas de control de acceso se exteriorizan respecto al

código de aplicación, de modo que se pueden realizar cambios en las políticas sin volver a compilar el código.

Es compacta...

La nueva infraestructura se escala de forma conveniente. El número de políticas de control de acceso aumenta con el número de procesos de negocio y no con el número de objetos. La mayor parte de la infraestructura de agrupación se basa en condiciones implícitas, de forma que mientras se satisfagan las condiciones, se aplicará la política.

- **Cross-site scripting** — Rechazan cualquier petición de usuario que contenga atributos o caracteres que se hayan designado como no permitidos, utilizando el nodo de protección contra la vulnerabilidad Cross Site Scripting del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.

Autenticación

- **Almacenamiento de contraseñas** — WebSphere Commerce cifra y almacena un hash unidireccional de contraseñas utilizando el esquema hash SHA-1 de la base de datos de WebSphere Commerce, en lugar de almacenar las propias contraseñas. Esto asegura que nadie pueda descifrar las contraseñas de usuario, incluidos el administrador de sitio o del sistema.
- **Invalidación de contraseñas** — Requiere que los usuarios cambien sus contraseñas cuando se están conectando al sistema por primera vez, utilizando el nodo de Invalidación de contraseña del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.
- **Política de cuentas** — Configure una política de cuentas para el sitio a fin de definir las políticas relacionadas con las cuentas que se están usando, empleando la página Política de cuentas de la Consola de administración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.
- **Política de contraseñas** — Configure una política de contraseñas para el sitio a fin de controlar las características de selección de contraseña del usuario utilizando la página Política de contraseñas de la Consola de administración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.
- **Política de bloqueo de cuentas** — Configure una política de bloqueo de cuentas para el sitio a fin de reducir las posibilidades de que se ponga en peligro una cuenta de usuario utilizando la página de Política de bloqueo de cuentas de la Consola de administración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.

Autorización

Mandatos protegidos por contraseña — Requieren que los usuarios entren sus contraseñas si están ejecutando peticiones que ejecutan mandatos que se han designado utilizando el nodo de Mandatos protegidos por contraseña del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.

Datos cifrados

Herramienta de actualización de base de datos — Actualiza los datos cifrados tales como contraseñas e información de tarjeta de crédito, así como la clave de comerciante en una base de datos de WebSphere Commerce, utilizando el nodo de Herramienta de actualización de base de datos del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.

Gestión de sesiones

Tiempo de espera de conexión — Desconecta a un usuario que está inactivo durante un extenso periodo de tiempo y solicita que se vuelva a conectar al sistema, utilizando el nodo de Tiempo de espera de conexión. Esta mejora se invoca mediante el Gestor de configuración de WebSphere Commerce y se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.

Anotación cronológica

Registro de accesos — Identifica rápidamente cualquier amenaza para la seguridad de WebSphere Commerce habilitando el registro de accesos. Esta mejora se invoca mediante el Gestor de configuración de WebSphere Commerce y se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio”, en la página 53.

Mejoras para el administrador del sistema

Las siguientes son las mejoras de seguridad realizadas en WebSphere Commerce 5.4 y mantenidas en WebSphere Commerce 5.5 que están generalmente destinadas a un administrador de sitio:

- Una mejora importante en la seguridad consiste en la posibilidad de configurar las herramientas administrativas de WebSphere Commerce para que se ejecuten en un número de puerto no estándar (por ejemplo el puerto 8000 en lugar del puerto 443). Mediante la restricción del acceso a este puerto, puede limitar el acceso a las herramientas de administración en la red local o la intranet.
- Desde la Consola de administración de WebSphere Commerce, inicie un programa de seguridad que comprueba y suprime archivos temporales de WebSphere Commerce que pueden contener riesgos potenciales de seguridad, utilizando la página Iniciar comprobación de seguridad.

Mejoras para el programador de WebSphere Commerce

Una mejora clave es que en WebSphere Commerce 5.4 se había implementado una infraestructura de control de acceso nueva que se ha mantenido en WebSphere Commerce 5.5. Esta nueva infraestructura utiliza políticas de control de acceso para determinar si a un determinado usuario se le permite realizar una acción determinada en un recurso determinado. La nueva infraestructura de control de acceso proporciona control de acceso detallado. Funciona conjuntamente con el control de acceso proporcionado por WebSphere Application Server, pero no lo sustituye. La nueva infraestructura de control de acceso se describe detalladamente en la Parte 3, “Administración de la autorización de seguridad”, en la página 95.

La nueva infraestructura de control de acceso mejora el control de acceso anterior de los modos siguientes:

Es expresiva...

Captura la intención de una gran variedad de políticas de acceso. La infraestructura es genérica para que se pueda manejar en un amplio conjunto de grupos de usuarios, grupos de recursos, grupos de acciones y grupos de relaciones.

Es jerárquica...
Las políticas de control de acceso que son propiedad de una organización también se aplican a las suborganizaciones.

Es personalizable...
Las políticas de control de acceso se exteriorizan respecto al código de aplicación, de modo que se pueden realizar cambios en las políticas sin volver a compilar el código.

Es compacta...
La nueva infraestructura se escala de forma conveniente. El número de políticas de control de acceso aumenta con el número de procesos de negocio y no con el número de objetos. La mayor parte de la infraestructura de agrupación se basa en condiciones implícitas, de forma que mientras se satisfagan las condiciones, se aplicará la política.

Para obtener más información sobre las consideraciones de seguridad para programadores, consulte la publicación *WebSphere Commerce, Guías de programación y aprendizaje*.

Mejoras de seguridad en WebSphere Commerce Suite 5.1 Pro Edition

Mientras que Commerce Suite 5.1 representaba una nueva arquitectura de comercio electrónico y era una reescritura completa de Commerce Suite 4.1 basado en C++, contenía al mismo tiempo todas las características de seguridad de las versiones anteriores de WebSphere Commerce Suite y añadía mejoras de seguridad nuevas. WebSphere Commerce 5.5 ha heredado dichas mejoras.

Commerce Suite 5.1 continuaba la protección frente al acceso no autorizado a los recursos de los administradores y comerciantes de WebSphere Commerce Suite que proporcionaban los releases anteriores realizando lo siguiente:

- Continuaba dando soporte a las características de control de acceso que aseguran que el usuario de WebSphere Commerce Suite esté autenticado o en modalidad SSL antes de obtener el acceso a información confidencial o de someter dicha información.
- Asignaba mandatos de WebSphere Commerce Suite a grupos, de modo que sólo el Administrador de sitio o los Administradores a nivel de tienda pudiesen ejecutar un mandato específico, siguiendo el mismo modelo que Commerce Suite 4.1.

Mejoras generales en la seguridad

Con la reescritura de Commerce Suite 5.1 en Java, se han eliminado diversos problemas inherentes de seguridad que afectan al software escrito en C++. Dado que Java no utiliza punteros, se ha eliminado el problema de desbordamiento de almacenamiento intermedio que es una vulnerabilidad de la seguridad de la mayor parte del software basado en C++. Cumpliendo con las especificaciones J2EE estándar del sector, WebSphere Commerce utiliza el sólido mecanismo de comprobación de tipos para asegurarse de que el servidor no ejecuta sentencias peligrosas especificadas por individuos malintencionados.

Se ha utilizado el algoritmo Triple DES (estándar de cifrado de datos) estándar de la industria para proteger la información confidencial en el sistema WebSphere Commerce. El paquete que contiene el algoritmo Triple DES está firmado digitalmente de forma que si dicho paquete se manipula indebidamente, el servidor WebSphere Commerce no se inicia. Estas mejoras se han mantenido en WebSphere Commerce 5.5.

Gestión de sesiones

La gestión de sesiones de WebSphere Commerce se ha reescrito por completo a fin de proporcionar la máxima seguridad, utilizando una técnica exclusiva para asegurar que no se roben los cookies. Mediante la utilización de un cookie de autenticación que sólo fluye a través de SSL (Secure Sockets Layer) y consta de una indicación de fecha y hora cifrada, el diseño de gestión de sesiones reescrito protege contra el robo de sesiones.

Autenticación

Las contraseñas del sistema y de aplicación necesarias para el servidor WebSphere Commerce durante la ejecución se han cifrado de forma segura, utilizando una clave de 128 bits especificada por el comerciante, y se almacenan en los archivos de configuración de WebSphere Commerce. La información confidencial que aparece en el recuadro de entrada de URL de los usuarios está cifrada para proteger a los compradores frente a la divulgación no autorizada de dicha información.

Anotación cronológica

En el diseño del sistema de anotación cronológica de WebSphere Commerce, la seguridad se ha considerado un aspecto clave para que la información confidencial, por ejemplo la contraseña y la información de tarjeta de crédito del comprador, no se anotara por omisión en los archivos de anotaciones cronológicas de WebSphere Commerce.

Capítulo 2. Autenticación

WebSphere Commerce considera la autenticación como el proceso mediante el cual se verifica que los usuarios y las aplicaciones son quienes afirman ser. Este apartado describe los detalles de los diversos aspectos de la autenticación de WebSphere Commerce.

Modelo de autenticación de WebSphere Commerce

El modelo de autenticación de WebSphere Commerce se basa en los conceptos siguientes:

- Mecanismos de identificación
- Mecanismos de autenticación
- Registro de usuarios

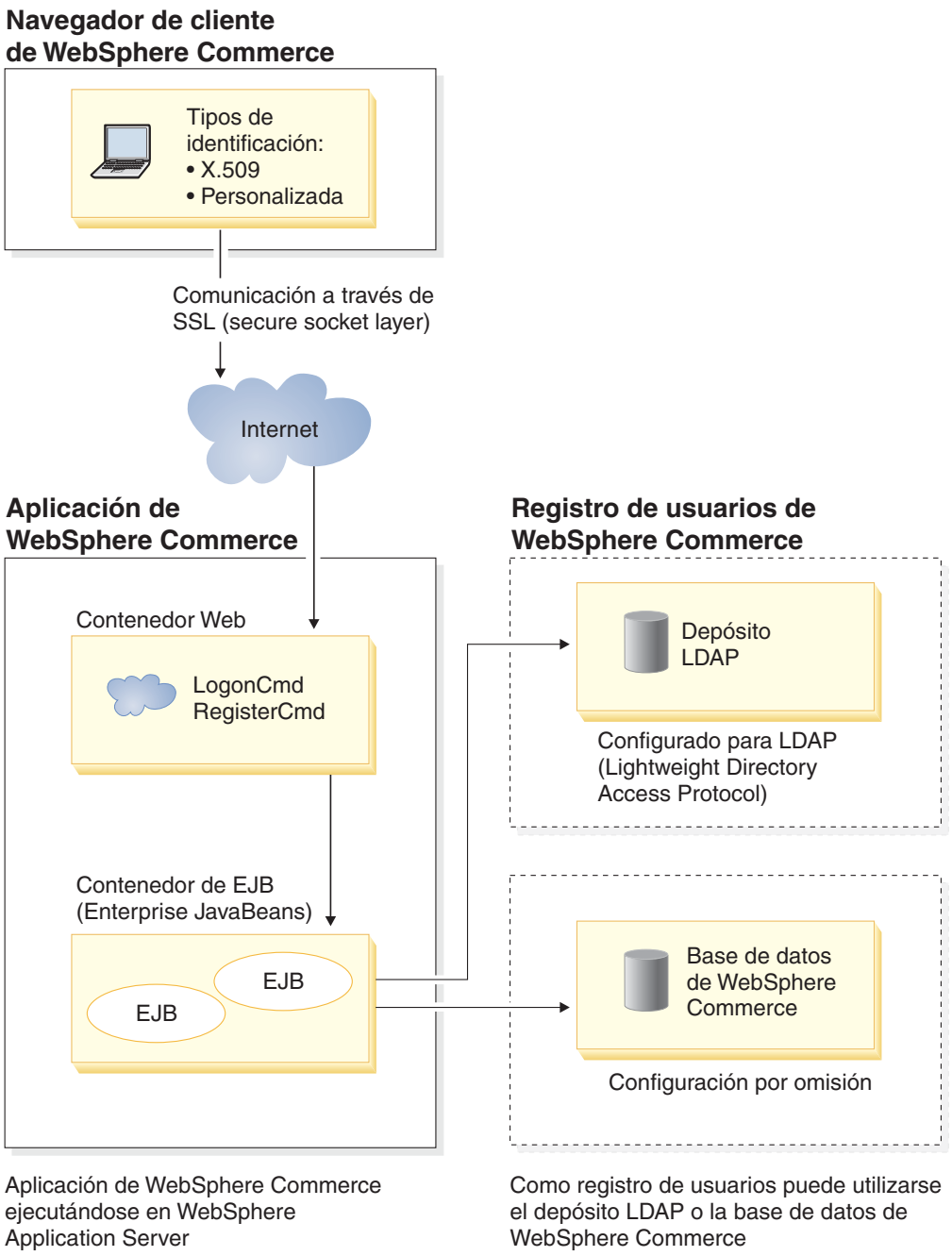


Figura 1. Modelo de seguridad de WebSphere Commerce

Mecanismos de identificación

Un mecanismo de identificación especifica cómo un servidor identifica y recupera datos de autenticación de un usuario. WebSphere Commerce da soporte a los métodos de autenticación o mecanismos de identificación siguientes:

Autenticación personalizada o basada en formulario
Este mecanismo de autenticación permite una conexión específica de sitio o tienda mediante una página HTML o un formulario JSP.

Autenticación basada en certificado (certificado X.509)
El mecanismo de identificación de certificado implica que el servidor Web esté configurado para realizar la autenticación mutua a través de SSL. Es necesario que el cliente presente un certificado a fin de establecer la conexión. Entonces este certificado se correlaciona mediante credenciales con un registro de usuarios.

Mecanismos de autenticación

Un *mecanismo de autenticación* autentica a un usuario verificando sus datos de autenticación con un registro de usuarios asociado. WebSphere Commerce emite una señal de autenticación que se asocia a un usuario en cada petición posterior, después del proceso de autenticación. Finaliza cuando el usuario se desconecta o cierra el navegador.

Validación de certificado

Es el proceso mediante el cual se verifica que el certificado de cliente X.509 es fiable para el servidor y que se adapta a la política de certificados del servidor Web. WebSphere Commerce también comprueba el certificado X.509 en la base de datos de WebSphere Commerce. El servidor Web efectúa un control de acceso general, mientras que WebSphere Commerce efectúa un control de acceso más estricto del certificado.

Enlace LDAP

Es el proceso mediante el cual se verifica que la información de identificación proporcionada es válida, realizando una operación de enlace LDAP para autenticar al usuario.

Enlace de base de datos

Es el proceso mediante el cual se verifica que el id de usuario y la contraseña que se han proporcionado durante el proceso de autenticación son válidos cuando se comparan con la información de autenticación almacenada en la base de datos de WebSphere Commerce.

Registro de usuarios

El registro de usuarios es un depósito que contiene información sobre los usuarios y la información de autenticación del usuario (por ejemplo, la contraseña). La información de autenticación proporcionada por una entidad principal (es decir, la representación de un usuario humano o una entidad de sistema en un registro de usuarios) puede verificarse o validarse en relación al registro de usuarios.

WebSphere Commerce soporta los registros de usuarios basados en dos dominios de usuarios: registro de usuarios de LDAP y la base de datos de WebSphere Commerce.

WebSphere Commerce soporta los siguientes proveedores LDAP:

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

Credenciales

El servidor WebSphere Commerce soporta mecanismos de autenticación basados en la validación de credenciales, por ejemplo certificados, señales o parejas de ID de usuario y contraseña. Las credenciales se verifican en un registro de usuarios que soporta un esquema de este tipo.

Señal de WebSphere Commerce

WebSphere Commerce utiliza un cookie de autenticación seguro para gestionar los datos de autenticación. El cookie de autenticación sólo se desplaza por SSL e incorpora la indicación de la hora para conseguir el máximo de seguridad. Este cookie se utiliza para autenticar al usuario bajo conexiones SSL, siempre que se ejecuta un mandato relacionado con datos confidenciales; por ejemplo el mandato `DoPaymentCmd` que solicita el número de tarjeta de crédito de un usuario. Existe un riesgo mínimo de que un usuario no autorizado pueda robar y utilizar este cookie.

Se utiliza un segundo cookie que se desplaza entre el navegador y el servidor, bajo conexiones SSL o no SSL, para verificar el usuario bajo conexiones no SSL.

Señal LTPA de WebSphere Application Server

Una señal LTPA son datos que contienen información de usuario necesaria para determinar permisos de acceso para un recurso que ha solicitado el usuario. Contiene los datos de autenticación junto con la firma digital del servidor LTPA de WebSphere Application Server.

En el caso del esquema de Lightweight Third Party Authentication de WebSphere Application Server, un directorio de LDAP que contenga la información acerca de los usuarios es el registro de usuarios en el que se realiza la autenticación. El servidor de recursos se pone en contacto con el Servidor de seguridad de WebSphere Application Server y especifica que LTPA es el mecanismo de autenticación. También proporciona los datos de autenticación asociados con la petición. Entonces el Servidor de seguridad de WebSphere Application Server valida los datos de autenticación en el servidor LTPA y devuelve una señal LTPA.

ID de conexión único

La filosofía en la que se basa el ID de conexión único de HTTP es conservar la autenticación de usuario en varias aplicaciones Web. La finalidad es no tener que solicitar al usuario las credenciales de seguridad varias veces en un dominio fiable determinado que incluya:

- Servidores WebSphere Application Server cooperadores pero diferentes
- Aplicaciones cooperadoras como, por ejemplo, servidores LDAP como IBM SecureWay Directory Server.

En un entorno de ID de conexión único (SSO), se utiliza un cookie HTTP para propagar la información de autenticación de un usuario a servidores Web diferentes evitándole al usuario tener que entrar la información de autenticación para cada nueva sesión de cliente-servidor (presuponiendo una autenticación básica).

Si desea conocer los pasos a realizar para implementar el ID de conexión único con WebSphere Commerce, consulte el Capítulo 7, “ID de conexión único”, en la página 87.

Políticas de autenticación

Una política de autenticación es un conjunto de normas que WebSphere Commerce aplica al proceso de autenticación y a la verificación de los datos de autenticación. WebSphere Commerce soporta políticas de cuentas, otras políticas relacionadas con la autenticación y políticas de sesión, tal como se describe en las secciones siguientes.

Políticas de cuentas

Las secciones siguientes describen las políticas de cuentas disponibles con WebSphere Commerce:

Política de cuentas

La página Política de cuentas de la Consola de administración de WebSphere Commerce le permite configurar una política de cuentas. Una política de cuentas define las políticas relacionadas con las cuentas, por ejemplo las políticas de contraseñas y de bloqueo de cuentas.

Una vez que haya creado una política de cuentas, puede asignarla a un usuario. Tenga en cuenta que no puede suprimir una política de cuentas si ésta se está utilizando (es decir, la política de cuentas se ha asignado a un usuario).

Para obtener información sobre cómo crear políticas de cuentas, consulte el apartado “Configuración de la política de cuentas” en la página 64.

Consulte también el tema de referencia ″Políticas de autenticación por omisión″ en la ayuda en línea de WebSphere Commerce.

Política de bloqueo de cuentas

La página Política de bloqueo de cuentas de la Consola de administración de WebSphere Commerce le permite configurar una política de bloqueo de cuentas para diferentes roles de usuario en WebSphere Commerce. Si se inician acciones malintencionadas contra una cuenta de usuario, la política de bloqueo de cuentas inhabilita dicha cuenta a fin de reducir las posibilidades de que las acciones la pongan en peligro.

La política de bloqueo de cuentas impone los elementos siguientes:

- El umbral de bloqueos de cuenta. Es el número de intentos de conexión no válidos antes de que se inhabilite la cuenta.
- Retardo de conexiones no satisfactorias consecutivas. Es el periodo de tiempo durante el cual no se permite que el usuario se conecte, después de dos intentos de conexión anómalos. El retardo se incrementa en el valor de retardo de tiempo configurado (por ejemplo 10 segundos) con cada anomalía de conexión consecutiva.

Para obtener información sobre cómo crear políticas de bloqueo de cuentas, consulte el apartado “Configuración de una política de bloqueo de cuentas” en la página 66.

Política de contraseñas

La página Política de contraseñas de la Consola de administración de WebSphere Commerce le permite controlar la selección de contraseña de un usuario con el fin de definir las características de la contraseña para asegurarse de que ésta cumple con la política de seguridad del sitio.

Esta característica define los atributos que debe satisfacer la contraseña. La política de contraseñas impone las condiciones siguientes:

- Si el ID de usuario y la contraseña pueden coincidir.
- Número máximo de apariciones de caracteres consecutivos.
- Número máximo de apariciones de cualquier carácter.
- Duración máxima de las contraseñas.
- Número mínimo de caracteres alfabéticos.
- Número mínimo de caracteres numéricos.
- Longitud mínima de la contraseña.
- Si se puede volver a utilizar la contraseña anterior del usuario.

Para obtener información sobre cómo crear políticas de contraseñas, consulte el apartado “Configuración de una política de contraseñas” en la página 65.

Consulte también el tema de referencia ″Políticas de autenticación por omisión″ en la ayuda en línea de WebSphere Commerce.

Otras políticas relacionadas con la autenticación

Las secciones siguientes describen las otras políticas relacionadas con la autenticación, disponibles con WebSphere Commerce:

Invalidación de contraseña

Utilice el nodo de Invalidación de contraseña del Gestor de configuración para habilitar o inhabilitar la característica de invalidación de contraseña. Esta característica, cuando está habilitada, requiere que los usuarios de WebSphere Commerce cambien su contraseña si la contraseña del usuario ha caducado. En ese caso, se redirige al usuario a una página en la que se le pide que cambie su contraseña. Los usuarios no podrán acceder a ninguna página segura del sitio hasta que hayan cambiado la contraseña.

Para obtener información sobre cómo utilizar el nodo de Invalidación de contraseña, consulte el apartado “Activación de la invalidación de contraseña” en la página 58.

Mandatos protegidos por contraseña

Utilice el nodo de Mandatos protegidos por contraseña del Gestor de configuración para habilitar o inhabilitar la característica de mandatos protegidos por contraseña. Cuando está habilitada esta característica, WebSphere Commerce requiere que los usuarios que están conectados a WebSphere Commerce entren su contraseña antes de continuar una petición que ejecute mandatos de WebSphere Commerce designados.

Precaución: Cuando configure los mandatos protegidos por contraseña, algunos de los mandatos mostrados en la lista de selección de mandatos pueden ser ejecutados por usuarios genéricos o invitados. Si se configuran dichos mandatos como protegidos por contraseña, se prohibirá a los usuarios genéricos e invitados que los ejecuten. Por consiguiente, deberá tener cuidado cuando configure mandatos para que estén protegidos por contraseña.

Nota: WebSphere Commerce sólo mostrará los mandatos que se han designado como `autenticados` o los que tienen establecido el distintivo `https` en la tabla `URLREG` de la lista de mandatos disponibles.

Para obtener información sobre cómo utilizar el nodo de Mandatos protegidos por contraseña, consulte el apartado “Habilitación de mandatos protegidos por contraseña” en la página 58.

Políticas de sesión

En WebSphere Commerce, las políticas de sesión se incluyen en la política de tiempo de espera de conexión.

Con la política de tiempo de espera de conexión, WebSphere Commerce desconectará a un usuario que esté inactivo durante un largo periodo de tiempo y le solicitará que vuelva a conectarse al sistema utilizando el nodo de Tiempo de espera de conexión. Esta mejora se invoca mediante el Gestor de configuración de WebSphere Commerce y se describe detalladamente en el apartado “Habilitación del tiempo de espera de conexión” en la página 57.

Capítulo 3. Conceptos relacionados con la autorización

En WebSphere Commerce el control de acceso o la autorización es el proceso de verificar si los usuarios o las aplicaciones tienen la autorización suficiente para acceder a un recurso. Este apartado describe detalladamente diversos aspectos del control de acceso en WebSphere Commerce.

El control de acceso o la autorización en WebSphere Commerce se ejecuta utilizando las políticas de control de acceso. Una política de control de acceso es una norma que describe qué grupo de usuarios tiene autorización para realizar un conjunto de actividades en un conjunto de recursos. WebSphere Commerce proporciona un conjunto de políticas de control de acceso por omisión. Estas políticas de control de acceso por omisión se especifican en formato XML y están diseñadas para cubrir muchos de los requisitos de control de acceso habituales que necesita un sitio de comercio electrónico.

Modelos de negocio

En WebSphere Commerce 5.4, después de crear la instancia el administrador de sitio ha de tomar las decisiones siguientes:

1. La estructura organizativa correcta del sitio
2. Los roles que se han de asignar a las organizaciones concretas
3. Las políticas de control de acceso necesarias

Una vez tomadas todas las decisiones, la tienda se puede publicar en la organización adecuada.

En WebSphere Commerce 5.5, este proceso se ha simplificado mediante los modelos de negocio. Un modelo de negocio proporciona la estructura, los roles, las políticas de control de acceso y las tiendas predefinidas de la organización a las que va dirigida una solución de comercio electrónico específica. Los modelos de negocio se pueden utilizar en la fase de desarrollo como una base a la que se puede añadir contenido o cuyo contenido se puede suprimir o modificar.

En WebSphere Commerce 5.5 están disponibles los siguientes modelos de negocio:

- Directo al consumidor
- Directo a B2B
- Cadena de demanda
- Alojamiento
- Cadena de oferta

Para comprender los modelos de negocio y el componente de control de acceso de WebSphere Commerce, en primer lugar, es necesario comprender la jerarquía organizativa típica de un sitio de comercio electrónico.

Nota: Para obtener más información sobre los modelos de negocio, consulte la publicación *WebSphere Commerce, Conceptos básicos*.

Jerarquía organizativa

Los usuarios y las entidades de organización del subsistema de miembros de WebSphere Commerce están organizados en una jerarquía. Esta jerarquía imita una jerarquía de organización típica, con entradas para las organizaciones y las unidades de organización y entradas para los usuarios de los nodos finales. La jerarquía incluye en la parte superior una entidad de organización artificial denominada *organización raíz*. Todas las otras entidades de organización y los usuarios son descendientes de esta organización raíz. Bajo la organización raíz puede haber una organización vendedora y varias organizaciones compradoras. Debajo de todas estas organizaciones pueden haber una o varias suborganizaciones. Los administradores de los compradores o vendedores son los jefes de las organizaciones y son los responsables del mantenimiento de sus organizaciones. En la parte de la organización vendedora, cada suborganización puede incluir una o varias tiendas. Los administradores de tienda son los responsables del mantenimiento de las tiendas. El diagrama siguiente muestra la jerarquía de organizaciones de un sitio de comercio electrónico de empresa a empresa.

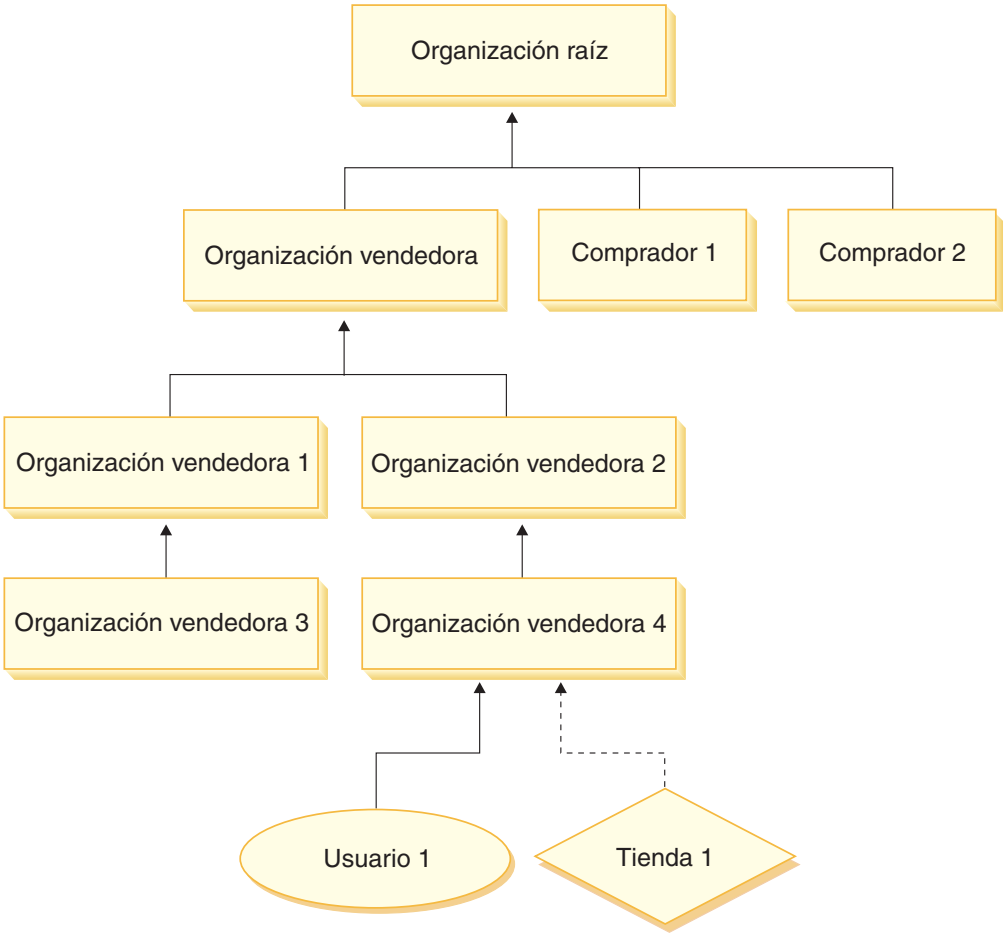


Figura 2. Jerarquía organizativa de un sitio de empresa a empresa

Organización raíz

La organización raíz está en el nivel superior de la jerarquía organizativa. Un administrador de sitio tiene acceso de superusuario para realizar cualquier operación en WebSphere Commerce. El Administrador de sitio instala, configura y

mantiene WebSphere Commerce y su software y hardware asociados. Normalmente, este rol controla los accesos y las autorizaciones (creando y asignando a los miembros el rol adecuado) y gestiona el sitio Web. El Administrador de sitio puede asignar roles a usuarios y especificar la o las organizaciones en las que el usuario tiene este rol. El Administrador de sitio debe asignar una contraseña a cada administrador para asegurarse de que solamente las partes autorizadas acceden a la información confidencial. Esto proporciona un modo de controlar las responsabilidades clave, como actualizar un catálogo o aprobar una RFQ (solicitud de presupuesto).

Nota: Un usuario puede tener roles en una organización que no sea su organización padre.

En un sitio de WebSphere Commerce, hay una organización vendedora. En un sitio de empresa a empresa, también hay una o varias organizaciones compradoras. El Administrador de sitio debe definir tanto las políticas de control de acceso de la organización vendedora (la propietaria de la tienda) como las políticas de control de acceso de cada organización que realiza compras en la tienda. En un sitio de empresa a consumidor, no hay organizaciones compradoras. Los clientes de un sitio de empresa a consumidor se consideran miembros de la organización por omisión.

Organizaciones (parte vendedora)

Tanto en los sitios de empresa a empresa como en los sitios de empresa a consumidor, el Administrador de sitio crea un vendedor de nivel superior. Debajo de esta organización vendedora se pueden crear otras suborganizaciones o unidades organizativas. Cualquiera de estas entidades de organización de la parte vendedora puede ser la propietaria de una o varias tiendas. A continuación, el Administrador de sitio define cualquier política de control de acceso especial para una organización vendedora y asigna un Administrador de vendedores para la gestión de dicha organización. El Administrador de vendedores registra a los usuarios y les asigna distintos roles que se ajustan a las necesidades de negocio de la organización, dependiendo de las políticas de control de acceso asociadas a dicha organización.

Las responsabilidades del administrador de vendedores podrían resumirse del modo siguiente:

- Crear suborganizaciones que puedan ser propietarias de tiendas. Opcionalmente, definir qué procesos de la organización es preciso aprobar. Este paso sólo es necesario en un sitio de empresa a empresa.
- Asignar roles a las suborganizaciones.
- Crear usuarios.
- Asignar roles a los usuarios.

Organizaciones (parte compradora)

En un sitio de empresa a empresa, el Administrador de sitio crea una o varias organizaciones compradoras, dependiendo de las necesidades del negocio. A continuación, el Administrador de sitio define cualquier política de control de acceso de una organización compradora y asigna al Administrador de compradores la gestión de la organización compradora. El Administrador de compradores registra a los usuarios y les asigna roles diferentes que se ajustan a las necesidades de negocio de la organización, dependiendo de las políticas de control de acceso asociadas a dicha organización.

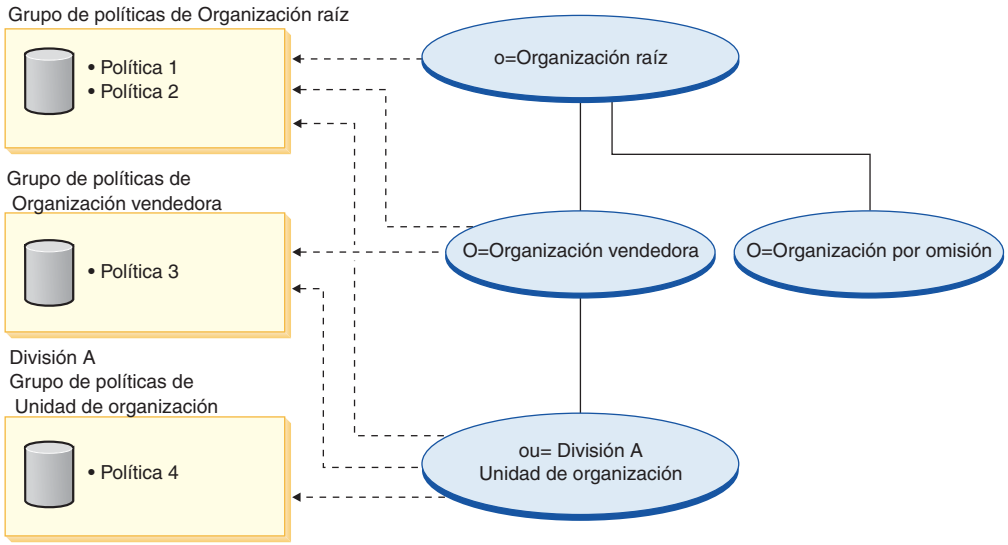
Las responsabilidades del administrador de compradores se pueden resumir del modo siguiente:

- Crear y administrar las suborganizaciones de la organización compradora. Opcionalmente, definir qué procesos de la organización es preciso aprobar. Este paso sólo es necesario en un sitio de empresa a empresa.
- Asignar roles a las suborganizaciones.
- Crear usuarios.
- Asignar roles a los usuarios.

Nota: El Administrador de sitio puede modificar y gestionar las políticas de control de acceso de la organización compradora, si resulta adecuado. Para obtener más información acerca de las tareas del Administrador de sitio, consulte la ayuda en línea de WebSphere Commerce.

Grupos de políticas

WebSphere Commerce 5.5 da soporte a varios modelos de negocio y cada modelo de negocio tiene su propio conjunto de políticas de control de acceso. Para agrupar los conjuntos de políticas en los modelos se han creado grupos de políticas. Las políticas se asignan explícitamente a los grupos de políticas adecuados y, a continuación, las organizaciones se pueden suscribir a uno o varios de estos grupos de políticas. Por ejemplo, en el diagrama siguiente, la organización vendedora se suscribe al grupo de políticas de la organización vendedora y al grupo de políticas de la organización raíz.

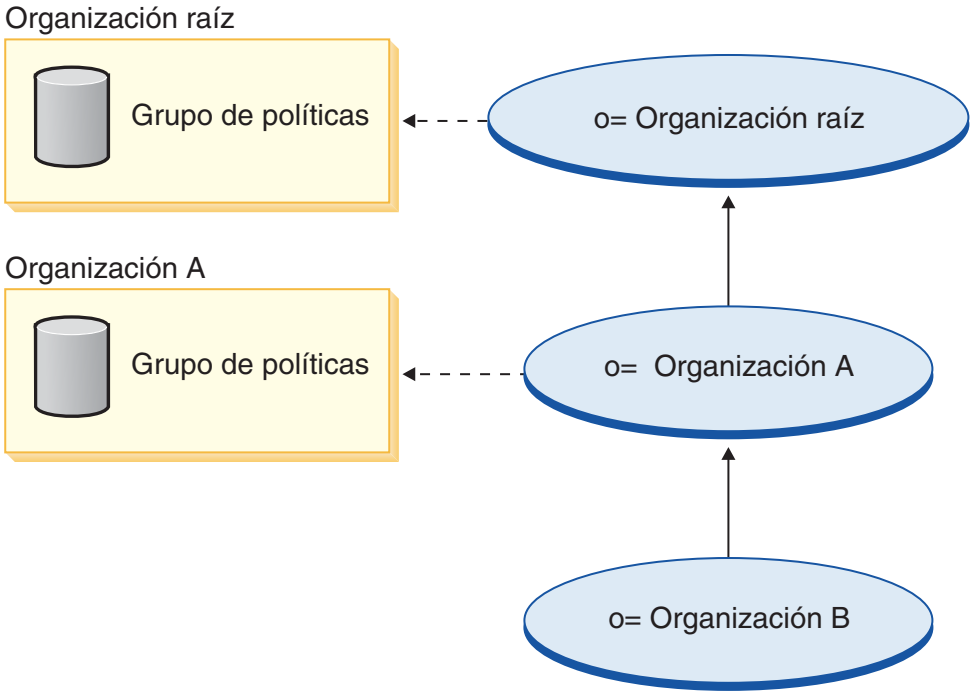


Las políticas se asignan a grupos de políticas. Por ejemplo, en el diagrama anterior, se asignan la política 1 y la política 2 al grupo de políticas de la organización raíz, la política 3 se asigna al grupo de políticas de la organización vendedora y la política 4 se asigna al grupo de políticas de la unidad organizativa del departamento A.

Suscripción a grupos de políticas

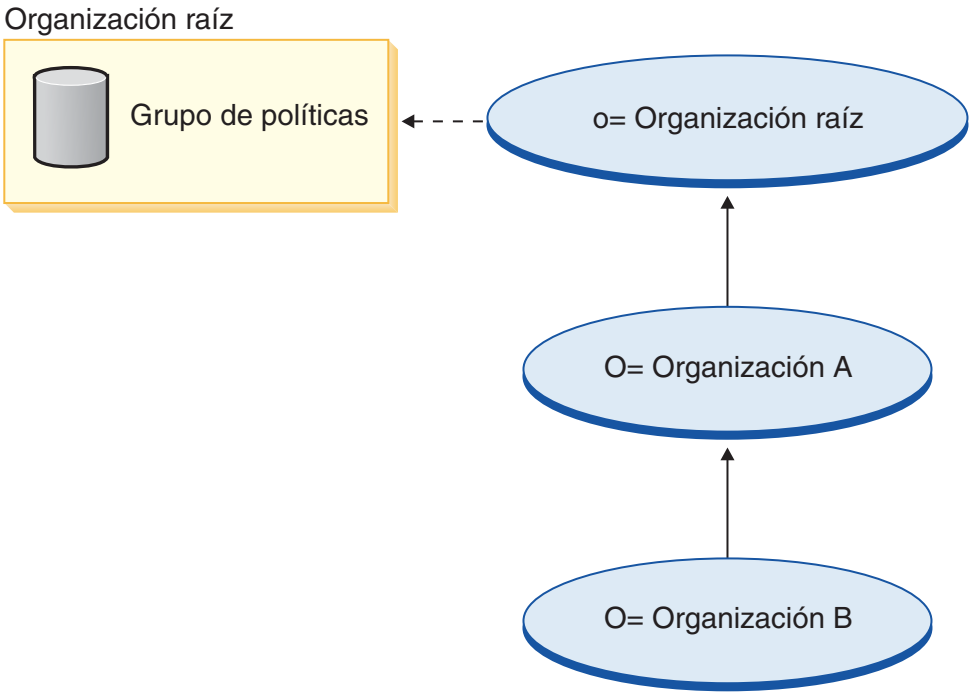
En las versiones anteriores de WebSphere Commerce se aplicaba una política a todos los recursos propiedad de los descendientes de la organización propietaria de dicha política. Por ejemplo, si la organización A tenía una política determinada y era la organización padre de la organización B entonces, de forma implícita, la organización B tenía también dicha política. En WebSphere Commerce 5.5, las

organizaciones se pueden suscribir a grupos de políticas. En WebSphere Commerce 5.5 si la organización B no se suscribe a ningún grupo de políticas, la infraestructura de control de acceso comienza a buscar en sentido ascendente en la jerarquía organizativa hasta que encuentra una organización que se suscriba como mínimo a un grupo de políticas. Si la organización padre inmediata con respecto a la organización B, esto es, la organización A, se suscribe a un grupo de políticas, la búsqueda se detiene y se aplican las políticas a la organización A y B.

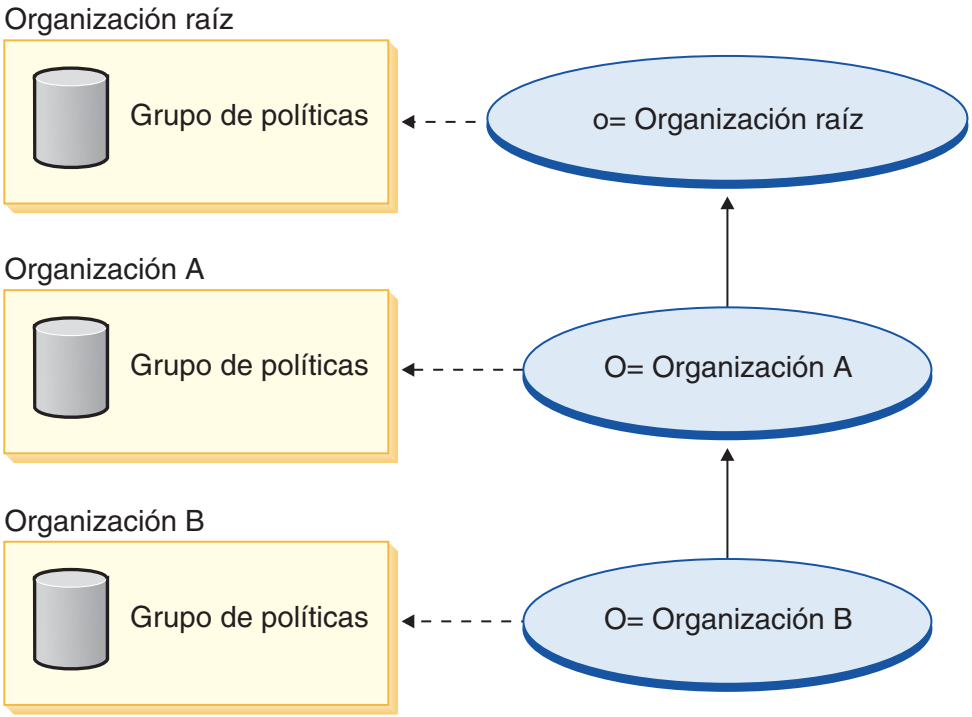


Si la organización A no se suscribe a un grupo de políticas, la búsqueda continúa por la jerarquía de la organización hasta que se encuentra una organización con una suscripción. Esto puede observarse en el diagrama siguiente en el que la organización raíz se suscribe a un grupo de políticas. Las políticas de dicho grupo

se aplican a la organización B y a la organización A.



Si la organización B se suscribe a un grupo de políticas, la búsqueda termina en la organización B. De modo que las políticas del grupo de políticas de la organización B sólo se podrán aplicar a la organización B.



Política de control de acceso

Una política de control de acceso autoriza a un grupo de usuarios a realizar acciones concretas en un grupo de recursos de WebSphere Commerce. A no ser que estén autorizados mediante una o más políticas de control de acceso, los usuarios no tienen acceso a ninguna función del sistema. Para comprender las políticas de control de acceso debe comprender cuatro conceptos importantes: usuarios, acciones, recursos y relaciones. Los usuarios son las personas que utilizan el sistema. Los recursos son los objetos del sistema que deben protegerse. Las acciones son las actividades que los usuarios pueden efectuar en los recursos. Las relaciones son condiciones opcionales que existen entre usuarios y recursos.

Elementos de una política de control de acceso

Una política de control de acceso se compone de cuatro elementos:

Grupo de acceso
El grupo de usuarios al que se aplica la política.

Grupo de acciones
El grupo de acciones que el usuario realiza en los recursos.

Grupo de recursos
Los recursos controlados por la política. Un grupo de recursos puede incluir objetos de negocio, tales como un `contrato` o `pedido`, o un conjunto de mandatos relacionados como, por ejemplo, todos los mandatos relacionados con una subasta que pueden ejecutar los usuarios que tienen un rol determinado.

Relaciones (opcional)
Cada clase de recurso puede tener asociado un conjunto de relaciones. Cada recurso puede tener un conjunto de miembros que complementan cada relación. Por ejemplo, una política puede especificar que solamente el creador de un pedido puede modificarlo. En este caso, la relación sería la de `creador` y existiría entre el usuario y el recurso de pedido.

Conceptos de las políticas de control de acceso

Las políticas de control de acceso permiten a los usuarios acceder a su sitio. A menos que se les haya autorizado a llevar a cabo sus responsabilidades, mediante una o varias políticas de control de acceso, los usuarios no pueden acceder a ninguna de las funciones del sitio.

Las políticas de control de acceso tienen el formato siguiente:

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

Los elementos de la política de control de acceso especifican que un usuario que pertenece a un grupo determinado de usuarios puede llevar a cabo las acciones del grupo de acciones especificado, en los recursos pertenecientes al grupo de recursos especificado, siempre que el usuario satisfaga una relación determinada con respecto al recurso. La relación solamente se especifica cuando se necesita. Por ejemplo, `[AllUsers,UpdateDoc,doc,creator]` especifica que todos los usuarios pueden actualizar un documento, si son los creadores del mismo.

Los apartados siguientes describen los conceptos y la terminología asociada al control de acceso.

Grupos de miembros

El subsistema de miembros de WebSphere Commerce también le permite crear grupos de miembros, que son usuarios agrupados en categorías por diferentes

motivos comerciales. Las agrupaciones pueden utilizarse para distintas finalidades como, por ejemplo, control de acceso, aprobación y marketing, que incluye el cálculo de descuentos y precios y la visualización de productos. Un grupo de miembros de tipo Grupo de acceso (-2) se utiliza para fines de control de acceso, mientras que un grupo de miembros de tipo Grupo de usuarios (-1) se crea con fines de uso general. Un grupo de miembros se asocia a los tipos de grupos de miembros de la tabla MBRGRPUSG.

Grupos de acceso: Un grupo de miembros de tipo Grupo de acceso (-2) se utiliza para agrupar usuarios para fines de control de acceso. Un grupo de acceso es un elemento de una política de control de acceso. Los criterios para los miembros de un grupo de acceso normalmente están basados en roles, en la organización a la que pertenece el usuario y en el estado de registro del usuario. Por ejemplo, un grupo de miembros llamado Administradores de vendedores es un grupo cuyos usuarios desempeñan el rol de Administrador de vendedores.

WebSphere Commerce incluye varios roles por omisión y a cada rol le corresponde un grupo de acceso por omisión que hace referencia implícitamente a este rol. Los roles se pueden utilizar como atributos para añadir usuarios a un grupo de acceso basándose en el tipo de actividades que realizan en el sitio. Por ejemplo, por omisión hay un rol llamado Administrador de vendedores y un grupo de miembros correspondiente llamado Administradores de vendedores. Un administrador de sitio utiliza la Consola de administración para crear, mantener y suprimir grupos de acceso para un sitio. Un administrador de sitio, un administrador de compradores, un administrador de vendedores o gestor de canales utiliza la Consola de administración de organizaciones de WebSphere Commerce para asignar roles a los usuarios o para asignar explícitamente usuarios a los grupos de acceso.

Grupo de acceso implícito: Un grupo de acceso implícito se define mediante un conjunto de criterios. Cualquiera que satisfaga el criterio es un miembro del grupo. El criterio suele estar basado en los roles de un usuario, en la organización padre o en el estado de registro. Las condiciones implícitas que definen a los miembros de un grupo de miembros están incluidas en la columna CONDITIONS de la tabla MBRGRPCOND. Utilizar grupos de acceso implícitos que especifican los atributos de usuarios, permite autorizar fácilmente el acceso a usuarios similares sin tener que asignar ni desasignar explícitamente usuarios individuales. También elimina la necesidad de actualizar los miembros de un grupo cuando se modifican los atributos de un usuario. Asimismo, dado que varios grupos de acceso pueden hacer referencia al mismo atributo de usuario, al asignar un atributo a un usuario se puede incluir implícitamente dicho usuario en varios grupos de acceso. Un criterio sencillo para un grupo de acceso es incluir a todos a los que se ha asignado un rol específico, independientemente de la organización para la que el usuario desempeña el rol. Un criterio más complejo será especificar que solamente los usuarios que desempeñan uno de los roles de un conjunto de roles posibles para una organización determinada pueden pertenecer al grupo de acceso.

Grupo de acceso explícito: También se puede añadir o suprimir de forma explícita un usuario de un grupo de miembros. Estas dos especificaciones explícitas se pueden llevar a cabo mediante la tabla MBRGRPMBR. Un grupo de acceso explícito contiene usuarios asignados explícitamente que pueden compartir o no atributos comunes. También permite excluir a los individuos que, aunque satisfacen las condiciones de inclusión en un grupo definido implícitamente, desea excluir.

Grupos de usuarios: Un grupo de miembros de tipo Grupo de usuarios (-1) es un conjunto de usuarios, definido por el comerciante, que comparten un interés

común. Los grupos de usuarios son similares a los clubes que ofrecen los grandes almacenes para sus clientes habituales o preferidos. El hecho de formar parte de un grupo de usuarios da derecho a los clientes a descuentos u otras ventajas para comprar productos. Por ejemplo, si la investigación de mercado muestra que los clientes de más edad compran repetidamente libros de viajes y equipaje, puede asignar estos clientes a un grupo de miembros llamado `Club de viajes de la tercera edad`. Del mismo modo, puede crear un grupo de usuarios para recompensar a los clientes habituales.

Acciones

Generalmente, una acción es una operación que se lleva a cabo en un recurso. En las políticas basadas en roles para mandatos de controlador, la acción es `Execute` y el recurso es el mandato que se ejecuta. En las políticas basadas en roles para Vistas, la acción es el nombre de la vista y el recurso es `com.ibm.commerce.commands.ViewCommand`. En el control de acceso a nivel de recursos, las acciones generalmente se correlacionan con mandatos de WebSphere Commerce y el recurso generalmente es la interfaz remota de un EJB (Enterprise Java Bean) protegido. Por ejemplo, el mandato de controlador `com.ibm.commerce.order.commands.OrderCancelCmd` funciona en el recurso `com.ibm.commerce.order.objects.Order`. Por último, la acción `Display` se utiliza para activar los recursos de bean de datos.

Un Administrador de sitio puede utilizar la Consola de administración de WebSphere para asociar acciones existentes con grupos de acciones, pero no para crear acciones nuevas. Se pueden crear acciones nuevas definiéndolas en un archivo XML y, a continuación, cargándolas en la base de datos. Las acciones se almacenan en la tabla `ACACTION`.

Grupos de acciones

Los grupos de acciones son conjuntos de acciones relacionadas. Un ejemplo de un grupo de acciones es el grupo `AccountManage` que incluye los mandatos siguientes:

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

Sólo el Administrador de sitio puede crear, actualizar y suprimir los grupos de acciones. Esto puede llevarse a cabo desde la Consola de administración de WebSphere y mediante XML. Los grupos de acciones se almacenan en la tabla `ACACTGRP`. Las acciones se asocian con grupos de acciones de la tabla `ACACTACTGP`.

Categoría de recursos

Una categoría de recursos hace referencia a una clase de recursos que deben protegerse mediante el control de acceso. Los recursos deben implementar la información de la interfaz Protectable. Las categorías de recursos son clases Java como, por ejemplo, pedido, RFQ y subasta. Los recursos son las instancias de estas clases. Por ejemplo, Auction1 creado por el Administrador de subastas A es un recurso; Auction2 creado por el Administrador de subastas B es otro recurso. Estos dos recursos pertenecen a la categoría de recursos: auction.

Nota: Para obtener más información acerca de la interfaz Protectable, consulte la publicación *IBM WebSphere Commerce, Guía del programador*.

Las categorías de recursos se definen en la tabla `ACRESCGRY` y por comodidad, a veces, se hace referencia a las mismas como recursos. Un Administrador de sitio puede asociar las categorías de recursos existentes con los grupos de recursos, utilizando la Consola de administración de WebSphere Commerce. Mediante XML se pueden crear nuevas categorías de recursos.

Recursos

Los recursos son los objetos del sistema que deben protegerse. Por ejemplo, RFQ, subastas, usuarios y pedidos son algunos de los recursos de WebSphere Commerce que deben protegerse. Cada recurso tiene un propietario. La propiedad del recurso puede utilizarse para determinar las políticas de control de acceso que se le aplican. Las políticas de control de acceso tienen un propietario, que es una entidad de organización. Una política solamente se aplica a los recursos cuyos propietarios son la misma entidad organizativa que se ha suscrito a un grupo de políticas que contiene la política. Si la organización que posee dicho recurso no se ha suscrito a ningún grupo de políticas, entonces se aplican las políticas de los grupos de políticas a los que se ha suscrito la organización predecesora más próxima.

Recursos de mandatos de controlador: En el control de acceso basado en roles para mandatos de controlador, la política se estructura de tal modo que la acción `Execute` se realiza en el recurso de mandato de controlador. Estas políticas están diseñadas para limitar la ejecución de los mandatos de controlador a los usuarios que tienen un rol especificado. El grupo de acceso de estas políticas generalmente es para los que tienen un único rol, por ejemplo, los jefes de producto (los que tienen el rol de Jefe de producto). A continuación, el grupo de recursos deberá ser el conjunto de mandatos de controlador que puede ejecutar un jefe de producto.

Mientras se pone en vigor un control de acceso basado en roles en un mandato del controlador, se debe determinar el propietario del mandato. Esto se efectúa llamando al método `getOwner()` en el mandato, si se ha implementado. Generalmente, este método no se implementa, por lo tanto, durante la ejecución de WebSphere Commerce se evaluará mediante uno de los métodos siguientes:

- Utilizando la organización propietaria de la tienda que actualmente está en el contexto del mandato.
- Si el contexto del mandato no contiene ninguna tienda, se utilizará la organización raíz como propietario.

Recursos de beans de datos: No todos los beans de datos requieren protección. En la aplicación WebSphere Commerce existente, los beans de datos que requieren protección ya implementan el control de acceso necesario. Cuando se crean nuevos beans de datos surge la cuestión sobre qué se ha de proteger. Los recursos que se han de proteger dependen de su aplicación. Un bean de datos debe protegerse, ya sea directa o indirectamente, si la información que debe visualizarse no está suficientemente protegida por el control de acceso basado en roles de la vista, que corresponde al archivo JSP (Java Server Page) que contiene el bean de datos.

Si un bean de datos se ha de proteger y puede existir por su cuenta, debe protegerse directamente. Si su existencia depende de la existencia de otro bean de datos, debe delegar la protección al otro bean de datos. Un ejemplo de un bean de datos que debe protegerse directamente es el bean de datos `Order`. Un ejemplo de un bean de datos que debe protegerse indirectamente es el bean de datos `OrderItem`, ya que no puede existir sin el bean de datos `Order`. Consulte la publicación *WebSphere Commerce, Guías de programación y aprendizaje* para obtener información acerca de cómo proteger el recurso de bean de datos.

Recursos de datos: Los recursos de datos hacen referencia a objetos de negocio que se pueden manipular como, por ejemplo, subastas, pedidos, RFQ y usuarios. Generalmente se protegen en el nivel de bean de negocio pero se puede proteger cualquier clase, siempre que implemente la interfaz Protectable. Los recursos de datos se protegen utilizando comprobaciones de control de acceso a nivel de recursos. El método más común de hacerlo es devolviendo recursos de datos en el

método getResources() de un controlador o mandato de tarea. Para obtener más información, consulte la publicación *WebSphere Commerce 5.4, Guía del programador*.

Grupos de recursos

Un grupo de recursos identifica un conjunto de recursos relacionados. Un grupo de recursos puede incluir objetos de negocio, por ejemplo un contrato o un conjunto de mandatos relacionados. En el control de acceso, los grupos de recursos especifican los recursos a los que la política de control de acceso autoriza el acceso.

Los grupos de recursos se definen en la tabla ACRESGRP. Los administradores de sitio pueden gestionar grupos de recursos y asociar recursos con grupos de recursos utilizando la Consola de administración de WebSphere Commerce o utilizando XML.

Grupos de recursos implícitos: Los grupos de recursos implícitos definen recursos que coinciden con un conjunto de atributos determinados. Uno de los atributos debe ser el nombre de clase Java. Otros atributos pueden ser el estado, el ID de tienda, el precio, etc. Por ejemplo, puede crear un grupo de recursos implícitos que incluya todos los pedidos que están en estado pendiente (ORDERS.STATUS=P). Los grupos de recursos implícitos se utilizan generalmente para agrupar recursos que se utilizarán en las políticas a nivel de recursos, cuando éstos comparten un atributo común además del nombre de clase Java.

Los grupos de recursos implícitos se definen utilizando la columna CONDITIONS de la tabla ACRESGRP. Los grupos de recursos implícitos simples se pueden crear mediante la Consola de administración de WebSphere Commerce. Mediante XML se pueden crear grupos cada vez más complejos.

Grupos de recursos explícitos: Los grupos de recursos explícitos se especifican asociando una o varias categorías de recursos a un grupo de recursos. Esta asociación se lleva a cabo en la tabla ACRESGPRES. La adición explícita de una categoría de recurso a un grupo, listando su nombre de clase Java, le permite agrupar recursos individuales que es posible que no compartan necesariamente atributos comunes.

Relaciones

Todos los recursos tienen algún tipo de relación asociada y un conjunto de miembros que satisfacen esa relación. Por ejemplo, todos los recursos tienen una relación de *propietario*, que la satisface el propietario del recurso. Otras relaciones pueden incluir los destinatarios de documentos y el creador de un pedido. Estas relaciones de recurso son importantes para determinar quién puede realizar determinadas acciones en una instancia concreta de un recurso. Por ejemplo, es posible que el creador de un documento no pueda suprimirlo, pero quizá sí lo pueda suprimir un auditor. De forma similar, es posible que un revisor sólo pueda leer y aprobar un documento, pero no enviarlo ni realizar otras operaciones.

Las relaciones se almacenan en la tabla ACRELATION y se especifican opcionalmente en una política de control de acceso, utilizando la columna ACRELATION_ID de la tabla ACPOLICY. Cuando se evalúa una política que requiere que se cumpla una relación entre el usuario y el recurso, se llamará al método fulfills(Long Member, String relationship) para evaluarlo. Cuando se comparan estas relaciones con los grupos de relaciones, se hace referencia a estas relaciones como relaciones simples.

Grupos de relaciones: Las políticas de control de acceso pueden especificar que un usuario debe satisfacer una relación determinada con respecto al recurso al que se está accediendo o pueden especificar que un usuario debe satisfacer las

condiciones especificadas en un grupo de relaciones. En la mayor parte de los casos, una relación es suficiente. Sin embargo, si se necesitan relaciones más complejas, se puede utilizar un grupo de relaciones. Un grupo de relaciones permite especificar varias relaciones y también una cadena de relaciones. Estas dos tareas se pueden realizar utilizando una estructura de cadena de relaciones. Una cadena de relaciones es una estructura que permite expresar una relación sencilla (directamente entre un usuario y el recurso), pero también se puede utilizar para expresar una serie de relaciones entre el usuario y el recurso. Por ejemplo, para poder expresar que un usuario debe tener un rol en una organización que tiene una relación (que no sea la relación de propietario) con el recurso, se debe utilizar un grupo de relaciones. En este ejemplo, hay una relación de rol entre el usuario y la organización y una relación entre la organización y el recurso.

Comparación de relaciones y grupos de relaciones: En la mayor parte de los casos, utilizar una relación es suficiente para satisfacer los requisitos de control de acceso de la aplicación ya que, conceptualmente, la mayor parte de las relaciones son relaciones directas entre un usuario y el recurso. Por ejemplo, la política indica que el usuario debe ser el creador del recurso. Sin embargo, si necesita especificar varias relaciones, debe utilizarse un grupo de relaciones. Por ejemplo, la política indica que el usuario debe ser el creador o el que somete el recurso.

Los grupos de relaciones también se necesitan para expresar una cadena de relaciones entre un usuario y el recurso. En una cadena de relaciones, no hay ninguna relación directa entre el usuario y el recurso, por ejemplo, un usuario pertenece a la organización compradora que especifica un pedido. En este caso, el usuario tiene una relación de hijo con la organización y dicha organización tiene una relación de organización compradora con el pedido.

Cadenas de relaciones: Cada grupo de relaciones consta de una o varias condiciones de apertura `RELATIONSHIP_CHAIN` que se agrupan mediante los elementos `andListCondition` u `orListCondition`. Una cadena de relaciones es una serie de una o varias relaciones. La longitud de una cadena de relaciones la determina el número de relaciones de que consta. Esto puede determinarse analizando el número de entradas `<parameter name= "X" value="Y">` de la representación XML de la cadena de relaciones. A continuación se muestra un ejemplo de una cadena de relaciones con una longitud de uno.

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

En las cadenas de relaciones cuya longitud es uno, el elemento `<parameter name="Relationship" value="unValor">` especifica una relación directa entre el usuario y el recurso. El atributo de valor es la serie que representa la relación entre el usuario y el recurso. También debe corresponderse con el parámetro de relación del método `fulfills()` del recurso protegible.

Cuando una cadena de relaciones tiene una longitud de dos, se trata de una serie de dos relaciones. El primer elemento, `<parameter name= "X" value="Y">`, es entre un usuario y una entidad de organización. El último elemento, `<parameter name= "X" value="Y"/>`, es entre la entidad de organización y el recurso. A continuación se muestra un ejemplo de una cadena de relaciones con una longitud de dos:

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="valor1" value="valor2"/>
<parameter name="RELATIONSHIP" value="valor3"/>
</openCondition>
```

Los valores posibles de valor1 son HIERARCHY y ROLE. HIERARCHY especifica que hay una relación jerárquica entre el usuario y la entidad de organización en la jerarquía de miembros. ROLE especifica que el usuario tiene un rol en la entidad de organización.

Si valor1 es HIERARCHY, los valores posibles son child, que devuelve la entidad de organización de la que el usuario es un hijo directo en la jerarquía de miembros. Si el valor de valor1 es ROLE, los valores posibles son cualquier entrada de la columna NAME de la tabla ROLE, que devuelve todas las entidades de organización para las que el usuario actual tiene este rol.

La entrada valor3 es una serie que representa la relación entre una o varias entidades de organización que se recuperan a partir de la evaluación del primer parámetro y el recurso. Este valor corresponde al parámetro de relación del método fulfills() del recurso protegible. Si el parámetro de evaluación, valor1 devuelve más de una entidad de organización, esta parte de RELATIONSHIP_CHAIN se satisface si como mínimo una de estas entidades de organización satisface la relación que especifica el parámetro valor2.

Nota: Un grupo de relaciones que conste de una sola cadena de relaciones con un solo elemento de parámetro, es funcionalmente equivalente a una relación simple. En este caso, resulta más fácil utilizar la relación en lugar del grupo de relaciones de la política. Para obtener más información acerca de cómo definir grupos de relaciones, consulte el apartado "Definición de grupos de relaciones" en la página 162.

Tipos de políticas de control de acceso

Hay dos tipos de políticas de control de acceso:

- Políticas estándar agrupables (tipo de política -2)
- Políticas de plantilla agrupables (tipo de política -3)

Tanto las políticas de plantilla agrupables como las políticas estándar agrupables deben pertenecer a un grupo de políticas para poder aplicarlas al sistema. Una política estándar agrupable se aplica, una vez, a las organizaciones que se suscriben a un grupo de políticas que contiene la política.

Las políticas de plantilla agrupables son de naturaleza dinámica ya que tiene un grupo de acceso que cuando el sistema está ejecutándose alcanza el ámbito de la organización propietaria del recurso. Por ejemplo, cuando este tipo de política se aplica a un recurso propiedad de la organización XYZ, debe comprobarse si el usuario desempeña uno de los roles especificados para la Organización XYZ o sus antecesores.

Políticas de control de acceso por omisión especiales

Las políticas siguientes necesitan una descripción adicional:

- La política en la que los administradores de sitio pueden hacerlo todo SiteAdministratorsCanDoEverything
- La política BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup para ejecutar mandatos en nombre del cliente

La política SiteAdministratorsCanDoEverything es una política por omisión especial que concede acceso de superusuario a los administradores que tienen el rol de administrador de sitio. En esta política, un administrador de sitio puede

realizar cualquier acción en cualquier recurso, incluso si estas acciones o recursos no se han definido. Es importante recordarlo cuando se asigna este rol a los usuarios.

La política BecomeUserCustomerServiceGroupExecutesBecomeUserCmdsResourceGroup es una política especial que permite que determinados usuarios administrativos ejecuten mandatos especificados en nombre de otros usuarios. Esta política es necesaria cuando, por ejemplo, un cliente solicita un representante del servicio al cliente para que cree un pedido en su nombre. En este caso, el representante de servicio puede ejecutar el mandato de modo que parece que el propio cliente ha ejecutado el mandato.

Roles

Como se ha mencionado anteriormente, WebSphere Commerce proporciona conjuntos de roles por omisión. El Administrador de sitio debe asignar roles específicos a cada organización antes de asignar usuarios a dichos roles. Una organización solamente puede tener los roles que se han asignado a su organización padre.

El ámbito de todos los roles de WebSphere es el de una organización. Por ejemplo, si un usuario tiene el rol de jefe de producto de la organización X. En este caso, la organización X debe dar soporte al el rol de jefe de producto. Por lo general, para poder asignar un rol a un usuario de una organización, dicha organización debe dar soporte a ese rol. A continuación, se pueden definir las políticas de control de acceso de modo que solamente este usuario pueda realizar las operaciones propias del jefe de producto dentro del contexto de la organización X y sus suborganizaciones.

Nota: Los roles se asignan a usuarios y organizaciones en la tabla `MBRROLE`.

Los roles por omisión que se incluyen en WebSphere Commerce se pueden agrupar en las categorías siguientes:

- Roles de operaciones técnicas
- Roles de marketing
- Roles operativos
- Roles de servicio al cliente
- Roles de relaciones de empresa
- Roles de gestión de productos y comercialización

En WebSphere Commerce 5.5, cada rol se asocia con uno o varios modelos de negocio. En cada modelo, un rol puede realizar un número de tareas seleccionadas utilizando Commerce Accelerator, la consola de administración y las herramientas de la Consola de administración de organizaciones. Para obtener más información sobre los modelos de negocio, consulte la publicación *WebSphere Commerce, Conceptos básicos*.

El diagrama siguiente muestra el acceso de cada rol a cada una de las herramientas. Antes de asignar roles a usuarios, asegúrese de que tiene la información correcta sobre las restricciones de acceso aplicables a dicho rol.

Roles correlacionados con las herramientas de WebSphere Commerce en cada tienda de ejemplo

Tabla 1. Roles correlacionados con las herramientas de WebSphere Commerce

Roles	Ejemplos	Herramientas
Representante de cuentas	• Directo a B2B: ToolTech	• Accelerator
Administrador de compradores	• Directo a B2B: ToolTech	• Consola de administración de organizaciones
Aprobador de compradores	• Directo a B2B: ToolTech	• Consola de administración de organizaciones
Comprador (parte vendedora)	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech	• Accelerator
Comprador (parte compradora)	• Directo a B2B: ToolTech • Alojamiento: Tienda alojada • Cadena de oferta: Tienda alojada de proveedor	Este rol está disponible en los ejemplos pero no tiene acceso a ninguna herramienta específica.
Gestor de categorías	• Directo al consumidor: FashionFlow • Directo a B2B: ToolTech • Cadena de demanda: Tienda alojada, tienda de elementos de catálogo • Alojamiento: Tienda alojada, tienda de elementos de catálogo • Cadena de oferta: Tienda de elementos de catálogo, tienda alojada de proveedor	• Accelerator
Gestor de canales	• Cadena de demanda: Centro de canal • Alojamiento: Centro de alojamiento • Cadena de oferta: Directorio de tiendas	• Accelerator • Consola de administración de organizaciones
Representante de servicio al cliente	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech	• Accelerator
Supervisor de servicio al cliente	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech	• Accelerator

Tabla 1. Roles correlacionados con las herramientas de WebSphere Commerce (continuación)

Roles	Ejemplos	Herramientas
Director de logística	• Directo a B2B: ToolTech • Cadena de oferta: Tienda alojada de proveedor	• Accelerator
Director de marketing	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech • Cadena de demanda: Centro de canal, tienda alojada, tienda de elementos de escaparate de revendedor • Alojamiento: Tienda alojada, tienda de elementos de escaparate alojada	• Accelerator
Director de operaciones	• Directo al consumidor: Fashion Flow • Cadena de demanda: Tienda alojada • Alojamiento: Tienda alojada	• Accelerator
Empaquetador	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech	• Accelerator
Responsable de compras	• Directo a B2B: ToolTech • Cadena de oferta: Tienda alojada de proveedor	Este rol está disponible en los ejemplos pero no tiene acceso a ninguna herramienta específica.
Administrador de responsables de compras	• Directo a B2B: ToolTech • Cadena de oferta: Tienda alojada de proveedor	Este rol está disponible en los ejemplos pero no tiene acceso a ninguna herramienta específica.
Jefe de producto	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech	• Accelerator
Receptor	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech	• Accelerator

Tabla 1. Roles correlacionados con las herramientas de WebSphere Commerce (continuación)

Roles	Ejemplos	Herramientas
Cliente registrado	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech • Cadena de demanda: Centro de canal, tienda alojada • Alojamiento: Centro de alojamiento, tienda alojada • Cadena de oferta: Directorio de tiendas, tienda alojada de proveedor	Este rol está disponible en los ejemplos pero no tiene acceso a ninguna herramienta específica.
Administrador de devoluciones	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech	• Accelerator
Director de ventas	• Directo a B2B: ToolTech • Cadena de oferta: Tienda alojada de proveedor	• Accelerator
Vendedor	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech • Cadena de demanda: Tienda alojada • Alojamiento: Tienda alojada • Cadena de oferta: Tienda alojada de proveedor	• Accelerator
Administrador de vendedores	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech • Cadena de demanda: Centro de canal, tienda alojada • Alojamiento: Centro de alojamiento, tienda alojada • Cadena de oferta: Directorio de tiendas, tienda alojada de proveedor	• Consola de administración de organizaciones

Tabla 1. Roles correlacionados con las herramientas de WebSphere Commerce (continuación)

Roles	Ejemplos	Herramientas
Administrador de sitio (Organización raíz)	• Directo al consumidor: Fashion Flow • Directo a B2B: ToolTech • Cadena de demanda: Centro de canal, tienda alojada, tienda de elementos de catálogo, tienda de elementos de escaparate de revendedor • Alojamiento: Centro de alojamiento, tienda alojada, tienda de elementos de catálogo, tienda de elementos de escaparate alojada • Cadena de oferta: Directorio de tiendas, tienda alojada de proveedor, tienda de elementos de catálogo, tienda de elementos de proveedor	• Accelerator • Consola de administración de organizaciones • Consola de administración

Notas:

1. El rol de administrador de sitio es el único rol con acceso a la consola de administración.
2. Para obtener más información sobre roles específicos y los menús de cada herramienta a la que tienen acceso, consulte el archivo ″Roles″ en la ayuda en línea de producción de WebSphere Commerce.
3. Para obtener más información acerca de cada tienda de ejemplo, consulte el apartado ″Tiendas″ de la Ayuda en línea a la producción y el desarrollo de WebSphere Commerce

Cómo impide el control de acceso las acciones no autorizadas

Este apartado describe cómo funciona el control de acceso basado en políticas para asegurarse de que los usuarios solamente puedan realizar las acciones para las que están autorizados.

Comprobación de las autorizaciones antes de realizar una acción iniciada por el usuario

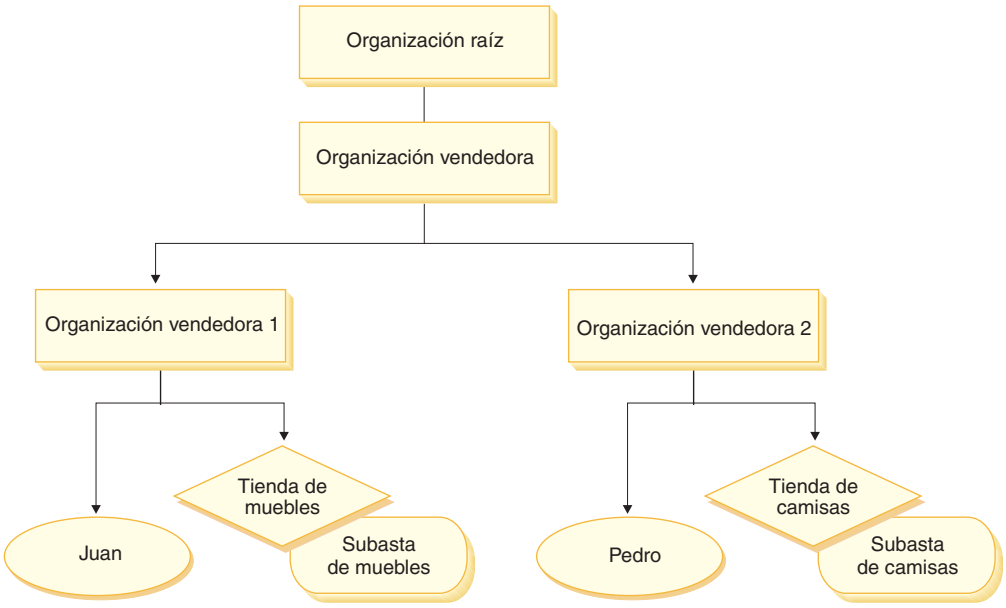
El *Gestor de políticas* es el componente de control de acceso que determina si el usuario actual puede ejecutar la acción especificada en el recurso especificado. Las políticas de control de acceso están especificadas en formato XML. Durante la creación de la instancia, se cargan automáticamente los grupos de políticas y las políticas por omisión en las tablas de base de datos correspondientes. Cuando se inicia WebSphere Commerce Application Server, la información de control de acceso se coloca en la antememoria para que el Gestor de políticas pueda comprobar rápidamente la autorización de un usuario cuando se le solicite. Si la información de control de acceso se modifica en la base de datos mediante la

Consola de administración de WebSphere Commerce o cargando los datos de políticas XML, la antememoria de control de acceso se deberá actualizar. Esto puede llevarse a cabo actualizando el registro de control de acceso en la Consola de administración de WebSphere Commerce. Si se cambian los datos de políticas, entonces debe actualizarse el registro de políticas de control de acceso. Si se cambian los datos del grupo de políticas, entonces debe actualizarse el registro de políticas de control de acceso. Si se reinicia WebSphere Commerce también se actualizará la antememoria.

Cuando un usuario intenta efectuar una acción en un recurso protegido, se llevará a cabo una comprobación de acceso para asegurarse de que el usuario tiene autorización. El Gestor de políticas gestiona las políticas de control de acceso que se aplican a la organización propietaria del recurso. A continuación, comprueba estas políticas y evalúa si el usuario tiene autorización para realizar la acción en el recurso de destino. Si encuentra como mínimo una de estas políticas, el Gestor de políticas otorga el acceso; de lo contrario, lo deniega.

Niveles de control de acceso

En WebSphere hay dos niveles generales para el control de acceso: a nivel de mandatos (conocido también como basado en roles) y a nivel de recursos (conocido también como a nivel de instancias).



Control de acceso a nivel de mandatos o basado en roles

El control de acceso a nivel de mandatos o basado en roles es un control de acceso menos filtrado. Determina "quién puede hacer qué". Con el control de acceso basado en roles, puede especificar que todos los usuarios de un rol determinado pueden ejecutar determinados mandatos. Se puede tomar como ejemplo la política de control de acceso: los vendedores pueden ejecutar mandatos de vendedores. En esta política, uno de los mandatos de vendedores es el mandato `ModifyAuction`. En la figura anterior, José y Pedro son vendedores, por lo tanto, ambos pueden modificar subastas.

El control de acceso basado en roles se utiliza para mandatos de controlador y vistas. Este tipo de control de acceso no tiene en cuenta el recurso en el que se ejecutará el mandato. Simplemente determina si al usuario se le permite ejecutar

una vista o mandato de controlador específico. Este nivel de control de acceso es obligatorio y entra en vigor durante la ejecución.

Control de acceso a nivel de mandatos para mandatos de controlador: Cuando ejecuta un mandato de controlador, debe existir una política de control de acceso que permita a los usuarios realizar la acción `Execute` en el recurso de mandato. El recurso es el nombre de la interfaz del mandato de controlador. El grupo de acceso suele estar dentro del ámbito de un solo rol. Por ejemplo, puede especificar que los usuarios que tengan el rol de Representante de cuentas puedan ejecutar cualquier mandato del grupo de recursos `AccountRepresentativesCmdResourceGroup`.

Control de acceso a nivel de mandatos para vistas: Cuando se llama directamente a una vista desde el URL, o si es el resultado de una redirección desde un mandato, debe tener una política de control de acceso. Dicha política debe tener especificado el nombre de vista (`viewname`) como una acción en la tabla `ACACTION`. Esta acción debe tener un grupo de acciones asociado mediante la tabla `ACACTACTGP`. A continuación, debe hacerse referencia a este grupo de acciones en la política a nivel de mandatos adecuada en la tabla `ACPOLICY`.

Control de acceso a nivel de instancias o a nivel de recursos

Las políticas de control de acceso a nivel de instancias o a nivel de recursos proporcionan un control de acceso general, ya que determinan `quién puede ejecutar qué mandato en qué recursos`. El ejemplo anterior de una política de control de acceso basada en roles que permite que los vendedores modifiquen las subastas, se puede ajustar de modo que el control de acceso a nivel de recursos sea: los vendedores pueden modificar las subastas que son propiedad de la organización para la que desempeñan su rol. En la página 37, José tiene el rol de vendedor para la organización vendedora 1. Pedro tiene el rol de vendedor para la organización vendedora 2. José crea una subasta de muebles en la tienda de muebles. Pedro crea una subasta de camisas en la tienda de camisas. José puede modificar la subasta de muebles, pero *no* la subasta de camisas. Pedro puede modificar la subasta de camisas pero *no* la subasta de muebles.

Resumiendo, el primer sistema realiza una comprobación de acceso a nivel de mandatos. Si el usuario puede ejecutar un mandato, se crea una política de control de acceso a nivel de recursos posterior para determinar si el usuario puede acceder al recurso en cuestión.

El control de acceso a nivel de recursos se aplica a mandatos y beans de datos.

Control de acceso a nivel de recursos para mandatos: Una vez completada la comprobación de control de acceso a nivel de mandatos, si se ha otorgado acceso, se lleva a cabo la comprobación a nivel de recursos en uno de los dos casos siguientes:

- El mandato implementa `getResources()` — este método especifica las instancias de los recursos que se deben comprobar en la acción actual, donde el mandato es la acción actual. Durante la ejecución de WebSphere Commerce se otorgará acceso al usuario a todos los recursos que especifique `getResources()`. Por omisión, `getResources()` devuelve valores nulos, es decir, no realiza una comprobación a nivel de recursos.
- El mandato llama a `checkIsAllowed(Object Resource, String Action)` — en los casos en los que el escritor del mandato desconoce los recursos que se deben comprobar en el momento en que la ejecución llama a getResources(), el mandato puede llamar al método `checkIsAllowed()`, según sea necesario, para determinar si la acción actual y el par de recursos están autorizados. La acción es generalmente el nombre de la interfaz del mandato actual. Cuando se llama a

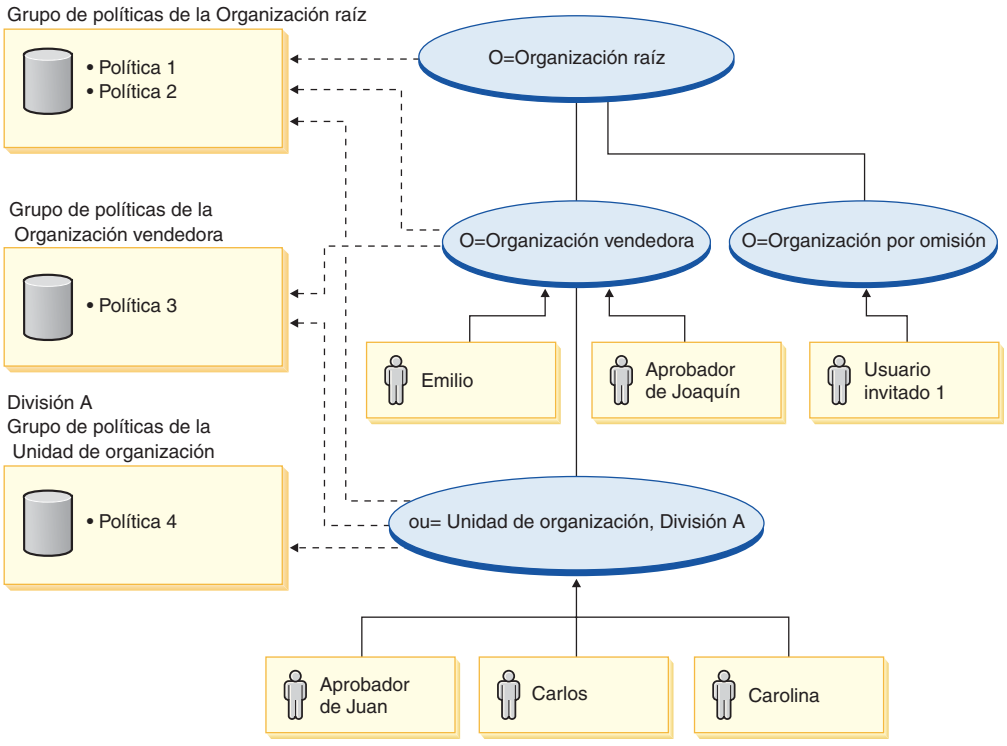
este método, si se deniega el acceso, se generará una excepción:
`ECApplicationException( ECMessage._ERR_USER_AUTHORITY, ..)`

Control de acceso a nivel de recursos para beans de datos: Como se ha descrito anteriormente, las vistas están protegidas por políticas a nivel de mandatos que, generalmente, están basadas en roles. Por ejemplo, la política a nivel de mandatos puede especificar que un administrador de vendedores tenga acceso a una vista específica. Normalmente, es necesario asegurarse adicionalmente de que todos los beans de datos de la JSP están relacionados con la organización para la que el usuario desempeña el rol de administrador de vendedores. Esto se lleva a cabo haciendo que todos los beans de datos que necesiten protección (ya sea directa o indirectamente) implementen la interfaz Delegator. Estos beans de datos delegan en un bean de datos primario (independiente) que, a su vez, implementa la interfaz Protectable. Un bean de datos primario se delegará en sí mismo y, por lo tanto, implementará ambas interfaces. A continuación, cuando se invoca el bean de datos mediante el método `activate()` del gestor de beans de datos, la ejecución de WebSphere Commerce se asegurará de que haya una política que otorgue al usuario actual la autorización para realizar la acción `Display` en el recurso de bean de datos primario.

Evaluación de las políticas de control de acceso

Este apartado se puede utilizar como guía para evaluar las políticas de control de acceso. En este apartado se incluye un escenario y se le guía por un ejemplo de cómo evaluar una política de control de acceso agrupable estándar y otra de plantilla. Cada apartado comienza por una descripción de políticas relacionadas y de escenarios en los que se utiliza cada una de estas políticas. Para obtener más información sobre las políticas estándar y de plantilla agrupables, consulte el apartado “Tipos de políticas de control de acceso” en la página 31.

El diagrama siguiente muestra gráficamente el escenario:



Jerarquía organizativa

En el diagrama puede ver las cuatro organizaciones siguientes que están en el sitio:

- Organización raíz
- Organización vendedora
- Organización por omisión
- Organización del departamento A

Las líneas continuas del diagrama indican la propiedad, las líneas discontinuas indican las suscripciones. Como puede ver, la organización raíz es la organización padre de la organización vendedora y de la organización por omisión. La organización vendedora es la organización padre de la organización del departamento A.

Usuarios

En el diagrama, Joaquín y Emilio están registrados en la organización vendedora. Juan, Carlos y Carolina están registrados en la organización del departamento A. El usuario invitado 1 no está registrado pero, para fines de control de acceso, pertenece de forma implícita a la organización por omisión.

Roles

Joaquín desempeña el rol de aprobador para la organización vendedora. Juan tiene asignado el rol de aprobador de la organización del departamento A.

Grupos de acceso

En este escenario se utilizan los siguientes grupos de acceso:

- Usuarios registrados: este grupo incluye implícitamente a todos los usuarios que están registrados al menos en una organización del sitio.
- Aprobadores para organización vendedora: este grupo incluye implícitamente a todos los usuarios que tienen el rol de aprobador de la organización vendedora.
- Aprobadores del departamento A: este grupo incluye implícitamente a todos los usuarios que tienen el rol de aprobador de la organización del departamento A.

Documentos

El objeto de documentos es un recurso protegido. El propietario de un documento está definido de modo que sea la organización en la que se ha creado.

Requisitos de control de acceso para actualizar documentos

A continuación se muestran los requisitos de control de acceso para actualizar documentos:

1. Los usuarios registrados pueden actualizar un documento de los que son el creador.
2. Los aprobadores del departamento A pueden actualizar documentos que son propiedad del departamento A pero no documentos que son propiedad de la organización vendedora. Los aprobadores de la organización vendedora pueden actualizar los documentos que son propiedad del departamento A y de la organización vendedora.

Evaluación de las políticas estándar agrupables

Este apartado es una guía para evaluar las políticas estándar agrupables y los escenarios.

Políticas de control de acceso relacionadas con la actualización de los documentos

A continuación se muestra el formato de política y las políticas de control de acceso que están relacionadas con la actualización de documentos:

Formato de política: `[Access Group, Action Group, Resource Group, Relationship]`

Política 1:

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

Se trata de una política basada en roles estándar y agrupable que forma parte del grupo de políticas de la organización raíz a la que se han suscrito la organización raíz, la organización vendedora y la organización del departamento A. En esta política, los usuarios registrados pueden ejecutar mandatos `Update Document`.

Política 2:

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

Se trata de una política a nivel de recursos estándar y agrupable que forma parte del grupo de políticas de la organización raíz a la que se han suscrito la organización raíz, la organización vendedora y la organización del departamento A. En esta política, los usuarios registrados pueden actualizar un documento si son los creadores de dicho documento.

Política 3:

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

Se trata de una política a nivel de recursos estándar y agrupable que forma parte del grupo de políticas de la organización vendedora a la que se han suscrito la organización vendedora y la unidad organizativa del departamento A. En esta política, los aprobadores de la organización vendedora pueden actualizar documentos que son propiedad de la organización vendedora.

Política 4:

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

Se trata de una política a nivel de recursos estándar y agrupable que forma parte del grupo de políticas de la organización del departamento A a la que se ha suscrito la organización del departamento A. En esta política, los aprobadores del departamento A pueden actualizar documentos que son propiedad del departamento A.

Escenarios

Escenario 1 : Carlos intenta actualizar su propio documento: A continuación se muestra la evaluación de control de acceso para este escenario:

Comprobación a nivel de mandato:

1. No se ha especificado ningún ID de tienda, por lo tanto, el propietario del mandato se establece en la organización raíz. Por lo tanto, solamente se utilizarán las políticas pertenecientes a la organización raíz para evaluar si el usuario tiene acceso a nivel de mandatos: las políticas 1 y 2 a las que se ha suscrito la organización raíz.
2. La política 1 otorga acceso ya que Carlos es miembro del grupo de acceso de usuarios registrados y está realizando la acción `Execute` en el recurso de mandato `Update Document`.

Comprobación a nivel de recursos:

1. El mandato `Update Document` especifica que el recurso de documento se ha de proteger. El documento de Carlos es propiedad del departamento A. Dado que el departamento A se suscribe a los grupos de políticas, solamente se aplicarán las políticas pertenecientes a estos grupos de políticas: las políticas 1, 2, 3 y 4.
2. La política 2 otorga acceso ya que Carlos es miembro del grupo de acceso de usuarios registrados y está realizando la acción de mandato `Execute` en el recurso de documento y satisface la relación de creador con el documento.

Dado que Carlos ha pasado las dos comprobaciones de control de acceso, a nivel de mandatos y a nivel de recursos, puede actualizar su propio documento.

Escenario 2: Joaquín intenta actualizar el documento de Carolina: A continuación se muestra la evaluación de control de acceso para este escenario:

Comprobación a nivel de mandato:

1. No se ha especificado ningún ID de tienda, por lo tanto, el propietario del mandato se establece en la organización raíz. Por lo tanto, solamente se utilizarán las políticas pertenecientes a la organización raíz para evaluar si el usuario tiene acceso a nivel de mandatos: las políticas 1 y 2 son propiedad de la organización raíz.
2. La política 1 otorga acceso ya que Joaquín es miembro del grupo de acceso de usuarios registrados y está realizando la acción `Execute` en el recurso de mandato `Update Document`.

Comprobación a nivel de recursos:

1. El mandato `Update Document` especifica que el recurso de documento se ha de proteger. El documento de Carolina es propiedad del departamento A. Dado que el departamento A se suscribe a los grupos de políticas, solamente se aplicarán las políticas pertenecientes a estos grupos de políticas: las políticas 1, 2, 3 y 4.
2. La política 3 otorga acceso ya que Joaquín es miembro del grupo de acceso de `Aprobadores de organización vendedora` y está realizando la acción `Update Document` en el recurso de documento.

Dado que Joaquín ha pasado las dos comprobaciones de control de acceso, a nivel de mandatos y a nivel de recursos, puede actualizar el documento de Carolina.

Escenario 3: Juan intenta actualizar el documento de Emilio: A continuación se muestra la evaluación de control de acceso para este escenario:

Comprobación a nivel de mandato:

1. No se ha especificado ningún ID de tienda, por lo tanto, el propietario del mandato se establece en la organización raíz. Por lo tanto, solamente se utilizarán las políticas pertenecientes a la organización raíz para evaluar si el usuario tiene acceso a nivel de mandatos: las políticas 1 y 2 son propiedad de la organización raíz.
2. La política 1 otorga acceso ya que Juan es miembro del grupo de acceso de usuarios registrados y está realizando la acción `Execute` en el recurso de mandato `Update Document`.

Comprobación a nivel de recursos:

1. El mandato `Update Document` especifica que el recurso de documento se ha de proteger. El documento de Emilio es propiedad de la organización vendedora.

Dado que la organización vendedora se suscribe a los grupos de políticas, se aplicarán todas las políticas pertenecientes a estos grupos de políticas: las políticas 1, 2 y 3.

2. La política 3 NO otorga acceso ya que Juan NO es miembro del grupo de acceso Aprobadores de la organización vendedora.

Aunque Juan ha pasado la comprobación a nivel de mandato, como no ha pasado la comprobación de control de acceso a nivel de recursos, no puede actualizar el documento de Emilio.

Escenario 4: el usuario invitado 2 intenta actualizar su propio documento: A continuación se muestra la evaluación de control de acceso para este escenario:

Comprobación a nivel de mandato:

1. No se ha especificado ningún ID de tienda, por lo tanto, el propietario del mandato se establece en la organización raíz. Por lo tanto, solamente se utilizarán las políticas pertenecientes a los grupos de políticas a los que se ha suscrito la organización raíz para evaluar si el usuario tiene acceso a nivel de mandatos: las políticas 1 y 2 son propiedad de la organización raíz.
2. La política 1 NO otorga acceso ya que el usuario invitado 1 NO es miembro del grupo de acceso `Usuarios registrados`.

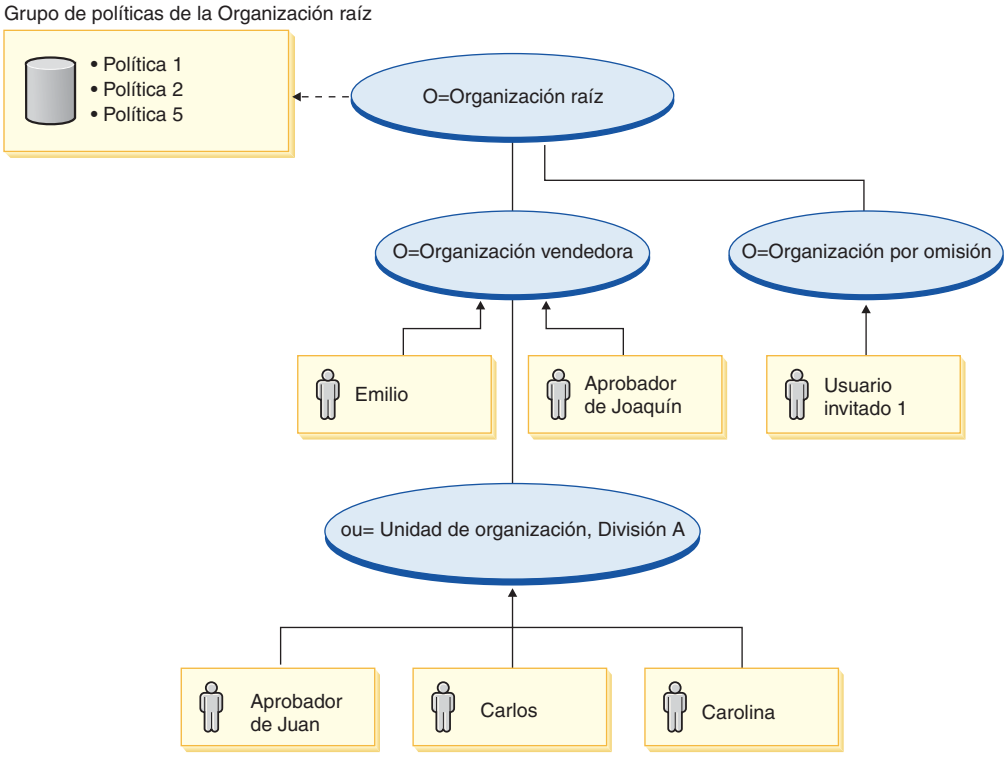
Comprobación a nivel de recursos:

1. La comprobación a nivel de recursos no se lleva a cabo ya que la comprobación a nivel de mandato no ha sido satisfactoria.

Dado que el usuario invitado 1 no ha pasado la comprobación a nivel de mandato, no puede actualizar su propio documento.

Evaluación de las políticas de plantilla agrupables

Esta sección se basa en la configuración que se muestra en el siguiente diagrama.



Políticas de control de acceso relacionadas con la actualización de documentos

En esta configuración, se continúan aplicando las políticas de control de acceso 1 y 2, no obstante, las políticas estándar agrupables 3 y 4 se sustituyen ahora por la política de plantilla 5. Para obtener más información sobre las políticas 1 y 2, consulte el apartado “Evaluación de las políticas estándar agrupables” en la página 40.

Política 5:

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

Esta política es una política de plantilla agrupable a nivel de recursos. Forma parte del grupo de políticas de la organización raíz a la que se ha suscrito la organización raíz. Las políticas de plantilla agrupables se aplican dinámicamente a la organización propietaria del recurso durante la ejecución. Estas políticas generalmente utilizan grupos de acceso definidos con parámetros. En este caso, se utiliza el siguiente grupo de acceso definido con parámetros:

- Aprobadores para organización: este grupo incluye implícitamente a todos los usuarios que tienen el rol de aprobador de la organización propietaria del recurso de documento o de las organizaciones predecesoras.

Escenarios

Los siguientes escenarios están basados en la configuración que se muestra en el diagrama anterior que solamente tiene un grupo de políticas. El grupo de políticas de la organización raíz incluye las políticas 1,2 y 5.

Escenario 1: Joaquín intenta actualizar el documento de Carolina: A continuación se muestra la evaluación de control de acceso para este escenario:

Comprobación a nivel de mandato:

1. No se ha especificado ningún ID de tienda, por lo tanto, el propietario del mandato se establece en la organización raíz. Por lo tanto, solamente se utilizarán las políticas pertenecientes a la organización raíz para evaluar si el usuario tiene acceso a nivel de mandatos: las políticas 1, 2 y 5.
2. La política 1 otorga acceso ya que Joaquín es miembro del grupo de acceso de usuarios registrados y está realizando la acción `Execute` en el recurso de mandato `Update Document`.

Comprobación a nivel de recursos:

1. El mandato `Update Document` especifica que el recurso de documento se ha de proteger. El documento de Carolina es propiedad del departamento A. El departamento A no se suscribe a ningún grupo de políticas, por lo tanto, la infraestructura de control de acceso comienza a buscar en sentido ascendente en la jerarquía organizativa hasta que encuentra una organización que se suscriba como mínimo a un grupo de políticas. Asimismo, la organización vendedora, que es la organización padre inmediata del departamento A, no se suscribe a grupos de políticas. Continuando en sentido ascendente por la jerarquía organizativa, se llega a la organización raíz. Esta organización se suscribe a un grupo de políticas. De este modo, se pueden aplicar sus políticas: las políticas 1, 2 y 5.
2. La política de plantilla 5 se aplica a la organización que es la propietaria del recurso: el departamento A. El grupo de acceso definido con parámetros, Aprobadores de la organización, abarca de forma dinámica el ámbito del contexto de recurso actual, de modo que comprobará si el usuario cumple con la condición del grupo de acceso para la organización propietaria del recurso o sus predecesores. En este caso, Joaquín es aprobador de la organización

vendedora (predecesora del departamento A), por lo tanto, cumple con la condición del grupo de acceso. Dado que ejecuta la acción del mandato Update Document en el recurso de documento, también se cumplen los demás elementos de la política 5 y, de este modo, la comprobación de política a nivel de recurso se pasa satisfactoriamente.

Dado que Joaquín ha pasado las dos comprobaciones de control de acceso, a nivel de mandatos y a nivel de recursos, puede actualizar el documento de Carolina.

Escenario 2: Juan intenta actualizar el documento de Emilio: A continuación se muestra la evaluación de control de acceso para este escenario:

Comprobación a nivel de mandato:

1. No se ha especificado ningún ID de tienda, por lo tanto, el propietario del mandato se establece en la organización raíz. Por lo tanto, solamente se utilizarán las políticas pertenecientes a la organización raíz para evaluar si el usuario tiene acceso a nivel de mandatos: las políticas 1, 2 y 5.
2. La política 1 otorga acceso ya que Juan es miembro del grupo de acceso de usuarios registrados y está realizando la acción `Execute` en el recurso de mandato `Update Document`.

Comprobación a nivel de recursos:

1. El mandato `Update Document` especifica que el recurso de documento se ha de proteger. El documento de Emilio es propiedad de la organización vendedora. La organización vendedora no se suscribe a ningún grupo de políticas, por lo tanto, la infraestructura de control de acceso comienza a buscar en sentido ascendente en la jerarquía organizativa hasta que encuentra una organización que se suscriba como mínimo a un grupo de políticas. Continuando en sentido ascendente por la jerarquía organizativa, se llega a la organización raíz. Esta organización se suscribe a un grupo de políticas. De este modo, se pueden aplicar sus políticas: las políticas 1, 2 y 5.
2. La política de plantilla 5 se aplica a la organización que es la propietaria del recurso: la organización vendedora. El grupo de acceso definido con parámetros, Aprobadores de la organización, abarca de forma dinámica el ámbito del contexto de recurso actual, de modo que comprobará si el usuario cumple con la condición del grupo de acceso para la organización propietaria del recurso o sus predecesores. En este caso, Juan es aprobador de la organización del departamento A (descendiente de la organización vendedora), por lo tanto, no cumple con la condición del grupo de acceso.

Aunque Juan ha pasado la comprobación a nivel de mandato, como no ha pasado la comprobación de control de acceso a nivel de recursos, no puede actualizar el documento de Emilio.

Análisis detallado de una política

Ahora que ya se ha descrito la estructura básica de una política de control de acceso y los tipos de política existentes, analizaremos detenidamente una de las políticas por omisión, utilizando una serie de ejemplos diferentes. La política que analizaremos es la siguiente:

```
AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
```

Nota: Esta política es una política a nivel de recursos. Su tipo de política es de plantilla agrupable.

En el primer ejemplo, describiremos cómo se puede leer la política utilizando la Consola de administración de organizaciones de WebSphere Commerce, identificar sus partes y comprender lo que significa la política. En el segundo ejemplo analizaremos la política en formato XML, para que resulte más fácil comprender qué aspecto tiene la misma información en el código.

En el tercer ejemplo avanzaremos un paso más en la descripción de cómo una política está relacionada con otras políticas. Comprender las dependencias entre políticas es un prerrequisito importante para realizar cambios en las políticas de control de acceso o para crear políticas nuevas.

Ejemplo 1: lectura de una política

En este ejemplo, utilizaremos la Consola de administración de organizaciones de WebSphere Commerce para buscar una política e identificar las partes que la definen. También utilizaremos estos componentes para describir de forma general la política.

Búsqueda de la política en la Consola de administración de organizaciones

1. Inicie la sesión en la Consola de administración de organizaciones de WebSphere Commerce. En el menú Gestión de acceso, seleccione **Políticas**.
2. Seleccione la organización raíz del recuadro de lista, ya que la organización raíz es la propietaria de la mayor parte de las políticas de control de acceso por omisión.
3. En la página de políticas, desplácese por la lista de políticas y localice la política siguiente:
   `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`

   Observe que puede desplazarse por la lista de políticas mediante la barra de desplazamiento y también mediante los enlaces **Primera**, **Anterior**, **Siguiente** y **Última**.

Visualización de los componentes de la política

1. Seleccione la política pulsando el recuadro que hay junto a la misma y pulse **Mostrar grupo de acciones**.
2. En la página Grupos de acciones, verá el grupo de acciones AuctionManage. Este es el grupo de acciones asociado a la política. Seleccione `AuctionManage` y pulse **Mostrar acciones**.
3. En la página siguiente, verá la lista de mandatos o acciones siguientes, incluidos en el grupo de acciones `AuctionManage`:
   - `com.ibm.commerce.negotiation.commands.CloseBiddingCmd`
   - `com.ibm.commerce.negotiation.commands.DeleteAuctionCmd`
   - `com.ibm.commerce.negotiation.commands.ModifyAuctionCmd`

   Aquí, `AuctionManage` incluye cerrar una subasta (`CloseBiddingCmd`), suprimir una subasta, (`DeleteAuctionCmd`) y modificar una subasta (`ModifyAuctionCmd`). Para obtener más información sobre los mandatos, consulte la sección Referencias de la ayuda en línea.

   Observe que también puede acceder a la lista de acciones desde la página Políticas o pulsando **Mostrar acciones**.
4. Para regresar a la página de políticas, seleccione una de las acciones y pulse **Mostrar políticas**.

5. Vuelva a seleccionar la política pero ahora pulse **Mostrar grupo de miembros** para ver el grupo de miembros (el grupo de acceso) que se utiliza en esta política.
6. Anote el nombre del grupo de miembros (de acceso). En este caso, el grupo de miembros (de acceso) es `AuctionAdministratorsForOrg`.
7. En el menú Gestión de acceso, seleccione **Grupos de acceso**.
8. Busque `AuctionAdministratorsForOrg`. Selecciónelo y pulse **Cambiar.**
9. Pulse **Criterios**. En la página Criterios, busque en Roles y organizaciones seleccionados. Deberá ver los roles siguientes:
   - `Vendedor - para organización`
   - `Gestor de productos - para organización`
   - `Comprador (parte vendedora) - para organización`
   - `Gestor de categorías - para organización`

   Cualquier usuario que tenga asignados estos roles para la organización propietaria del recurso de subasta, formará parte del grupo de acceso `AuctionAdministratorsForOrg`.
10. No modifique la página Criterios. En el menú Gestión de acceso, seleccione otra vez **Políticas**. Localice la política siguiente:

    `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`
11. Seleccione la política y pulse **Mostrar recursos**. En la página recursos, verá el recurso `com.ibm.commerce.negotiation.objects.Auction`. Este es el recurso en el que se llevan a cabo las acciones que se listan en el grupo de acciones. En este caso, el recurso es una subasta. Tenga en cuenta que puede acceder a esta misma lista desde la página Políticas si pulsa **Mostrar grupo de recursos** y se desplaza hasta los recursos individuales.
12. Ahora seleccione **Políticas** en el menú Gestión de acceso y localice la política siguiente:

    `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`
13. Seleccione la política y pulse **Cambiar**. En la página Cambiar política, observe el menú desplegable bajo **Relación**. Verá que la relación se ha establecido en ninguna. Esto significa que la política no tiene ninguna relación.
14. Pulse **Cancelar** y **Aceptar** para cerrar el recuadro de diálogo.

Descripción del significado de una política

Ahora que se han identificado los componentes individuales de esta política, es posible unirlos para así comprender lo que hace esta política. En primer lugar, sabemos que la política se aplica a todos los usuarios que pertenecen al grupo `AuctionAdministratorsForOrg`. Esto lo hemos aprendido al pulsar **Mostrar grupo de miembros**. A partir de ahí, hemos utilizado el menú Gestión de acceso para ir a la página Grupo de acceso y hemos visto que el grupo de acceso tenía los roles siguientes: `vendedor, jefe de producto, comprador (parte vendedora)` y `gestor de categorías`. De forma colectiva, se puede hacer referencia a los usuarios que tienen uno de estos cuatro roles como administrador de subastas.

También sabemos que el grupo de acciones contiene los mandatos para modificar, retractar y cerrar una subasta, y que el grupo de recursos incluye solamente el recurso de subasta que se va a gestionar. Además, esto lo sabemos si pulsamos **Mostrar acciones** y **Mostrar recursos** en la página Políticas y nos desplazamos hasta el nivel de información detallada. Por último, podemos decir que la política no incluye una relación entre el grupo de acceso y los recursos.

Y si lo unimos todo, podemos llegar a la conclusión de que esta política permite a los administradores de subastas realizar todas las actividades asociadas con la gestión de subastas en un recurso de subasta como, por ejemplo, modificar, retractar y cerrar una subasta, siempre que el administrador desempeñe el rol para la organización propietaria de la subasta.

Se puede comprender mejor el significado de una política mediante su nombre. En este ejemplo, la política comienza por el nombre del grupo de usuarios designado, `AuctionAdministratorForOrg`. La anotación `ForOrg`, indica que se trata de una política de plantilla agrupable. `AuctionManageCommands` describe el grupo de acciones y `AuctionResource` describe el grupo de recursos.

Ejemplo 2: lectura de una política en XML

Las políticas de control de acceso se almacenan en un archivo XML que se carga en la base de datos durante la creación de la instancia. Cuando visualiza una política en la consola de administración de WebSphere Commerce, está utilizando la interfaz para ver y modificar la información almacenada en la base de datos. La información de la base de datos la utiliza el Gestor de políticas para evaluar el control de acceso. Si la información de base de datos es más reciente que el archivo XML, puede utilizar la herramienta Extractor para extraer la información de política de control de acceso desde la base de datos a un archivo XML.

En el archivo XML una política es similar a la siguiente:

```
<!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
-->
<Policy
 Name="AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="groupable Template">
</Policy>
```

Aquí, la política se define de este modo:

`Name`: el nombre de la política.

`OwnerID`: la organización a la que se aplica la política.

`UserGroup`: el grupo de acceso.

`ActionGroupName`: el grupo de acciones.

`ResourceGroupName`: el grupo de recursos.

`PolicyType`: el tipo de política, por ejemplo, estándar o de plantilla agrupable.

El archivo que contiene todas las políticas de control de acceso por omisión se denomina `defaultAccessControlPolicies.xml` y está ubicado en el directorio siguiente:

`X:\`*`dir_inst`*`\xml\policies\xml`.

Nota: Las descripciones de cada archivo de control de acceso por omisión están contenidas en el archivo `defaultAccessControlPolicies_entorno_nacional.xml`, que se encuentra en el mismo directorio. Si realiza un cambio en una política de control de acceso por omisión en el archivo de control de acceso por omisión, deberá actualizar también su descripción correspondiente en `defaultAccessControlPolicies_es_ES.xml`. Le aconsejamos que los cambios en los archivos XML los realicen únicamente los usuarios avanzados.

Ejemplo 3: identificación de otras políticas asociadas a su política

En este último ejemplo, estudiaremos cómo una política de control de acceso puede tener dependencias con otras políticas.

Las políticas que definen los mandatos (acciones) que puede realizar un grupo de usuarios (un grupo de acceso) en un recurso se denominan políticas a nivel de recursos. Por ejemplo, la política que hemos estado analizando detalladamente:

`AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource` es un ejemplo de una política a nivel de recursos.

Sin embargo, las acciones que permite una política a nivel de recursos también dependen de las acciones que se permiten a cada rol que pertenece al grupo de acceso de la política. Las políticas que describen las acciones permitidas para un rol determinado se denominan políticas basadas en roles.

Para identificar las políticas asociadas a una política a nivel de recursos, ha de efectuar lo siguiente:

Buscar roles asociados a la política

1. Inicie la sesión en la Consola de administración de WebSphere Commerce y localice la política a nivel de recursos en la página Políticas. Utilizando el mismo ejemplo, sabemos que la política que buscamos es:
   `AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource`
2. Identifique el grupo de acceso asociado a la política. En este caso, ya sabemos que el grupo de acceso es `AuctionAdministratorsForOrg`.
3. Busque los roles asociados al grupo de acceso. A partir de los ejemplos anteriores, sabemos que los roles para `AuctionAdministratorsForOrg` son: `Compradores (parte vendedora)`, `Gestores de categorías`, `Gestor de productos` y `Vendedores`.

Buscar políticas basadas en roles para cada rol

1. Vaya al Apéndice A al final de este documento y busque el apartado con el encabezado: Políticas basadas en roles. Utilizaremos el Apéndice para localizar cada política basada en roles que esté asociada a un rol.
2. Busque la política `Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup`. Esta política está asociada con el rol `Compradores (parte vendedora)`. Esto lo sabemos por el prefijo `Buyers(sell-side)` (Compradores (parte vendedora)) de la política.
3. Busque el resto de las políticas basadas en roles asociadas a los roles `Compradores (parte vendedora)`, `Gestor de categorías`, `Gestor de productos` y `Vendedores`, utilizando los prefijos para identificar las políticas correctas. Deberá obtener la lista siguiente:
   - `Buyers(sell-side)ExecuteBuyers(sell-side)CommandsResourceGroup`

- Buyers(sell-side)ExecuteBuyers(sell-side)Views
- CategoryManagersExecuteCategoryManagersCmdResourceGroup
- CategoryManagersExecuteCategoryManagersViews
- ProductManagersExecuteProductManagersCmdResourceGroup
- ProductManagersExecuteProductManagersViews
- SellersExecuteSellersCmdResourceGroup
- SellersExecuteSellersViews

4. Toda política basada en roles permite a los usuarios que tengan dicho rol ejecutar una vista o un mandato de controlador determinado. Para ver qué acciones y recursos están asociados a una política basada en roles, busque la política en la página Políticas de la Consola de administración de WebSphere Commerce, utilizando el mismo procedimiento del Ejemplo 1.

Por qué es importante identificar las dependencias entre las políticas

Comprender qué políticas basadas en roles están asociadas a una política a nivel de recursos suele ser un requisito previo para personalizar las políticas y crear nuevas políticas.

En la Parte 3, “Administración de la autorización de seguridad”, en la página 95, se le proporcionará más información sobre las políticas a nivel de recursos y las políticas basadas en roles, incluido cómo puede reconocerlas, la descripción de sus diferencias y cómo se relacionan entre sí.

Parte 2. Administración de la autenticación de seguridad

Esta parte describe las tareas de autenticación de seguridad que normalmente realiza el administrador de sitio de WebSphere Commerce.

Capítulo 4. Mejora de la seguridad del sitio

Para mejorar la seguridad del sitio de WebSphere Commerce, puede habilitar cualquiera de las características siguientes en el Gestor de configuración de WebSphere Commerce:

- Desconectar un usuario que está inactivo durante un extenso periodo de tiempo y solicitar que vuelva a conectarse al sistema, utilizando el nodo de tiempo de espera de conexión. Para obtener detalles, consulte el apartado "Habilitación del tiempo de espera de conexión" en la página 57.
- Exigir a los usuarios que cambien sus contraseñas cuando se están conectando al sistema por primera vez, utilizando el nodo de Invalidación de contraseña. Para obtener detalles, consulte el apartado "Activación de la invalidación de contraseña" en la página 58.
- Exigir a los usuarios que entren sus contraseñas si están ejecutando peticiones que ejecutan mandatos designados, utilizando el nodo de Mandatos protegidos por contraseña. Para obtener detalles, consulte el apartado "Habilitación de mandatos protegidos por contraseña" en la página 58.
- Actualizar datos cifrados tales como contraseñas e información de tarjeta de crédito, así como la clave de comerciante en una base de datos de WebSphere Commerce, utilizando el nodo de Herramienta de actualización de base de datos. Para obtener detalles, consulte el apartado "Actualización de datos cifrados" en la página 59.
- Rechazar cualquier petición de usuario que contenga atributos o caracteres que están designados como no permitidos, utilizando el nodo de protección contra la vulnerabilidad Cross Site Scripting. Para obtener detalles, consulte el apartado "Habilitación de la protección contra la vulnerabilidad Cross Site Scripting" en la página 60.
- Identificar de forma rápida cualquier amenaza para la seguridad de WebSphere Commerce habilitando el registro de accesos. Para obtener detalles, consulte el apartado "Habilitación del registro de accesos" en la página 63.

Además, puede habilitar las características siguientes desde el menú desplegable Seguridad de la Consola de administración de WebSphere Commerce:

- Configurar una política de cuentas para el sitio a fin de definir las políticas relacionadas con las cuentas que se están usando, utilizando la página Política de cuentas. Para obtener detalles, consulte el apartado "Configuración de la política de cuentas" en la página 64.
- Configurar una política de contraseñas para el sitio a fin de controlar las características de selección de contraseña del usuario utilizando la página Política de contraseñas (sólo si los usuarios están autenticados en la base de datos de WebSphere Commerce). Para obtener detalles, consulte el apartado "Configuración de una política de contraseñas" en la página 65.
- Configurar una política de bloqueo de cuentas para el sitio a fin de reducir las posibilidades de que se ponga en peligro una cuenta de usuario, utilizando la página Política de bloqueo de cuentas (sólo si los usuarios están autenticados en la base de datos de WebSphere Commerce). Para obtener detalles, consulte el apartado "Configuración de una política de bloqueo de cuentas" en la página 66.
- Iniciar un programa de seguridad que comprueba y suprime archivos de WebSphere Commerce temporales que pueden contener riesgos potenciales para

la seguridad utilizando la página Iniciar comprobación de seguridad . Para obtener detalles, consulte el apartado “Inicio de una comprobación de seguridad” en la página 67.

Para obtener información sobre los conceptos relacionados, consulte los temas siguientes en la ayuda en línea de WebSphere Commerce:

- Gestor de configuración
- Archivo de configuración de WebSphere Commerce
- Consola de administración
- Seguridad

Para obtener información sobre las tareas relacionadas, consulte los temas siguientes en la ayuda en línea de WebSphere Commerce.

- Iniciar el Gestor de configuración
- Abrir la Consola de administración

Consideración de seguridad para el servidor Web IIS (Internet Information Services)

Atención

Si está utilizando el servidor Web IIS con WebSphere Commerce, debe tener en cuenta la siguiente consideración de seguridad y llevar a cabo la acción recomendada para que los datos de WebSphere Commerce corran el mínimo riesgo posible.

Problema: En el servidor Web IIS, el permiso de lectura en un directorio virtual proporciona acceso al código fuente de los archivos JSP. Si utiliza el servidor Web IIS, para impedir que se descargue el código fuente JSP, debe separar físicamente el contenido estático del contenido dinámico de las páginas Web. Esto es debido a que la seguridad de IIS está basada en la ubicación del directorio y no en el tipo de archivo. En la configuración por omisión de IIS, los archivos de imágenes y los archivos JSP se colocan bajo un único alias. Debe utilizar la configuración por omisión únicamente para fines de comprobación.

Solución: Para proteger todos los elementos Web, *se debe acceder al contenido dinámico mediante un directorio virtual con permiso sólo de ejecución (no de lectura) mientras el contenido estático debe trasladarse a un directorio virtual diferente con permiso sólo de lectura*. Para obtener más información sobre cómo establecer los permisos en un directorio virtual, consulte las instrucciones en la información de ayuda de IIS. También se le recomienda que consulte la documentación actual de Microsoft Corporation para obtener información acerca de los parches de seguridad y las políticas de configuración.

Vistas para la seguridad

Antes de utilizar determinadas características de seguridad de WebSphere Commerce, es necesario que defina las vistas asociadas para la tienda para poder utilizar dichas características. La información siguiente describe cómo definir las vistas para:

- Tiempo de espera de conexión (consulte el apartado “Tiempo de espera de conexión” en la página 55)

- Invalidación de contraseña (consulte el apartado "Invalidación de contraseña")
- Mandatos protegidos por contraseña (consulte el apartado "Mandatos protegidos por contraseña" en la página 56)
- Protección contra la vulnerabilidad Cross Site Scripting (consulte el apartado "Protección contra la vulnerabilidad Cross Site Scripting" en la página 57)

Para obtener información general sobre cómo crear vistas y desarrollar el escaparate de la tienda, consulte la publicación *WebSphere Commerce, Guía del desarrollador de tiendas*.

Tiempo de espera de conexión

Para utilizar la característica de seguridad Tiempo de espera de conexión, necesita definir las vistas LoginTimeoutErrorView y ReLogonFormView para la tienda.

LoginTimeoutErrorView

Si la información de tiempo de espera de conexión es incorrecta, WebSphere Commerce redirige el navegador del usuario a esta vista. Si ocurre esto, probablemente se debe a que alguien ha intentado manipular indebidamente el cookie.

Tabla 2. Atributos de LoginTimeoutErrorView

ECConstants.EC_LOGIN_TIMEOUT_ERROR_MSGCODE	
	1 Se ha establecido el tiempo de caducidad en un valor no válido.
	2 Se ha establecido el tiempo de conexión en un valor no válido.
	3 Se ha establecido el tiempo de conexión o el tiempo de caducidad en un valor no válido.

ReLogonFormView

Esta vista se muestra a los usuarios después de que haya caducado su sesión. Necesita proporcionar al usuario un formulario para que entre el ID de conexión y la contraseña del usuario. El botón Someter invocará el mandato de conexión. También tiene que haber un botón Cancelar para redirigir al usuario a otra página, en la mayoría de los casos, la página de escaparate de la tienda.

No hay atributos para ReLogonFormView.

Tabla 3. Atributos del formulario de ReLogonFormView

ECUserConstants.EC_UREG_LOGONID	ID de conexión del usuario.
ECUserConstants.EC_UREG_LOGONPASSWORD	Contraseña de conexión del usuario.
ECUserConstants.EC_RELOGIN_URL	URL que se visualiza si las credenciales proporcionadas no son válidas. En la mayoría de los casos, será el nombre de esta vista.
ECConstants.EC_STORE_ID	Identificador de tienda.
ECConstants.EC_URL	URL que se visualiza cuando las credenciales que se entran pertenecen a un usuario diferente. En la mayoría de los casos, será una página de presentación de tienda o el mismo URL que se utiliza en la página de conexión de tienda.

Invalidación de contraseña

Para utilizar la característica de seguridad Invalidación de contraseña, necesita definir la vista ChangePassword para la tienda.

ChangePassword

Esta vista se visualiza si ha caducado la contraseña de un usuario. Debe proporcionar al usuario un formulario para entrar la contraseña actual (caducada)

y una contraseña nueva. El botón Someter invoca el mandato ResetPassword. También tiene que haber un botón Cancelar que redirija al usuario a otra página, en la mayoría de los casos, la página de escaparate de la tienda.

Tabla 4. Atributos de ChangePassword

ECConstants.EC_PASSWORD_EXPIRED_FLAG		
	1	La contraseña del usuario ha caducado. Este atributo es necesario para distinguir esta vista de la vista utilizada para la característica de cambio de contraseña dado que son iguales. La vista para el cambio de contraseña puede invocarla un usuario y la JSP asignada a esta vista debe ser la misma para ambos casos. La JSP deberá buscar este atributo para decidir cuál debe visualizar.
	null	El atributo no está en un URL. Se trata del comportamiento normal de cambio de contraseña
ECUserConstants.EC_UREG_LOGONID		ID de conexión de usuario actual.
ECConstants.EC_LOGIN_RETURN_URL		URL al que se redirige el navegador después de un cambio de contraseña satisfactorio. Este URL se pasará a un mandato de acción bajo el nombre ECConstants.EC_URL.

Tabla 5. Atributos del formulario de ChangePassword

ECUserConstants.EC_UREG_LOGONID	ID de conexión del usuario. El ID de conexión actual se ha pasado a la vista.
ECUserConstants.EC_UREG_LOGONPASSWORDOLD	Contraseña antigua.
ECUserConstants.EC_UREG_LOGONPASSWORD	Contraseña nueva.
ECUserConstants.EC_UREG_LOGONPASSWORDVERIFY	Verificación de contraseña nueva.
ECConstants.EC_URL	URL al que se redirigen los usuarios después de un cambio de contraseña satisfactorio. El valor se ha pasado a la vista.
ECUserConstants.EC_RELOGIN_URL	URL al que se redirige el navegador si el cambio de contraseña no es satisfactorio.

Mandatos protegidos por contraseña

Para utilizar la característica de seguridad Mandatos protegidos por contraseña, necesita definir las vistas PasswordReEnterErrorView y PasswordReEnterFormView para la tienda.

PasswordReEnterErrorView

Esta vista se utiliza en los escenarios siguientes:

- Un usuario no puede proporcionar la contraseña correcta y se le desconecta.
- La autenticación ha fallado.

En ambos casos, el usuario debe tener un modo de continuar a otra página mediante un enlace en la página actual.

Tabla 6. Atributos de PasswordReEnterErrorView

ECConstants.EC_PASSWORD_REREQUEST_MSGCODE		
	0	Se ha producido un problema al intentar autenticar al usuario.
	null	El atributo no está en un URL. Se desconecta al usuario que no ha podido proporcionar la contraseña.

PasswordReEnterFormView

Esta vista se visualiza cuando el usuario intenta ejecutar un mandato protegido por contraseña. Debe proporcionar al usuario un formulario para entrar la contraseña. Tiene que haber dos campos de entrada para la contraseña.

Tabla 7. Atributos de PasswordReEnterFormView

ECConstants.EC_PASSWORD_REREQUEST_URL	El URL se ejecuta utilizando el botón Someter del formulario.

Tabla 7. Atributos de PasswordReEnterFormView (continuación)

ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	Código de mensaje que especifica el mensaje que se muestra al usuario: **1** Las contraseñas que se han entrado no coinciden. **2** No se ha entrado ninguna contraseña. **3** Se ha entrado una contraseña incorrecta.

ACCIÓN: El URL se pasa como un parámetro denominado:

Tabla 8. Atributos del formulario de PasswordReEnterFormView

ECConstants.EC_PASSWORD_REREQUEST_PASSWORD1	Primera contraseña.
ECConstants.EC_PASSWORD_REREQUEST_PASSWORD2	Segunda contraseña.

Protección contra la vulnerabilidad Cross Site Scripting

Para utilizar la característica de seguridad de protección contra la vulnerabilidad Cross Site Scripting necesita definir las vistas ProhibitedAttrsErrorView, ProhibitedCharacterErrorView y ProhibCharEncodingErrorView para la tienda.

ProhibitedAttrsErrorView
Esta vista se muestra al usuario cuando la petición no se procesa porque contiene atributos prohibidos.

ProhibitedCharacterErrorView
Esta vista se muestra al usuario cuando la petición no se procesa porque contiene caracteres prohibidos.

ProhibCharEncodingErrorView
Es igual que la vista anterior ProhibitedCharacterErrorView.

Habilitación del tiempo de espera de conexión

Nota: Para utilizar la característica de seguridad Tiempo de espera de conexión para una tienda, necesita definir las vistas LoginTimeoutErrorView y ReLogonFormView para la tienda tal como se describe en el apartado "Tiempo de espera de conexión" en la página 55.

Utilice el nodo de Tiempo de espera de conexión del Gestor de configuración para habilitar o inhabilitar la característica Tiempo de espera de conexión. Cuando esta característica está habilitada, a un usuario de WebSphere Commerce que esté inactivo durante un extenso periodo de tiempo se le desconectará del sistema y se le solicitará que vuelva a conectarse. Si el usuario se conecta de forma satisfactoria, WebSphere Commerce ejecuta la petición original realizada por el usuario. Si el usuario no se puede conectar, la petición original se descarta y el usuario permanece desconectado del sistema.

Tenga en cuenta que para las herramientas de WebSphere Commerce (por ejemplo la Consola de administración, WebSphere Commerce Accelerator, etc), el tiempo de espera de conexión no presenta una página de reconexión al usuario. En lugar de ello, cierra la ventana de navegador y el usuario debe decidir si vuelve a conectarse a la herramienta. De este modo, en el caso de las herramientas, no se procesa la petición original que el usuario somete.

Para habilitar esta característica:

1. Inicie el Gestor de configuración y vaya al nodo de Tiempo de espera de conexión para la instancia del modo siguiente: **WebSphere Commerce >**

nombre_sistema_principal **> Lista de instancias >** *nombre_instancia* **> Propiedades de instancia> Tiempo de espera de conexión**

2. Para activar la característica Tiempo de espera de conexión, pulse el recuadro de selección **Habilitar**.
3. Entre el valor de tiempo de espera de conexión, en segundos, en el campo Valor.
4. Para aplicar los cambios en el Gestor de configuración, pulse **Aplicar**.
5. Después de actualizar satisfactoriamente la configuración para la instancia, recibirá un mensaje indicando una actualización satisfactoria.
6. En la Consola de administración de WebSphere Application Server, detenga y reinicie la instancia de servidor WebSphere Commerce.

Tenga en cuenta que el valor de tiempo de espera de conexión se almacena en el archivo *instancia*.xml en milisegundos, mientras que el valor en el Gestor de configuración se entra en segundos.

Activación de la invalidación de contraseña

Nota: Para utilizar la característica de seguridad Invalidación de contraseña, necesita definir la vista ChangePassword para la tienda tal como se describe en el apartado "Invalidación de contraseña" en la página 55.

Utilice el nodo de Invalidación de contraseña del Gestor de configuración para habilitar o inhabilitar la característica Invalidación de contraseña. Esta característica, cuando está habilitada, requiere que los usuarios de WebSphere Commerce cambien su contraseña si la contraseña del usuario ha caducado. En este caso, se redirige al usuario a una página en la que se le pide que cambie su contraseña. Los usuarios no podrán acceder a ninguna página segura del sitio hasta que hayan cambiado la contraseña. Para habilitar esta característica:

1. Inicie el Gestor de configuración y vaya al nodo de Invalidación de contraseña para la instancia, del modo siguiente: **WebSphere Commerce >** *nombre_sistema_principal* **> Lista de instancias >** *nombre_instancia* **> Propiedades de instancia > Invalidación de contraseña**
2. Para activar la característica Invalidación de contraseña, pulse el recuadro de selección **Habilitar**.
3. Para aplicar los cambios en el Gestor de configuración, pulse **Aplicar**.
4. Después de actualizar satisfactoriamente la configuración para la instancia, recibirá un mensaje indicando una actualización satisfactoria.
5. En la Consola de administración de WebSphere Application Server, detenga y reinicie la instancia de servidor WebSphere Commerce.

Habilitación de mandatos protegidos por contraseña

Nota: Para utilizar la característica de seguridad Mandatos protegidos por contraseña, necesita definir las vistas PasswordReEnterErrorView y PasswordReEnterFormView para la tienda tal como se describe en el apartado "Mandatos protegidos por contraseña" en la página 56.

Utilice el nodo de Mandatos protegidos por contraseña del Gestor de configuración para habilitar o inhabilitar la característica de mandatos protegidos por contraseña. Cuando está habilitada esta característica, WebSphere Commerce requiere que los

usuarios que están conectados a WebSphere Commerce entren su contraseña antes de continuar una petición que ejecute mandatos de WebSphere Commerce designados.

Precaución: Cuando configure mandatos protegidos por contraseña, algunos de los mandatos mostrados en la lista de selección de mandatos pueden ser ejecutados por usuarios genéricos o invitados. Si se configuran dichos mandatos como protegidos por contraseña, se prohibirá a los usuarios genéricos e invitados que los ejecuten. Por consiguiente, deberá tener cuidado cuando configure mandatos para que estén protegidos por contraseña.

Para habilitar esta característica:

1. Inicie el Gestor de configuración y vaya al nodo Mandatos protegidos por contraseña para la instancia, del modo siguiente: **WebSphere Commerce >** *nombre_sistema_principal* **> Lista de instancias >** *nombre_instancia* **> Propiedades de instancia > Mandatos protegidos por contraseña**
2. En la pestaña General:
   a. Para habilitar la característica Mandatos protegidos por contraseña, pulse **Habilitar**.
   b. Entre el número de reintentos en el campo Reintentos. (El número de reintentos por omisión es 3.)
3. En la pestaña Avanzada:
   a. En la ventana Lista de mandatos protegidos por contraseña, seleccione un mandato de WebSphere Commerce que desee proteger y pulse **Añadir**. El mandato que ha seleccionado figura en la ventana Lista de mandatos protegidos por contraseña protegidas actuales.
   b. Si desea inhabilitar la protección por contraseña de cualquier mandato de WebSphere Commerce, seleccione el mandato en la ventana Lista de mandatos protegidos por contraseña y pulse **Eliminar**.
4. Para aplicar los cambios en el Gestor de configuración, pulse **Aplicar**.
5. Después de actualizar satisfactoriamente la configuración para la instancia, recibirá un mensaje indicando una actualización satisfactoria.
6. En la Consola de administración de WebSphere Application Server, detenga y reinicie la instancia de servidor WebSphere Commerce.

Nota: WebSphere Commerce sólo mostrará los mandatos que se han designado como `autenticados` o los que tienen establecido el distintivo `https` en la tabla `URLREG` de la lista de mandatos disponibles.

Actualización de datos cifrados

Utilice la Herramienta de actualización de base de datos disponible en el nodo de base de datos del gestor de configuración para modificar la clave de comerciante y actualizar todos los datos cifrados (por ejemplo contraseñas o números de tarjeta de crédito) en una o varias bases de datos de WebSphere Commerce para una instancia determinada. Para utilizar la herramienta:

1. Inicie el Gestor de configuración y vaya a la entrada de base de datos específica, del modo siguiente: **WebSphere Commerce >** *nombre_sistema_principal* **> Lista de instancias >** *nombre_instancia* **> Propiedades de instancia > Base de datos >** *nombre_basedatos*
2. Pulse el botón derecho del ratón en *nombre_basedatos* y seleccione **Ejecutar herramienta de actualización de base de datos**

- Seleccione **Actualizar todas las bases de datos para esta instancia** para migrar los datos cifrados de todas las bases de datos de la instancia seleccionada.

  400 As iSeries da soporte a una sola configuración de base de datos, esta opción no se aplica a iSeries.
- Seleccione **Actualizar la base de datos seleccionada** para migrar los datos cifrados de una base de datos específica seleccionando la base de datos en la lista desplegable (por omisión).

3. Seleccione una acción que desee ejecutar en el recuadro Acciones y rellene la información necesaria en el campo Parámetros:

Acciones	Parámetros	Acción necesaria
Cambiar clave de comerciante	Clave de comerciante antigua	Entre la clave de comerciante existente utilizada al crear la instancia actual de WebSphere Commerce.
	Clave de comerciante nueva	Entre la clave de comerciante nueva. Es un número hexadecimal de 16 dígitos para que el Gestor de configuración vuelva a cifrar los datos cifrados actualmente. La Clave de comerciante debe tener un carácter alfanumérico (de a a f) como mínimo y un carácter numérico (de 0 a 9) como mínimo. Los caracteres alfanuméricos deben entrarse en letras minúsculas y no se puede entrar el mismo carácter más de cuatro veces en una fila.

4. Pulse en **Aceptar** para ejecutar la herramienta de actualización de base de datos para la base de datos de WebSphere Commerce seleccionada o para todas las bases de datos de WebSphere Commerce.
5. Después de actualizar satisfactoriamente la configuración para la instancia, recibirá un mensaje indicando una actualización satisfactoria.
6. En la Consola de administración de WebSphere Application Server, detenga y reinicie la instancia de servidor WebSphere Commerce.

Habilitación de la protección contra la vulnerabilidad Cross Site Scripting

Nota: Para utilizar la característica de seguridad de protección contra la vulnerabilidad Cross Site Scripting para una tienda, debe definir las vistas `ProhibitedAttrsErrorView`, `ProhibitedCharacterErrorView` y `ProhibCharEncodingErrorView` para la tienda, tal como se describe en el apartado "Protección contra la vulnerabilidad Cross Site Scripting" en la página 57.

Utilice el nodo Protección contra la vulnerabilidad Cross Site Scripting del Gestor de configuración para habilitar o inhabilitar esta característica de protección para la instancia. Cuando está habilitada, la protección contra la vulnerabilidad Cross Site Scripting rechaza las peticiones de usuario que contienen atributos o series que están designadas como no permitidos. En este nodo del Gestor de configuración, puede especificar los atributos y las series que no están permitidos. También puede excluir mandatos de la protección contra la vulnerabilidad Cross Site Scripting permitiendo que los valores de atributos especificados para dichos mandatos en

concreto contengan series prohibidas. Por omisión, la protección contra la vulnerabilidad Cross Site Scripting está inhabilitada.

Aviso: La protección contra la vulnerabilidad Cross Site Scripting es una característica restrictiva en el sentido que restringe la ejecución de los mandatos basándose en la configuración. La característica no comprueba qué atributos o series se han definido como prohibidos, de modo que cuando la configure, asegúrese de que los atributos prohibidos no sean los utilizados por los mandatos. Asimismo asegúrese de que las series prohibidas no sean valores que se suelen pasar a los mandatos. Tenga muchísimo cuidado cuando configure esta característica.

Para habilitar esta característica:

1. Inicie el Gestor de configuración y vaya al nodo Protección contra la vulnerabilidad Cross Site Scripting para la instancia, del modo siguiente: **WebSphere Commerce >** *nombre_sistema_principal* **> Lista instancias >** *nombre_instancia* **> Propiedades de instancia > Protección contra la vulnerabilidad Cross Site Scripting**
2. Utilice la pestaña General para activar la característica Protección contra la vulnerabilidad Cross Site Scripting del modo siguiente:
   a. Pulse **Habilitar**.
   b. Para añadir atributos que desea prohibir para los mandatos de WebSphere Commerce, pulse el botón derecho del ratón en la tabla Atributos prohibidos y seleccione **Añadir fila**. Escriba el atributo que desea prohibir. Sólo puede especificar un atributo por fila.
   c. Para eliminar atributos de la tabla Atributos prohibidos, resalte en la tabla la línea que contiene el atributo, pulse el botón derecho del ratón en dicha línea y seleccione **Suprimir fila**.
   d. Para añadir series que desea prohibir para los mandatos de WebSphere Commerce, pulse el botón derecho del ratón en la tabla Caracteres prohibidos y seleccione **Añadir fila**. Añada la serie que desea prohibir. Sólo puede especificar una serie por fila.
   e. Para eliminar caracteres de la tabla Caracteres prohibidos, resalte en la tabla Caracteres prohibidos la línea que contiene el carácter, pulse el botón derecho del ratón en dicha línea y seleccione **Suprimir fila**.

   Nota: Las series siguientes están especificadas por omisión en los campos de caracteres prohibidos. Estas series se utilizan muy comúnmente como códigos de script en los ataques Cross Site Scripting.
   - `<SCRIPT`
   - `&lt;SCRIPT`
   - `<%` y `&lt;%`

   .
3. Utilice la pestaña Avanzada para excluir mandatos de WebSphere Commerce de la protección contra Cross Site Scripting permitiendo que los valores de atributos especificados para esos mandatos en particular contengan series prohibidas, como se indica a continuación:
   a. Seleccione los mandatos en el recuadro Lista de mandatos.
   b. En la ventana Lista de atributos excluidos, escriba una lista de atributos, separados por comas, para los que se permiten los caracteres prohibidos y pulse **Añadir**.

c. Para eliminar un mandato junto con sus atributos, seleccione el mandato en la ventana Lista de mandatos excluidos y pulse **Eliminar**.

También puede eliminar atributos específicos de un mandato seleccionando el atributo y pulsando **Eliminar**.

4. Para aplicar los cambios en el Gestor de configuración, pulse **Aplicar**.
5. Después de actualizar satisfactoriamente la configuración para la instancia, recibirá un mensaje indicando una actualización satisfactoria.
6. En la Consola de administración de WebSphere Application Server, detenga y reinicie la instancia de servidor WebSphere Commerce.

Notas:

1. Cuando se excluyen mandatos de la protección contra la vulnerabilidad Cross Site Scripting, los valores de los atributos especificados se codifican utilizando la configuración de símbolos de HTML. Por ejemplo, el mandato `cmd1?user=<Thomas>` se codifica como `ascmd1?user=&#60;Thomas&#62;`
2. Cuando especifique la serie en los campos de caracteres prohibidos, tenga presente que:
   - Una determinada secuencia de caracteres puede hacer que la serie se convierta en un solo carácter de acuerdo con los estándares de codificación de URL. Por ejemplo, la serie `<%bb` se convertirá en una serie `<X` donde *X* es un solo carácter que tiene un valor de representación hexadecimal de HEX '`bb`' (187 decimal). En este caso, la protección contra la vulnerabilidad Cross Site Scripting no captará `<%bb` si esta serie se pasa en un URL.
   - Una determinada secuencia de caracteres puede hacer que falle la conversión de serie si éstos no cumplen con los estándares de codificación de URL. Por ejemplo, la serie `<%gg` hará que falle la conversión porque HEX '`gg`' no es una representación de valor hexadecimal válida. En este caso, la serie `<%gg` producirá una excepción, haciendo que no haya ninguna respuesta a la petición de URL que contiene dicha serie, tanto si la protección contra la vulnerabilidad Cross Site Scripting está habilitada como si no lo está.

Ejemplo: Examine los ejemplos siguientes:

- Series prohibidas: `<SCRIPT`, `<%`

  Atributos prohibidos: `mycomment`, `description`

Mandato	Estado
cmd1?description=Available...	rechazado
cmd2?userid=Thomas...	aceptado
cmd3?mycomment=<SCRIPT>...	rechazado
cmd4?password=<%...%>...	rechazado

- Si desea permitir que el atributo `text` del mandato `cmd1` contenga las series prohibidas (`<SCRIPT`, `<%`) pero no así otros atributos. Por ejemplo, para el atributo `txt`, puede excluir `cmd1` y especificar `text` como el atributo excluido.

Mandato	Estado
cmd1?text=<SCRIPT>...	aceptado
cmd1?text=<%...%>...	aceptado
cmd1?txt=<SCRIPT>...	rechazado
cmd1?txt=<%..%>...	rechazado

Habilitación del registro de accesos

Cuando está habilitada, la característica de registro de accesos anota cronológicamente todas las peticiones de entrada realizadas a WebSphere Commerce Server o sólo las peticiones que generan violaciones de acceso. Una anomalía de autenticación, una autorización insuficiente para ejecutar un mandato o el restablecimiento de una contraseña que no se ajusta a las normas para las contraseñas del sitio son ejemplos de violaciones de acceso. Cuando está habilitada, el registro de accesos permite que un administrador de WebSphere Commerce identifique de forma rápida las amenazas para la seguridad en el sistema WebSphere Commerce.

Cuando se produce un suceso de anomalía de autenticación o de anomalía de autorización, se anota cronológicamente la información siguiente en las tablas de base de datos de archivos de anotaciones cronológicas `ACCLOGMAIN` y `ACCLOGSUB`:

- Nombre de sistema principal del cliente
- ID de la hebra que ejecuta el mandato
- ID de usuario del cliente
- Hora en la que se ha producido el suceso
- Mandato que se ha ejecutado
- Tienda para la que se ha ejecutado el mandato
- Recurso en el que se ha realizado la operación
- Resultado de la comprobación de control de acceso

Para habilitar el registro de accesos, realice lo siguiente:

1. Inicie el Gestor de configuración.
2. Seleccione **Nombre de sistema principal** > **Instancia** > **Lista_instancias** y, a continuación, abra la carpeta **Componentes**.
3. Seleccione **AccessLoggingEventListener**.
4. En el panel General, active el recuadro de selección **Habilitar componente**.
5. Seleccione el panel Avanzada y habilite **Iniciar**.
6. Pulse **Aplicar**.
7. Salga del Gestor de configuración.
8. Reinicie WebSphere Application Server.

Para cambiar el tamaño del archivo de anotaciones cronológicas o para especificar si todas las peticiones se anotarán o no, deberá editar manualmente el archivo *instancia*`.xml` para la instancia de WebSphere Commerce ubicada en el subdirectorio de instancias de WebSphere Commerce.

1. Abra en un editor el archivo *instancia*`.xml` para la instancia.
2. Localice el nodo siguiente, que está ubicado en el nodo `<LogSystem>/<activitylog>`:

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

   donde:

   - *aa* es un valor entero que especifica el número máximo de entradas que se anotarán en la memoria antes de que se graben las entradas en la base de datos. Generalmente cuanto mayor sea el número, mejor será el rendimiento en lo que respecta al registro de accesos. El valor por omisión es 32.
   - *bbbbb* es `true` o `false`. El valor `true` significa que se anotan cronológicamente todas las peticiones de entrada. El valor `false` significa que sólo se anotan

cronológicamente las violaciones de acceso. Para evitar un registro excesivo o innecesario, se recomienda el valor `false`. Utilice `true` sólo cuando sospeche que existen problemas de autenticación o se produce una violación de la seguridad en el sitio. El valor por omisión es `false`.

3. Cuando haya realizado las actualizaciones, guarde el archivo *instancia*`.xml` de la instancia de WebSphere Commerce.
4. Reinicie WebSphere Application Server.

En el ejemplo siguiente, el registro de accesos conserva 3 entradas en memoria antes de anotar cronológicamente las entradas en las tablas de base de datos. Además, anota todas las peticiones de entrada a WebSphere Commerce Server:

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

Configuración de la política de cuentas

La página Política de cuentas de la Consola de administración de WebSphere Commerce le permite configurar una política de cuentas. Esta página lista todas las políticas de cuentas existentes, incluidas las políticas predefinidas que proporciona WebSphere Commerce. Una política de cuentas define las políticas relacionadas con las cuentas, por ejemplo las políticas de contraseñas y de bloqueo de cuentas. En esta página:

- Puede crear una nueva política de cuentas pulsando **Nueva**.
- Puede cambiar las características de una política de cuentas existente seleccionando la política en la lista y pulsando **Cambiar**.
- Puede suprimir una política de cuentas existente seleccionando la política en la lista y pulsando **Suprimir**.

Para crear una política de cuentas nueva:

1. Abra la Consola de administración de WebSphere Commerce.
2. En el menú desplegable Seguridad de la Consola de administración, pulse **Política de cuentas**.
3. En la página Política de cuentas, pulse **Nueva** para crear una política de cuentas nueva.
4. Entre un nombre para la política de cuentas en el campo Nombre (por ejemplo, `mi_política_cuentas`).
5. En el menú Política de contraseñas, seleccione una política de contraseñas ya existente.
6. En el menú Política de bloqueo de cuentas, seleccione una política de bloqueo de cuentas ya existente.
7. Pulse **Aceptar**.

Una vez haya creado una política de cuentas, puede asignarla a un usuario. Tenga en cuenta que no puede suprimir una política de cuentas si ésta se está utilizando (es decir, la política de cuentas se ha asignado a un usuario).

Consulte también el apartado “Políticas de autenticación por omisión” en la página 68 para obtener más información.

Configuración de una política de contraseñas

La página Política de contraseñas de la Consola de administración de WebSphere Commerce le permite controlar la selección de la contraseña de un usuario con el fin de definir las características de la contraseña y así asegurarse de que ésta cumple con la política de seguridad del sitio. Esta página lista todas las políticas de cuentas existentes, incluidas las políticas predefinidas que proporciona WebSphere Commerce por omisión.

Una política de contraseñas define los atributos que debe satisfacer la contraseña. La política de contraseñas impone las condiciones siguientes:

- Si el ID de usuario y la contraseña deben coincidir.
- Número máximo de apariciones de caracteres consecutivos.
- Número máximo de apariciones de cualquier carácter.
- Duración máxima de las contraseñas.
- Número mínimo de caracteres alfabéticos.
- Número mínimo de caracteres numéricos.
- Longitud mínima de la contraseña.
- Si se puede volver a utilizar la contraseña anterior del usuario.
- Puede crear una nueva política de contraseñas pulsando en **Nueva**.
- Puede cambiar las características de una política existente seleccionando la política en la lista y pulsando **Cambiar**.
- Puede suprimir una política existente seleccionando la política de contraseñas en la lista y pulsando **Suprimir**.

Para crear una política de contraseñas nueva:

1. Abra la Consola de administración de WebSphere Commerce.
2. En el menú desplegable Seguridad de la Consola de administración, pulse **Política de contraseñas**.
3. En la página Política de contraseñas, pulse **Nueva** para crear una nueva política de contraseñas.
4. Entre un nombre para la política de contraseñas en el campo Nombre (por ejemplo `mi_política_contraseñas`)
5. Actualice lo siguiente según sea necesario para modificar cualquiera de los valores respecto al valor por omisión para los compradores:
   - **¿Pueden coincidir el ID de usuario y la contraseña?** Define si el ID de usuario y la contraseña pueden ser idénticos o no. Seleccione `Sí` o `No` en la lista.
   - **Número máximo de tipos de caracteres consecutivos**. Define el número máximo de apariciones de caracteres consecutivos en una contraseña. El valor mínimo es 2 caracteres consecutivos. Por ejemplo, con un valor de 2, un usuario no puede entrar una contraseña como `aaabc`.
   - **Número máximo de apariciones de cualquier carácter**. Define el número máximo de veces que el mismo carácter puede aparecer en una contraseña. El valor mínimo es 1 instancia de un carácter. Por ejemplo, con un valor de 2, un usuario no puede entrar una contraseña como `abcaabc`.
   - **Duración máxima de la contraseña.** Define el periodo máximo de tiempo, en días, durante el cual puede existir una contraseña. El valor mínimo es 1 día. Una vez transcurrido este periodo de tiempo, se solicita al usuario que cambie la contraseña.

- **Número mínimo de caracteres alfabéticos**. Define el número mínimo de caracteres alfabéticos que se necesitan en una contraseña. El valor mínimo es 0 caracteres alfabéticos.
- **Número mínimo de caracteres numéricos**. Define el número mínimo de caracteres numéricos que se necesitan en una contraseña. El valor mínimo es 0 caracteres numéricos.
- **Longitud mínima de la contraseña**. Define la longitud más pequeña de una contraseña, en caracteres. El valor mínimo es 1 carácter.
- **¿Se puede volver a utilizar la contraseña?** Define si la contraseña anterior de un usuario se puede volver a utilizar. Seleccione `sí` o `no` en la lista.

6. Pulse **Aceptar**.

Notas:

1. No puede suprimir una política de contraseñas si ésta se está utilizando (es decir, la política de contraseñas se ha asignado a un usuario).
2. Las políticas de contraseñas sólo entran en vigor si los usuarios están autenticados en la base de datos de WebSphere Commerce.

Consulte también el apartado "Políticas de autenticación por omisión" en la página 68 para obtener más información.

Configuración de una política de bloqueo de cuentas

La página Política de bloqueo de cuentas de la Consola de administración de WebSphere Commerce le permite configurar una política de bloqueo de cuentas para diferentes roles de usuario en WebSphere Commerce. Esta página lista todas las políticas de cuentas existentes, incluidas las políticas predefinidas que proporciona WebSphere Commerce por omisión. Si se inician acciones malintencionadas contra una cuenta de usuario, la política de bloqueo de cuentas inhabilita dicha cuenta a fin de reducir las posibilidades de que las acciones la pongan en peligro.

Una política de bloqueo de cuentas impone los elementos siguientes:

- El umbral de bloqueo de cuenta. Es el número de intentos de conexión no válidos antes de que se inhabilite la cuenta.
- Retardo de conexiones no satisfactorias consecutivas. Es el periodo de tiempo durante el cual no se permite que el usuario se conecte, después de dos intentos de conexión anómalos. El retardo se incrementa en el valor de retardo de tiempo configurado (por ejemplo 10 segundos) con cada anomalía de conexión consecutiva.

Para establecer la política de bloqueo de cuentas:

1. Abra la Consola de administración de WebSphere Commerce.
2. En el menú desplegable Seguridad de la Consola de administración, pulse **Política de bloqueo de cuentas**.
3. La página Política de bloqueo de cuentas lista todas las políticas de bloqueo de cuentas existentes. En esta página:
   - Puede crear una política nueva pulsando **Nueva.**
   - Puede cambiar las características de una política existente seleccionando la política en la lista y pulsando **Cambiar**.
   - Puede suprimir una política existente seleccionando la política en la lista y pulsando **Suprimir**.

Para una política de bloqueo de cuentas nueva, en la página Política de bloqueo de cuentas:

1. Entre un nombre para la política de bloqueo de cuentas en el campo Nombre (por ejemplo `mi_política`).
2. Entre un umbral de bloqueos de cuenta en el campo Umbral de bloqueos de cuenta. Por ejemplo, entre 6 (para seis intentos)
3. Entre el retardo de conexiones consecutivas no satisfactorias en segundos en el campo Tiempo de espera. Por ejemplo, entre 10 (para diez segundos).
4. Pulse **Aceptar**.

Notas:

1. No puede suprimir una política de bloqueo de cuentas si ésta se está utilizando (es decir, la política de bloqueo de cuentas se ha asignado a un usuario).
2. Las políticas de bloqueo de cuentas sólo entran en vigor si los usuarios están autenticados en la base de datos de WebSphere Commerce.

Inicio de una comprobación de seguridad

400 Esta característica no es aplicable en WebSphere Commerce para iSeries.

La página Iniciar comprobación de seguridad de la Consola de administración de WebSphere Commerce le permite iniciar manualmente un programa de seguridad que comprueba y suprime archivos temporales de WebSphere Commerce que por su contenido pueden suponer un peligro para la seguridad. Normalmente, el programa de comprobación de seguridad se ejecuta como un trabajo planificado y, por omisión, se ejecuta una vez al mes.

Para invocar el programa de comprobación de seguridad:

1. Abra la Consola de administración de WebSphere Commerce.
2. En el menú desplegable Seguridad de la Consola de administración, pulse **Comprobador de seguridad**.
3. En la página Iniciar comprobación de seguridad, pulse **Iniciar**.

Los resultados de la comprobación de seguridad, incluidas todas las acciones realizadas por el programa se graban en la ventana Archivo de anotaciones cronológicas de comprobación de seguridad y en el archivo `sec_check.log` del subdirectorio `logs`:

AIX Linux

Solaris `dir_instalación_WC/instances/`*`nombre_instancia`*`/logs`

Windows `dir_instalación_WC\instances\`*`nombre_instancia`*`\logs`

Windows En plataformas que no son de Windows, los permisos de archivos se los establece automáticamente WebSphere Commerce para que los usuarios que no tengan autorización no puedan acceder a los archivos confidenciales. En las plataformas Windows, necesitará establecer los permisos manualmente del modo siguiente. Este procedimiento asegura que solamente el grupo de administradores tenga acceso de `lectura/grabación/ejecución` a los archivos confidenciales.

1. En Windows Explorer, pulse el botón derecho del ratón en la carpeta *`unidad`*`:\WebSphere`.

2. Pulse **Propiedades** y **Seguridad**. Por omisión, el grupo ″Todos″ tiene el permiso **all** para esta carpeta.
3. Pulse **Agregar**.
4. Se visualiza una ventana (Seleccionar usuarios, equipos...). En esta ventana, seleccione el grupo **Administradores**.

   Nota: Aquí esto puede resultar un poco ambiguo, porque puede que vea Administrador como un usuario, pero lo que necesita añadir es el grupo Administrador, no el usuario Administrador.

   Pulse **Agregar** y, a continuación, pulse **Aceptar**.
5. En la pestaña Seguridad, se habrá añadido el grupo Administradores. Es necesario que elimine ″Todos″. Seleccione **Todos** y elimine la selección del recuadro ″Hacer posible que los los permisos...″
6. Pulse **Quitar** en la ventana Seguridad que se visualiza.

Campo Cifrado PDI del Gestor de configuración

Cuando configure la instancia de WebSphere Commerce, se le recomienda que seleccione el recuadro de selección Cifrado PDI. Cuando se habilita Cifrado PDI, se especifica que la informaciónde las tablas ORDPAYINFO y ORDPAYMTHD debe cifrarse. Cuando se selecciona el recuadro, la información de pago se almacena en la base de datos de WebSphere Commerce en formato cifrado.

Políticas de autenticación por omisión

WebSphere Commerce envía dos políticas de autenticación por omisión:

- “Compradores”
- “Administradores” en la página 69

Compradores

La política de cuentas por omisión para compradores contiene la política de bloqueo de cuentas por omisión y la política de contraseñas por omisión para compradores.

La política de bloqueo de cuentas por omisión para compradores contiene los siguientes atributos por omisión:

Atributo	Valor por omisión
Umbral de bloqueo de cuenta	6 intentos
Retardo de conexiones no satisfactorias consecutivas	10 segundos

La política de contraseñas por omisión para compradores contiene los siguientes atributos por omisión:

Atributo	Valor por omisión
Si el ID de usuario y la contraseña pueden coincidir	N (no pueden coincidir)
Número máximo de apariciones de caracteres consecutivos	3 caracteres
Número máximo de instancias de cualquier carácter	4 instancias

Atributo	Valor por omisión
Duración máxima de las contraseñas	180 días
Número mínimo de caracteres alfabéticos	1 carácter alfabético
Número mínimo de caracteres numéricos	1 carácter numérico
Longitud mínima de la contraseña	6 caracteres
Si se puede volver a utilizar la contraseña anterior	N (no se puede volver a utilizar)

A los compradores que se registra personalmente se les asigna la política de autenticación por omisión: Compradores.

Administradores

La política de cuentas por omisión para administradores contiene la política de bloqueo de cuentas por omisión y la política de contraseñas por omisión para compradores.

La política de bloqueo de cuentas por omisión para administradores contiene los siguientes atributos por omisión:

Atributo	Valor por omisión
Umbral de bloqueo de cuenta	3 intentos
Retardo de conexiones no satisfactorias consecutivas	20 segundos

La política de contraseñas por omisión para compradores contiene los siguientes atributos por omisión:

Atributo	Valor por omisión
Si el ID de usuario y la contraseña pueden coincidir	N (no pueden coincidir)
Número máximo de apariciones de caracteres consecutivos	3 caracteres
Número máximo de instancias de cualquier carácter	4 instancias
Duración máxima de las contraseñas	90 días
Número mínimo de caracteres alfabéticos	1 carácter alfabético
Número mínimo de caracteres numéricos	1 carácter numérico
Longitud mínima de la contraseña	8 caracteres
Si se puede volver a utilizar la contraseña anterior	N (no se puede volver a utilizar)

Al usuario administrador `wcsadmin` por omisión que se envía con WebSphere Commerce se la asigna la política de autenticación por omisión: `Administradores`.

Capítulo 5. Gestión de sesiones

Los navegadores Web y los sitios de comercio electrónico utilizan HTTP para comunicarse. Dado que HTTP es un protocolo sin estado (lo que significa que cada mandato se ejecuta de forma independiente sin ningún conocimiento de los mandatos que le han precedido), tiene que existir un modo para gestionar sesiones entre la parte del navegador y la parte del servidor.

WebSphere Commerce soporta dos tipos de gestión de sesiones: basada en cookies y de reescritura de URL. El administrador puede elegir dar soporte sólo a la gestión de sesiones basada en cookies o a la gestión de sesiones basada en cookies y de reescritura de URL. Si WebSphere Commerce sólo soporta la gestión de sesiones basada en cookies, los navegadores de los compradores deben poder aceptar cookies. Si se selecciona la gestión de sesiones basada en cookies y de reescritura de URL, WebSphere Commerce intentará primero utilizar cookies para gestionar sesiones y si el navegador del comprador se ha configurado de modo que acepta cookies, utilizará la reescritura de URL.

Gestión de sesiones basada en cookies

Cuando se utiliza la gestión de sesiones basada en cookies, el servidor Web envía al navegador un mensaje (cookie) que contiene información del usuario. Este cookie se devuelve al servidor cuando el usuario intenta acceder a determinadas páginas. Al devolver el cookie, el servidor es capaz de identificar al usuario y recupera la sesión del usuario de la base de datos de sesiones, manteniendo de este modo la sesión del usuario. Una sesión basada en cookies finaliza cuando el usuario se desconecta o cierra el navegador. La gestión de sesiones basada en cookies es segura y tiene ventajas de rendimiento. La gestión de sesiones basada en cookies es segura porque utiliza un código de identificación que solamente fluye a través de SSL. La gestión de sesiones basada en cookies tiene importantes ventajas de rendimiento porque el mecanismo de almacenamiento en antememoria WebSphere Commerce solamente soporta las sesiones basadas en cookies y no la reescritura de URL. Se recomienda la gestión de sesiones basada en cookies para las sesiones de comprador.

Si no está utilizando la reescritura de URL y desea asegurarse de que los usuarios tengan cookies habilitados en los navegadores, seleccione **Prueba de aceptación de cookies** en la página Gestión de sesiones del Gestor de configuración. Esto informa al comprador de que si el navegador no acepta cookies, o si éstos se han inhabilitado, necesitará un navegador con soporte para cookies para navegar por el sitio de WebSphere Commerce.

Por razones de seguridad, la gestión de sesiones basada en cookies utiliza dos tipos de cookies:

- Cookie de sesión no seguro

  Se utiliza para gestionar datos de sesión. Contiene el ID de sesión, el idioma negociado, la tienda actual y la moneda preferida de los compradores cuando se crea el cookie. Este cookie puede desplazarse entre el navegador y el servidor bajo una conexión SSL o no SSL. Existen dos tipos de cookies de sesión no seguros:

  – Un cookie de sesión de WebSphere Application Server está basado en el estándar de sesión HTTP de servlet. Los cookies de WebSphere Application

Server permanecen en la memoria o en la base de datos cuando se efectúa un despliegue entre varios nodos. Para obtener más información, busque ″gestión de sesiones″ en el Centro de información de WebSphere Application Server (`http://www.ibm.com/software/webservers/appserv/infocenter.html`).

– Un cookie de sesión de WebSphere Commerce es interno para WebSphere Commerce y no permanece en la base de datos.

Para seleccionar qué tipo de cookie va a utilizar, seleccione `WCS` o `WAS` para el parámetro **Gestor de sesiones de cookies** en la página Gestión de sesiones del gestor de configuración.

- Cookie de autenticación segura

  Se utiliza para gestionar datos de autenticación. Un cookie de autenticación se desplaza a través de SSL y lleva una indicación de la hora para proporcionar la máxima seguridad. Es el cookie utilizado para autenticar al usuario siempre que se ejecuta un mandato que maneje datos confidenciales, por ejemplo el mandato `DoPaymentCmd` que solicita el número de tarjeta de crédito de un usuario. Existe un riesgo mínimo de que un usuario no autorizado pueda robar y utilizar este cookie. WebSphere Commerce siempre genera cookies de código de autenticación cuando se está utilizando la gestión de sesiones basada en cookies.

Se necesitan los cookies de código de autenticación y de sesión para ver páginas seguras.

Para los errores de cookie, se llama a `CookieErrorView` bajo las circunstancias siguientes:

- El usuario se ha conectado desde otra ubicación con el mismo ID de conexión.
- El cookie ha quedado corrupto y/o se ha manipulado indebidamente.
- Si la aceptación de cookies se establece en “`true`” y el navegador del usuario no tiene soporte para cookies.

Utilización de cookies para la gestión de sesiones

Para utilizar cookies en WebSphere Commerce, haga lo siguiente:

1. Abra el Gestor de configuración.
2. Seleccione la **Instancia** y, a continuación, abra la carpeta **Gestión de sesiones**.
3. Seleccione los valores de sesión apropiados.
   - Prueba de aceptación de cookies

     Seleccione este recuadro si el navegador del cliente acepta cookies para un sitio que sólo soporta cookies.
   - Gestor de sesiones de cookies

     Seleccione si desea que WebSphere Commerce o WebSphere Application Server realice la gestión de cookies. El valor por omisión es WebSphere Commerce.

     – Un cookie de sesión de WebSphere Application Server está basado en el estándar de sesión HTTP de servlet. Los cookies de WebSphere Application Server permanecen en la memoria o en la base de datos cuando se efectúa un despliegue entre varios nodos. Para obtener más información, busque ″gestión de sesiones″ en el Centro de información de WebSphere Application Server (`http://www.ibm.com/software/webservers/appserv/infocenter.html`.

     – Un cookie de sesión de WebSphere Commerce es interno a WebSphere Commerce y no permanece en la base de datos.

4. Pulse la pestaña **Avanzadas**. Seleccione los valores de sesión apropiados.
   - Vía de acceso de cookies

     Especifica la vía de acceso para el cookie, que es el subconjunto de los URL a los que se debe enviar un cookie. Generalmente este campo no se debe modificar.

     Para obtener información detallada acerca de las vías de acceso de cookies, consulte la especificación de cookies de Netscape y el RFC 2109.
   - Dominio del cookie

     Especifica un patrón de restricción de dominio. Generalmente este campo no se debe modificar.

     Un dominio especifica los servidores que deben ver un cookie. Por omisión, los cookies solamente se devuelven al servidor WebSphere Commerce Server que los ha emitido. Por omisión, los cookies sólo se devuelven al sistema principal que los ha guardado. La especificación de un patrón de nombre de dominio prevalece sobre esto. El patrón debe empezar con un punto y debe contener dos puntos como mínimo. Un patrón sólo coincide con una entrada más allá del punto inicial. Por ejemplo, "`.ibm.com`" es válido y coincide con "`a.ibm.com`" y con "`b.ibm.com`" pero no con "`www.a.ibm.com`". Para obtener detalles sobre los patrones de dominio, consulte el RFC 2109 y la Especificación de cookie de Netscape.
5. Pulse **Aplicar**.
6. Cierre el Gestor de configuración.
7. En la Consola de administración de WebSphere Application Server, detenga y reinicie la instancia de servidor WebSphere Commerce.

Reescritura de URL

Con la reescritura de URL, en todos los enlaces que se devuelven al navegador o que se redireccionan se añade el ID de sesión. Cuando el usuario pulsa estos enlaces, el formulario de URL reescrito se envía al servidor como parte de la petición del cliente. Un motor de servlets reconoce el ID de sesión en el URL y lo guarda para obtener el objeto correcto para este usuario. Si desea utilizar la reescritura de URL, no puede utilizar archivos HTML (archivos con extensiones `.html` o `.htm`) para los enlaces. Para utilizar la reescritura de URL, se deben utilizar archivos JSP para la visualización. Una sesión con reescritura de URL caduca cuando el comprador se desconecta.

Nota: El almacenamiento en antememoria dinámico de WebSphere Commerce y la reescritura de URL no pueden actuar conjuntamente. Si la reescritura de URL está activada, debe inhabilitará el componente de almacenamiento en antememoria dinámico de WebSphere Commerce. Para obtener más información, consulte el capítulo sobre almacenamiento en antememoria dinámico de la publicación *WebSphere Commerce, Guía de administración*.

Utilización de gestión de sesiones de reescritura de URL

Para especificar cómo se deben gestionar las sesiones, realice lo siguiente:

1. Abra el Gestor de configuración.
2. Seleccione la **Instancia** y, a continuación, abra la carpeta **Gestión de sesiones**.
3. Seleccione los valores de sesión apropiados.

   Habilite la reescritura de URL. Seleccione este recuadro para utilizar la reescritura de URL para la gestión de sesiones.

   Gestor de sesiones de cookies. Seleccione WebSphere Application Server.

4. Pulse **Aplicar**.
5. Cierre el Gestor de configuración.
6. En la Consola de administración de WebSphere Application Server, detenga y reinicie la instancia de servidor WebSphere Commerce.

Escritura de plantillas de JSP para la reescritura de URL

Si desea utilizar la reescritura de URL para mantener el estado de sesión, no incluya enlaces a partes de la aplicación Web en archivos HTML corrientes. Esta restricción es necesaria porque no se puede utilizar la codificación de URL en archivos HTML corrientes. Para mantener el estado utilizando la reescritura de URL, cada página que el usuario solicita durante la sesión debe tener código que el intérprete Java pueda comprender. Si tiene archivos HTML corrientes de este tipo en la aplicación Web y en partes del sitio a las que puede que el usuario acceda durante la sesión, conviértalos en archivos JSP. Esto afectará al escritor de aplicaciones porque, a diferencia del mantenimiento de sesiones con cookies, el mantenimiento de sesiones con reescritura de URL requiere que cada plantilla JSP de la aplicación utilice la codificación de URL para cada atributo `HREF` en los códigos `<A>`. La sesión se perderá si una o varias plantillas JSP de una aplicación no llaman a `encodeURL(Serie url)` o codifican los métodos `RedirectURL(Serie url)`.

Escritura de enlaces

Con la reescritura de URL, en todos los enlaces que se devuelven al navegador o se redireccionan se debe añadir el ID de sesión. Por ejemplo, este enlace en una página Web:

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

se reescribe como

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

Cuando el usuario pulsa este enlace, el formulario de URL reescrito se envía al servidor como parte de la petición del cliente. El Motor de servlets reconoce `;$jsessionid$DA32242SSGE2` como ID de sesión y lo guarda para obtener el objeto `HttpSession` correcto para este usuario.

El ejemplo siguiente muestra cómo se puede incorporar código Java a un archivo JSP:

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

Para volver a escribir los URL que está devolviendo al navegador, llame al método `encodeURL()` en la plantilla JSP antes de enviar el URL a la corriente de salida. Por ejemplo, si una plantilla JSP que no utiliza la reescritura de URL tiene:

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

sustitúyala por:

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

Para volver a escribir los URL que está redireccionando, llame al método `encodeRedirctURL()`. Por ejemplo, si la plantilla JSP tiene:

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

Los métodos `encodeURL()` y `encodeRedirectURL()` forman parte del objeto `HttpServletResponse`. En ambos casos, estas llamadas comprueban si la reescritura de URL está configurada antes de codificar el URL. Si no está configurada, se devuelve el URL original.

Escritura de formularios: Si desea escribir formularios para someterlos, llame a `response.encodeURL("Logon");` en el código `ACTION` de la plantilla de formulario. Por ejemplo,

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

Escritura de la primera página: La página de entrada, generalmente la página de presentación, no puede contener marcos. Si desea utilizar marcos en la tienda, puede hacer que una página sin marcos con un enlace a la tienda actúe como página de entrada de la tienda. Sin embargo, si la tienda utiliza marcos y un cliente intenta acceder a esas páginas con marcos sin pasar primero por la página de entrada, puede que la sesión de dicho cliente se pierda. Los clientes también pueden perder la sesión si utilizan el botón **Anterior** (sólo con marcos) para volver a la página de entrada y renuevan la página de entrada. La renovación de la página de entrada les proporciona un nuevo ID de sesión. Para ayudar a evitar este tipo de pérdida de sesión, es necesario un enlace que retroceda a la página de entrada como alternativa al botón **Anterior**.

Gestión de sesiones a nivel de tienda

El diagrama siguiente ilustra la infraestructura de registro a nivel de tienda de WebSphere Commerce. El registro a nivel de tienda utiliza los roles de control de acceso para asociar un comprador con una tienda.

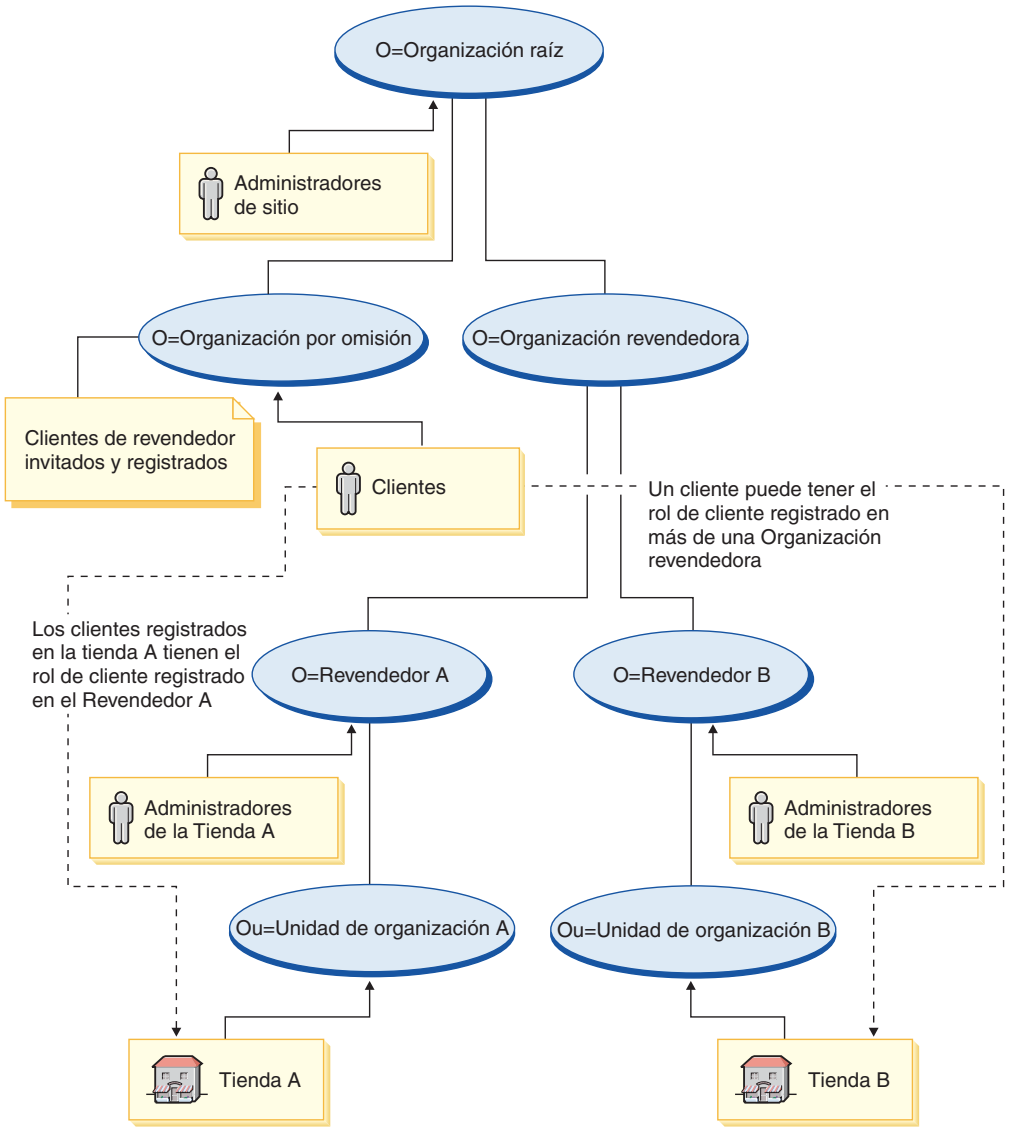


Figura 3. Registro a nivel de tienda

No es necesario que los usuarios que compren en un tienda sean miembros de la organización de la tienda pero deben desempeñar en la organización un rol de compras, es decir, el rol de cliente registrado. Los usuarios que desempeñan un rol administrativo en una organización suelen asociarse a la organización estableciendo una relación de predecesora con la organización.

Por ejemplo, suponga que tiene una tienda llamada Tienda_A como en el diagrama anterior. Asimismo, suponga que Marta compra en la Tienda_A y que Juanjo es un empleado de la Tienda_A responsable de las tareas administrativas de la misma. Para dar forma a este escenario desde una perspectiva de organización, Juanjo debe estar bajo la organización de la Tienda_A pero no así Marta. Dado que Marta no es una empleada de la Tienda_A, se asocia a Marta con la Tienda_A haciéndola desempeñar el rol de compras en la organización de la Tienda_A.

Una tienda determina todos los compradores registrados que tiene buscando a todos los usuarios que poseen un rol de compras en la organización de la tienda. A continuación, el administrador de usuarios puede seguir realizando las tareas de toda la tienda como, por ejemplo, definir una campaña para todos los usuarios

registrados en una tienda, o acciones específicas como, por ejemplo, restaurar la contraseña de un usuario registrado en su tienda.

En relación con el diagrama de la Figura 3 en la página 76, tenga en cuenta el escenario siguiente:

- Marta, que es miembro de la organización por omisión, tiene un rol de compras en la organización de Revendedora_A. La organización padre de Revendedora_A es la organización revendedora.
- Revendedora_A es la propietaria de la Tienda_A.
- Marta no tiene un rol organizativo en la organización Revendedora_B.
- Revendedora_B es la propietaria de la Tienda_B.

Marta se conecta a la Tienda_A y compra de modo habitual. Cuando Marta accede a la Tienda_B, se le asigna una nueva identidad de sesión para la Tienda_B como usuaria invitada. Si vuelve a acceder una vez más a la Tienda_A, WebSphere Commerce utilizará la información de identidad de la sesión anterior en la Tienda_A para gestionar la sesión.

La identidad de la sesión de la Tienda_A debe volver a utilizarse para la Tienda_B si:

- La Tienda_A y la Tienda_B pertenecen a la misma organización.
- Marta tiene un rol definido en las dos organizaciones Revendedora_A y Revendedora_B.

Capítulo 6. Establecimiento y cambio de contraseñas

La mayoría de los componentes de WebSphere Commerce utilizan ID de usuario y contraseñas validadas por el sistema operativo. Para obtener información sobre cómo cambiar dichas contraseñas, consulte la documentación del sistema operativo. Este capítulo describe cómo establecer y cambiar contraseñas para los componentes de WebSphere Commerce que no validan los ID de usuario y las contraseñas a través del sistema operativo.

Consulta rápida de los ID de usuario, las contraseñas y las direcciones Web

La administración en el entorno de WebSphere Commerce requiere diversos ID de usuario. Estos ID de usuario junto con sus requisitos de autorizaciones se describen en la lista siguiente. Para los ID de usuario de WebSphere Commerce, se indican las contraseñas por omisión.

400 **Perfiles de usuario de iSeries**

Al instalar y configurar WebSphere Commerce, se utilizan dos perfiles de usuario de iSeries a los que se hace referencia con frecuencia:

- Un perfil de usuario que se crea y utiliza para instalar WebSphere Commerce e iniciar el Gestor de configuración. Para instalar y configurar WebSphere Commerce, deberá utilizar un perfil de usuario de iSeries de `USRCLS(*SECOFR)` o utilizar el perfil de usuario `QSECOFR`. Si necesita crear un perfil de usuario, consulte la publicación *WebSphere Commerce, Guía de instalación* para iSeries.
- Un perfil de usuario creado por el Gestor de configuración cuando se crea una instancia de WebSphere Commerce. Este perfil de usuario se conoce también como *perfil de usuario de instancia*. El Gestor de configuración crea un perfil de usuario de `USRCLS(*USER)` cada vez que se crea una instancia de WebSphere Commerce. Si necesita crear un perfil de usuario, consulte la publicación *WebSphere Commerce, Guía de instalación* para iSeries.

ID de usuario del Gestor de configuración

La interfaz gráfica de la herramienta Gestor de configuración le permite modificar el modo en que WebSphere Commerce está configurado. El ID de usuario y la contraseña por omisión del Gestor del configuración son `webadmin` y `webibm`.

AIX Linux Solaris Windows Puede acceder al Gestor de configuración desde la máquina de WebSphere Commerce o desde cualquier máquina de la misma red que WebSphere Commerce.

400 Para iSeries, puede acceder al Gestor de configuración desde cualquier máquina de Windows que esté en la misma red que el servidor iSeries.

ID de usuario de IBM HTTP Server

AIX Linux Solaris Windows Si está utilizando IBM HTTP Server, puede acceder a la página de presentación del servidor Web abriendo el navegador Web y escribiendo la dirección Web siguiente:

`http://nombre_sistema_principal`

Si ha personalizado el servidor Web, puede que sea necesario escribir el nombre de la página frontal del servidor Web después del nombre de sistema principal.

Administrador de instancias de WebSphere Commerce

El ID de usuario y la contraseña de Administrador de instancias se aplican a las herramientas de WebSphere Commerce siguientes:

- WebSphere Commerce Accelerator. Para acceder a WebSphere Commerce Accelerator desde una máquina remota que ejecuta un sistema operativo Windows, abra el navegador Web Internet Explorer y escriba la dirección Web siguiente:

  `https://nombre_sistema_principal:8000/accelerator`
- Consola de administración de WebSphere Commerce. Para acceder a la Consola de administración de WebSphere Commerce desde una máquina remota que ejecuta un sistema operativo Windows, abra el navegador Web Internet Explorer y escriba la dirección Web siguiente:

  `https://nombre_sistema_principal:8002/adminconsole`
- Consola de administración de organizaciones de WebSphere Commerce. Para acceder a la Consola de administración de organizaciones de WebSphere Commerce desde una máquina remota que ejecuta un sistema operativo Windows, abra el navegador Web Internet Explorer y escriba la dirección Web siguiente:

  `https://nombre_sistema_principal:8004/orgadminconsole`

Para las herramientas anteriores, escriba el ID de usuario de administrador y la contraseña que ha especificado cuando ha creado la instancia de WebSphere Commerce.

Nota: El ID de usuario de administrador no se debe suprimir nunca y debe tener siempre autorización de administrador de instancias.

WebSphere Commerce requiere que el ID de usuario y la contraseña se ajusten a las normas siguientes:

- La contraseña debe tener un mínimo de 8 caracteres de longitud.
- La contraseña debe incluir 1 dígito numérico como mínimo.
- La contraseña no debe contener más de 4 apariciones de un carácter.
- La contraseña no debe repetir el mismo carácter más de 3 veces.

Administrador de WebSphere Commerce Payments

Cuando se instala WebSphere Commerce Payments, automáticamente se asigna al ID de administrador de sitio de WebSphere Commerce el rol de administrador de Payments. Siga las instrucciones de la publicación *WebSphere Commerce, Guía de instalación* para conmutar la clase de dominio de Payments a WCSRealm si todavía no se ha llevado a cabo esta acción.

El rol de Administrador de Payments permite que un ID de usuario controle y administre WebSphere Commerce Payments.

400 **Nota:**

- No suprima ni cambie el nombre del ID de usuario de administrador de sitio que ha creado para la instancia ni cambie ningún rol de WebSphere Commerce Payments asignado previamente ya que las funciones de WebSphere Commerce relacionadas con WebSphere Commerce Payments no funcionarán.

Windows **Windows**

El ID de usuario de Windows *debe* tener autorización de Administrador. Si utiliza DB2, es necesario que el ID de usuario y la contraseña satisfagan las normas siguientes:

- No pueden tener más de 8 caracteres de longitud.
- Sólo pueden contener los caracteres A - Z, a - z, 0 - 9, @, #, $ y _.
- No pueden empezar por un subrayado (_).
- El ID de usuario no puede ser ninguno de los siguientes, en letras mayúsculas, minúsculas ni en una combinación de ambas: USERS, ADMINS, GUESTS, PUBLIC, LOCAL.
- El ID de usuario no puede empezar con ninguna de las palabras siguientes, ni en mayúsculas, ni en minúsculas ni en una combinación de ambas: IBM, SQL, SYS.
- El ID de usuario no puede coincidir con ningún nombre de servicio de Windows.
- El ID de usuario debe estar definido en la máquina local y debe pertenecer al grupo del Administrador local.
- El ID de usuario debe tener el derecho de usuario avanzado *Actuar como parte del sistema operativo*.

Puede realizar la instalación sin el derecho de usuario avanzado *Actuar como parte del sistema operativo*, sin embargo, el programa de instalación de DB2 no podrá validar la cuenta que especifique para el servidor de administración. Se recomienda que cualquier cuenta de usuario utilizada para instalar DB2 tenga este derecho de usuario avanzado.

Importante

Si el ID de usuario de Windows *no* tiene autorización de Administrador, tiene una longitud de más de 8 caracteres o no está definido en la máquina local, se le informará del problema y no podrá continuar con la instalación.

Si utiliza DB2, utilizará este ID de usuario como nombre de usuario de base de datos DB2 (ID de conexión de usuario de base de datos).

Si tiene que crear un ID de usuario que satisfaga los criterios anteriores, puede encontrar información sobre cómo crear un ID de usuario de Windows en la ayuda en línea de Windows.

Cómo cambiar la contraseña del Gestor de configuración

Puede cambiar la contraseña del Gestor de configuración al iniciar el Gestor de configuración pulsando **Modificar** en la ventana donde entra el ID de usuario y la contraseña.

Alternativamente para cambiar el ID de usuario o la contraseña de Gestor de configuración vaya al subdirectorio `bin` en la vía de acceso de instalación de WebSphere Commerce y escriba lo siguiente en una ventana de mandatos:

1. Vaya al subdirectorio `bin` de WebSphere Commerce:

   ```
   cd dir_instalación_WC55/bin
   ```

2. Ejecute el script wcs_encrypt para obtener una versión cifrada de la contraseña:

   AIX 400 Linux Solaris

   ./wcs_encrypt.sh *contraseña_nueva*

   Windows

   wcs_encrypt *contraseña_nueva*

3. Abra el archivo PwdMgr.xml en el directorio *dir_instalación_WC55*/instances y modifique LoginPassword por la contraseña que ha cifrado en el paso 2.

Establecimiento de la contraseña de administrador de IBM HTTP Server

AIX Linux Solaris Windows Para establecer la contraseña de administrador de IBM HTTP Server.

1. Vaya al directorio *dir_instalación_HTTPServer*/bin de la máquina.
2. Escriba el mandato siguiente:

   AIX Linux Solaris ./htpasswd -b ../conf/admin.passwd *user contraseña*

   Windows htpasswd -b conf\admin.passwd *usuario contraseña* donde *usuario* y *contraseña* son el ID de usuario y la contraseña que desea que tengan autorización administrativa para IBM HTTP Server.

Ya ha establecido satisfactoriamente la contraseña de administración de IBM HTTP Server.

Nota: Si la contraseña de administrador no existe, deberá ejecutar htpassword con la opción -c para crear en primer lugar la contraseña.

Cómo cambiar la contraseña del archivo de claves SSL

AIX Linux Solaris Windows Si está utilizando IBM HTTP Server, siga los pasos siguientes para cambiar la contraseña del archivo de claves SSL.

1. Windows Pulse el menú **Inicio** → **Programas** → **IBM HTTP Server** → **Programa de utilidad de gestión de claves**.
2. En el menú **Archivo de base de datos de claves**, seleccione **Abrir**.
3. Vaya al subdirectorio ssl bajo la vía de acceso de instalación de IBM HTTP Server de la máquina. El archivo de claves (que tiene la extensión de archivo .kdb) debería estar en esta carpeta. Si no está, cree un archivo de claves nuevo siguiendo las instrucciones descritas en el Capítulo 17, "Habilitación de SSL para producción con IBM HTTP Server", en la página 201.
4. En el menú **Archivo de base de datos de claves**, seleccione **Cambiar contraseña**. Aparecerá la ventana Cambiar contraseña.
5. Entre la contraseña nueva y habilite **Ocultar la contraseña para un archivo**.
6. Pulse **Aceptar**. La contraseña se ha cambiado.

Ahora ya ha cambiado satisfactoriamente la contraseña de administración del archivo de claves SSL.

Generación de contraseñas cifradas de WebSphere Commerce

Puede generar contraseñas cifradas para poder restaurar manualmente la contraseña de un usuario desde la línea de mandatos. Hay otras herramientas (por ejemplo, el mandato ResetPassword) que realizan la misma tarea. Para restaurar manualmente la contraseña, el administrador debe tomar la contraseña cifrada de la salida de los programas de utilidad siguientes y actualizar el campo `LOGONPASSWORD` de la tabla `USERREG`. El administrador también debe actualizar el campo `SALT` de la tabla `USERREG` con el valor de SALT elegido.

AIX Linux Solaris Windows WebSphere Commerce le permite generar contraseñas cifradas. Para generar contraseñas cifradas, realice lo siguiente:

1. Vaya al subdirectorio `bin` bajo el directorio de instalación de WebSphere Commerce.
2. Ejecute el script siguiente desde una línea de mandatos:

   Windows `wcs_password.bat` *`contraseña SALT clave_comerciante`*

   AIX Linux Solaris `./wcs_password.sh` *`contraseña SALT clave_comerciante`*

   donde

   - *contraseña* es la contraseña en texto normal.
   - *SALT* es una serie aleatoria que se utiliza para generar una contraseña. Se encuentra en la columna `SALT` de la tabla de base de datos `USERREG` para el usuario en concreto cuya contraseña se está actualizando.
   - *clave_comerciante* es la clave de comerciante que se ha entrado durante la creación de instancia.

400 Para iSeries, para cambiar la contraseña cifrada para los compradores, utilice el mandato `chgwcspwd.sh`.

1. Inicie una sesión QShell en el sistema iSeries.
2. Vaya al directorio siguiente: *`dir_instalación_WC`*`/bin`
3. Ejecute el script siguiente desde una línea de mandatos: `chgwcspwd.sh` (Se mostrarán los parámetros de uso.)
4. Vuelva a ejecutar el mandato utilizando los parámetros adecuados.

Para obtener información detallada acerca de cómo ejecutar este mandato, consulte la Ayuda en línea a la producción y el desarrollo de WebSphere Commerce.

Generación de contraseñas cifradas de WebSphere Commerce Payments

WebSphere Commerce le permite generar contraseñas cifradas para WebSphere Commerce Payments. Para generar contraseñas cifradas, realice lo siguiente:

1. Vaya al subdirectorio `bin` bajo el directorio de instalación de WebSphere Commerce.
2. Ejecute el script siguiente desde una línea de mandatos:

   Windows `wcs_pmpassword.bat` *`contraseña SALT`*

   AIX 400 Linux Solaris `./wcs_pmpassword.sh` *`contraseña SALT`*

   donde:

   - *contraseña* es la contraseña en texto normal.

- *SALT* es una serie aleatoria que se utiliza para generar una contraseña. Se encuentra en la columna SALT de la tabla de base de datos USERREG para el usuario en concreto cuya contraseña se está actualizando.

Restauración de una cuenta de administrador

Si por algún motivo se bloquea o inhabilita una cuenta de WebSphere Commerce, puede desbloquearla o habilitarla del modo siguiente:

Si la cuenta *no es* una cuenta de administrador de sitio:

1. Abra la Consola de administración.
2. Pulse **Gestión de acceso** > **Usuarios**.
3. Pulse dos veces la cuenta de usuario o seleccione la cuenta de usuario en la lista y pulse **Cambiar**.
4. Seleccione **Habilitar** en el campo de estado de la cuenta.
5. Pulse **Aceptar**.

Si la cuenta *es* una cuenta de administrador de sitio o cualquier otra cuenta de usuario, ejecute las sentencias SQL siguientes desde una ventana de mandatos de DB2 o desde un indicador SQLPlus (para bases de datos Oracle):

```
CONNECT TO nombre_bd [USER id_usuario USING contraseña]
UPDATE USERREG SET STATUS=1, PASSWORDRETRIES=0 WHERE LOGONID='ID_conexión'
```

donde

nombre_bd
: Es el nombre de la base de datos de WebSphere Commerce (por ejemplo, MALL).

id_usuario
: Es el ID de usuario de administrador de la base de datos.

contraseña
: Es la contraseña que corresponde al ID de usuario de administrador de la base de datos.

ID_conexión
: Es el ID de usuario de la cuenta que desea restaurar (por ejemplo, wcsadmin).

Por ejemplo, para restaurar la cuenta wcsadmin, puede emitir las siguientes sentencias SQL si está conectado al sistema con el ID de usuario de administrador de base de datos:

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

400 Para escribir sentencias SQL en la plataforma iSeries, puede utilizar el gestor de consultas de DB2/400 y el kit de desarrollo SQL o puede utilizar iSeries Navigator. Para utilizar IBM iSeries Access para realizar consultas de base de datos, efectúe lo siguiente:

1. Inicie iSeries Navigator desde el PC donde está instalado.
2. Expanda el sistema iSeries. Expanda Bases de datos, pulse con el botón derecho del ratón en Base de datos relacional y seleccione **Ejecutar scripts SQL**. Se abre la ventana Ejecutar scripts SQL.
3. En el menú Conexión, seleccione **Configuración de JDBC**. Pulse la pestaña **Servidor**.

4. En el campo de bibliotecas por omisión, borre los valores existentes y escriba el nombre del esquema de base de datos de la instancia. Por omisión, el nombre de esquema es el nombre de la instancia. Pulse **Aceptar** para guardar los cambios.
5. Escriba las anteriores sentencias SQL en la ventana.

Capítulo 7. ID de conexión único

Este capítulo describe cómo configurar el ID de conexión único para WebSphere Commerce.

Prerrequisitos

Para habilitar el ID de conexión único, se deberán satisfacer los requisitos siguientes:

- Tiene que estar instalado y configurado un servidor LDAP existente. Para configurar un servidor LDAP, consulte la publicación *WebSphere Commerce, Guía de software adicional*.
- WebSphere Commerce tiene que estar instalado y configurado para utilizar LDAP.
- La seguridad de WebSphere Application Server tiene que estar habilitada. Para habilitar la seguridad de WebSphere Application Server, consulte el Capítulo 16, "Habilitación de la seguridad de WebSphere Application Server", en la página 189.

Habilitación del ID de conexión único

Atención

Existen varias limitaciones clave del ID de conexión único cuando éste se utiliza con WebSphere Commerce. Estas limitaciones son:

- Los cookies LTPA pueden fluir a través de puertos de servidor web diferentes.
- Puede que necesite modificar el archivo `ldapentry.xml` y añadir la clase de objeto `ePerson`. Se trata de un atributo del elemento `ldapocs`.
- Ha de modificar `instance.xml` y asegurarse de que el distintivo `MigrateUsersFromWCSdb` se haya establecido en `"ON"`.
- Las máquinas que participan en la configuración de ID de conexión único deben tener sincronizados los relojes del sistema.
- El ID de conexión único sólo se soporta entre aplicaciones que pueden leer y emitir la señal LTPA (Light Weight Third Party Authentication) de WebSphere Application Server.

Para habilitar el ID de conexión único, deberá realizar lo siguiente:

1. Habilite el ID de conexión único en WebSphere Application Server. Para obtener más información, busque informació sobre el ID de conexión único en el Centro de información de WebSphere Application Server (`http://www.ibm.com/software/webservers/appserv/infocenter.html`). Seleccione **SSO (Single Sign-On): WebSphere Application Server** y complete las secciones siguientes:
   - **Configuración de SSO para WebSphere Application Server**.
     - **Modificación de los valores de seguridad de WebSphere Application Server**.

Nota: El paso que describe detalladamente cómo rellenar los campos de LDAP puede ignorarse sin ningún riesgo.

- **Exporte las claves LTPA a un archivo**.

2. En la máquina de WebSphere Commerce, inicie el Gestor de configuración de WebSphere Commerce.
3. Para configurar el nodo **Subsistema de miembros**, realice lo siguiente:
   a. En **WebSphere Commerce** expanda *nombre_sistema_principal* → **Lista de instancias** → *nombre_instancia* → **Propiedades de instancia** → **Subsistema de miembros**.
   b. En el menú desplegable **Modalidad de autenticación**, seleccione **LDAP**.
   c. Habilite el recuadro de selección **ID de conexión único**.
   d. En el campo **Sistema principal**, entre el nombre de sistema principal totalmente calificado del servidor LDAP.
   e. Entre el nombre distinguido del administrador en el campo **Nombre distinguido del administrador**. Este deberá ser el mismo nombre que se ha utilizado en el servidor LDAP.
   f. En el campo **Contraseña del administrador**, entre la contraseña del administrador. Esta deberá ser la misma contraseña que se ha utilizado en el servidor LDAP. Confirme la contraseña en el campo **Confirmar contraseña**.
   g. Rellene cada uno de los campos restantes.
   h. Pulse **Aplicar** y, a continuación, pulse **Aceptar**.
4. Configure los roles que se asignarán a los usuarios que entran al sistema con el ID de conexión único (SSO). Cada vez que un usuario se conecta al sistema mediante SSO,WebSphere Commerce intentará asignar los roles desde el archivo `MemberRegistrationAttributes.xml` cuyo tipo de registro sea igual a SSO. Enlace con la sección nueva que describe MRA.xml.
5. Reinicie WebSphere Application Server.

Configuración de roles para usuarios de SSO

En WebSphere Commerce 5.5, los roles de seguridad se asignan como parte del proceso de registro. Con el ID de conexión único, el cliente puede ignorar el paso de registro en el sitio si ya se ha autenticado correctamente con un sistema colaborativo. La posibilidad de poderse autenticar de modo implícito en un sitio de WebSphere Commerce 5.5 tiene poco valor si al usuario se le acaba denegando el acceso a los recursos que desea utilizar, por ejemplo, si no puede comprar en una tienda.

Por lo tanto, las mismas funciones que se llevan a cabo en la asignación automática de roles se producen durante el registro de usuarios en el código de gestión de sesiones. En este caso, debe configurar los roles para los compradores SSO utilizando el tipo de registro SSO. De este modo, cuando un cliente se autentica en el sistema, WebSphere Commerce 5.5 proporcionará automáticamente todos los roles que debe tener en el sitio. Recuerde que la asignación de roles SSO ocurre a nivel de sitio y no a nivel de tienda (como sucede en el registro de usuarios típico). Por lo tanto, debe asegurarse de que se el atributo storeAncestor especificado sea realmente una predecesora del sitio (tienda 0).

Ejemplo:

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

En este ejemplo se proporcionarán cuatro roles a cualquier comprador que entre en el sistema con SSO.

Capítulo 8. Administración de certificados X.509

WebSphere Commerce da soporte a la conexión con certificados de cliente como mecanismo de seguridad para proteger el sitio y a los clientes. El certificado X.509 aumenta la autenticación básica para los clientes que entran en un sitio. Un cliente con este tipo de certificado puede acceder a un sitio de WebSphere Commerce seguro que se haya habilitado para la autenticación de certificados de cliente.

Cuando crea una instancia de WebSphere Commerce, selecciona la modalidad de autenticación. La modalidad de autenticación puede ser básica o X.509. El valor por omisión es la autenticación básica, lo que significa que durante la conexión la autenticación se realiza mediante un ID de conexión y una contraseña. Para activar la autenticación de conexión mediante certificados X.509, seleccione la autenticación X.509.

Antes de comenzar a utilizar certificados X.509, debe establecer una relación de confianza con una autoridad de certificación externa para manejar la autenticación electrónica de los certificados X.509. Si está utilizando Netscape Enterprise como servidor Web, deberá realizar los siguientes pasos adicionales para habilitar los certificados X.509 en el servidor Web. Consulte la documentación de Netscape Enterprise Server para obtener más información y las instrucciones completas.

Se puede acceder a los usuarios de X.509 mediante WebSphere Commerce Accelerator. Antes de habilitar la autenticación de certificados X.509, el administrador debe asegurarse de que existe un certificado de cliente que esté reconocido por el certificado de servidor y que esté instalado en el navegador. De lo contrario, el administrador no podrá conectarse. Cuando el administrador accede por primera vez a la ventana de conexión de la consola de administración de WebSphere Commerce, se crea un registro de comprador certificado y un cookie de comprador, de modo similar a cuando un comprador accede a un URI protegido. Cuando el administrador se conecta a la consola de administración de WebSphere Commerce utilizando el ID y la contraseña correctos, se emite un cookie de administrador que sustituye el cookie del comprador. De este modo, el administrador tendrá dos registros de usuario: el usuario administrador y el usuario comprador anterior.

Se muestra un mensaje de error cuando:

- Un sitio revoca un certificado X.509 de usuario.
- Un certificado de cliente no contiene la información necesaria para garantizar que el comprador es exclusivo en WebSphere Commerce.

La tarea de vista de error X.509 se ha registrado como `X509 ErrorView` en la tabla de base de datos `VIEWREG`.

Habilitación de certificados X.509

Cuando se crea una instancia de WebSphere Commerce, se selecciona la autenticación básica o la autenticación X.509 utilizando el gestor de configuración. El valor por omisión es la autenticación básica, lo que significa que la autenticación se realiza utilizando un ID de conexión y una contraseña.

Para habilitar la autenticación utilizando certificados X.509, efectúe lo siguiente:

1. Configure el certificado SSL del servidor Web IBM HTTP Server. El certificado del servidor SSL incluye una lista de autoridades de certificación de cliente para relaciones de confianza. Es posible que necesite añadir autoridades de certificación de cliente adicionales.
2. Inicie el Gestor de configuración de WebSphere Commerce.
3. Seleccione **Propiedades de la instancia -> servidor Web**.
4. Marque el recuadro **X.509** en Modalidad de autenticación. Pulse **Aplicar**. Ahora se aceptarán usuarios de certificados de cliente X.509. IBM HTTP se habilita automáticamente para el soporte de certificados cuando se selecciona la modalidad de autenticación X.509.
5. Inicie el detenga el servidor de WebSphere Commerce. WebSphere Commerce no registrará a los usuarios de X.509 de la tabla `CERT_X509` hasta que se haya reiniciado.

Nota: Puede configurar IBM HTTP Server para que los certificados X.509 sean opcionales o necesarios.

1. Abra el archivo de configuración `httpd.conf` y localice la directiva `SSLClientAuth`. Establezca la directiva en 1 (opcional) o en 2 (necesaria). El parámetro recomendado es *necesario*.
2. Dado que el cliente de WebSphere Commerce Payments no da soporte a la autenticación de cliente SSL, debe inhabilitar SSL entre el cliente de WebSphere Commerce Payments y el servidor Web.
   a. En un editor de texto, abra el archivo `PaymentServlet.properties`. El archivo está en el directorio de instalación de WebSphere Commerce Payments.
      - Localice la propiedad `UseNonSSLWCSClient`. Establezca la propiedad en el valor 1 (uno).
      - Si no puede encontrar la propiedad `UseNonSSLWCSClient` en el archivo, añada la línea:

        ```
        UseNonSSLWCSClient=1
        ```

   b. Guarde el archivo y salga del editor.
3. Si se ha instalado WebSphere Commerce Payments en la misma máquina que WebSphere Commerce:
   a. Inicie el Gestor de configuración.
   b. Seleccione la instancia y luego seleccione **Payments**.
   c. Marque **Utilizar cliente de WebSphere Commerce Payments no SSL**. Esto habilita las comunicaciones entre el cliente WebSphere Commerce Server y WebSphere Commerce Payments sin utilizar SSL.
   d. Pulse **Aplicar**.
   e. Cierre el Gestor de configuración.
4. Reinicie el servidor de aplicaciones WebSphere Commerce Payments desde la consola r de administración de WebSphere.
5. Reinicie el servidor de aplicaciones WebSphere Commerce desde la consola de administración de WebSphere.

Consulte la documentación de IBM HTTP Server para obtener más información y las opciones adicionales sobre cómo establecer los parámetros de restricciones y filtrado para certificados.

Actualización del estado de los usuarios de certificados X.509

Con WebSphere Commerce Accelerator, un administrador de sitio puede actualizar el estado de un usuario de certificado X.509, en un de los tres valores de estado siguientes:

Válido
El usuario puede acceder a un sitio de WebSphere Commerce con el certificado.

Revocado
El usuario no puede acceder al sitio de WebSphere Commerce. Cuando un usuario con un certificado revocado intenta conectarse, recibirá una página de error de certificado X.509.

Caducado
El usuario no puede acceder al sitio de WebSphere Commerce. Cuando un usuario con un certificado caducado intenta conectarse, recibirá una página de error de certificado X.509.

Cuando administre certificados X.509, es posible que desee establecer parámetros de restricciones y filtros para los titulares de certificados. Por ejemplo, es posible que desee también permitir que determinados tipos de titulares de certificados puedan acceder a su sitio protegido modificando el archivo de configuración `httpd.conf`.

Para obtener más información sobre instrucciones, consulte la documentación del servidor Web.

Escenario de autenticación típico

Los pasos siguientes ilustran un escenario de autenticación típico para los certificados X.509:

1. Un comprador accede a:
   - Un URL no protegido mediante `http://`
     No se realiza ninguna tarea de autenticación.
   - Un URL protegido mediante `https://`
     Se le solicita al comprador que seleccione un certificado de cliente.
   - Un mandato URL y se le redirige a `https://` debido a la modalidad de acceso del mandato URL.
     Se le solicita al comprador que seleccione un certificado de cliente.
2. WebSphere Commerce Server utiliza la información del certificado de cliente para ver si el comprador ya existe en la tabla `SHOPPER` de WebSphere Commerce.
   - Si el comprador existe y su estado de certificado es válido, se autentica al comprador y se reanuda el flujo de compra.
   - Si el comprador no existe:
     – Se registra automáticamente el comprador en la base de datos de WebSphere Commerce y se reanuda el flujo de compras.

Nota: Del certificado solamente se extrae la información de la tabla `CERT_X509`. No obstante, la información sobre la dirección del cliente se puede extraer del certificado de cliente X.509, si está disponible.

Parte 3. Administración de la autorización de seguridad

Esta parte describe las tareas de autorización de seguridad que normalmente realiza el administrador de sitio de WebSphere Commerce.

Capítulo 9. Introducción al control de acceso

El comercio electrónico no solamente ha cambiado el modo en que las empresas trabajan sino que ha aumentado de forma importante los tipos de relaciones que esperan tener con sus clientes y business partners. La Web es un factor clave para que su oferta tenga más valor para los clientes que ya posee y para preparar el terreno para nuevos clientes dispuestos a beneficiarse de la potencia y la creciente eficacia de Internet. A las ventajas claras que supone tener un negocio en la Web y al enorme potencial que supone para aumentar su base de clientes, se une el desafío de gestionar los flujos de negocio y los socios comerciales, mantener un entorno de alta seguridad, autorizar las transacciones adecuadas y mantener los procesos de trabajo de forma transparente.

La importancia del control de acceso es que permite prever estos procesos de trabajo gestionando el modo en que participarán los usuarios en el sistema, según sus actividades, y las relaciones comerciales que mantendrán con sus productos y servicios. Por ejemplo, es posible que desee que sólo los clientes que se hayan registrado en su sitio puedan ver los productos que están en subasta en la tienda y puedan realizar ofertas para las mismas. Del mismo modo, puede autorizar a los diseñadores gráficos para que personalicen las páginas de su tienda, pero puede impedir que gestionen el contenido real del catálogo de productos.

WebSphere Commerce le proporciona las herramientas adecuadas para la gestión de acceso, incluidas más de doscientas políticas de control de acceso por omisión que se cargan automáticamente en el sistema durante la instalación. Estas políticas se han diseñado para cubrir muchos de los requisitos típicos de control de acceso que necesita su negocio y pueden personalizarse para adaptarlos a su solución de comercio electrónico.

Gestionar el acceso a las actividades del mercado electrónico es una parte integral de la protección de los elementos financieros y de los recursos de la empresa, que permite proteger las transacciones de negocio entre los miembros autorizados de su sitio y validar la legitimidad de sus operaciones en línea. El control de acceso resulta especialmente crucial en el contexto de comercio electrónico, en el que la entrada a su negocio resulta ampliamente afectada por las relaciones que se inician a través de la Web.

Qué significa el control de acceso para su negocio

El control de acceso le permite gestionar los flujos de trabajo de su negocio y le asegura que los usuarios solamente realizarán las actividades adecuadas a sus roles y responsabilidades. WebSphere Commerce no sólo le proporciona políticas por omisión que puede utilizar directamente sino que también le proporciona las herramientas y la posibilidad de personalizar estas políticas según las necesidades de su negocio.

La tabla siguiente describe algunos ejemplos de sencillas modificaciones que pueden personalizar el acceso a su entorno de negocio.

Tareas que pueden realizar los usuarios por omisión	Tareas que pueden realizar los usuarios después de la personalización
Los clientes se pueden registrar.	Solamente los administradores de vendedores pueden registrar a clientes nuevos.
Los compradores pueden visualizar las RFQ que han solicitado.	Solamente los vendedores pueden visualizar las RFQ si la RFQ es el resultado de un contrato.
Sólo los clientes pueden cancelar pedidos que han creado si el pedido está en estado pendiente.	Los representantes de servicio al cliente también pueden cancelar pedidos en estado pendiente, si el precio total del producto es inferior a 1000 euros.
La persona que ha creado un pedido puede modificarlo.	Solamente un usuario de la organización compradora cuyo rol sea el de `comprador` puede modificar un pedido creado.
Los representantes de cuentas pueden visualizar todas las cuentas.	Los representantes de cuentas solamente pueden visualizar las cuentas activas.
Los empleados con el rol de gestor de logística pueden crear y modificar los centros de formalización de pedidos.	Los empleados con el rol de gestor de logística pueden crear pero no modificar los centros de formalización de pedidos.

En el capítulo siguiente, se describirá detalladamente una política de control de acceso y cómo se pueden crear organizaciones y usuarios.

Capítulo 10. Iniciación

En el capítulo anterior se ha descrito el importante rol que juega el control de acceso en comercio electrónico y las ventajas clave que ofrece para mejorar la eficacia y fiabilidad a los negocios en la Web.

En este capítulo, se describen los conceptos básicos de la gestión de acceso en WebSphere Commerce como, por ejemplo, cómo definir organizaciones y usuarios, y cómo acceder a las políticas que se utilizan para gestionar las actividades que estas organizaciones y sus usuarios realizan en el sistema. Después de describir brevemente los pasos necesarios para definir las organizaciones y los usuarios, describiremos detalladamente las políticas de control de acceso, su rol en WebSphere Commerce y analizaremos una política de control de acceso detenidamente.

Este capítulo está dividido en las secciones siguientes:

- Definición de organizaciones y usuarios
- Descripción del control de acceso
- Iniciación al control de acceso

Definición de organizaciones y usuarios

Para los administradores de sitio, una de las primeras tareas después de instalar y configurar WebSphere Commerce es definir y gestionar el acceso al sitio de comercio electrónico. Esto requiere crear las organizaciones que participarán en el sitio y también definir a los usuarios que serán miembros de dichas organizaciones. En WebSphere Commerce 5.5, se han introducido modelos de negocio. Una vez creada una instancia, los administradores pueden publicar los modelos de negocio de ejemplo existentes que establecerán la estructura de la organización. Para obtener más información sobre los modelos de negocio, consulte el apartado “Modelos de negocio” en la página 19.

En algunos casos, las organizaciones que se registrarán en su sitio pueden ser organizaciones compradoras o es posible que en su sitio se registren clientes que tengan con su negocio una relación de tipo empresa a consumidor. Independientemente de si está administrando un sitio de empresa a empresa o de empresa a consumidor, definir la estructura organizativa del sitio es un paso importante para gestionar los tipos de acceso al sistema que tienen los miembros.

En este apartado, describiremos los pasos generales que deberá realizar para definir la estructura del sitio. Si está utilizando los modelos de negocio de ejemplo que se proporcionan, puede pasar a la sección siguiente sobre control de acceso. Si desea definir su propia estructura de organización, continúe con los pasos siguientes.

Para obtener información detallada sobre cómo crear organizaciones, usuarios y roles, consulte la ayuda en línea que está disponible en la página de la biblioteca técnica:

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

Asimismo, le recomendamos que consulte la publicación *WebSphere Commerce, Conceptos básicos*. Para obtener una visión general de los modelos de negocio, consulte las publicaciones *WebSphere Commerce, Guía del desarrollador de tiendas* y *WebSphere Commerce, Guía de tiendas de ejemplo* respectivamente.

Definición de una organización vendedora

Generalmente, la organización vendedora es la organización que posee una o más tiendas en un sitio de WebSphere Commerce. La organización vendedora también puede tener suborganizaciones o divisiones, que a su vez pueden tener una o varias tiendas. Por ejemplo, la tienda de ejemplo InFashion, que vende artículos de moda, puede tener un departamento de señoras y un departamento de caballeros y cada uno de ellos puede ser una tienda en línea diferente.

De momento, supongamos que está estableciendo una organización vendedora que no dispone de ninguna suborganización. A continuación, se muestra una descripción general de lo que debe hacer para establecer una organización vendedora:

1. Cree una organización nueva. Cuando cree una organización nueva, creará un perfil para dicha organización, que incluirá el nombre de la organización, la descripción, la dirección y la persona de contacto, junto con el tipo de organización.
2. (Opcional) Defina las tareas que requerirán aprobación dentro de la organización vendedora como, por ejemplo, el proceso de pedidos o el registro de usuarios. Este paso solamente es necesario para un sitio de empresa a empresa. Consulte la ayuda en línea del producto para obtener información sobre las aprobaciones.
3. Asigne roles a la nueva organización. Una organización solamente puede tener los roles que se han asignado a su organización padre. Dado que la organización raíz es un antecesor de todas las demás organizaciones, se le deben asignar todos los roles posibles. WebSphere Commerce proporciona un conjunto de roles por omisión que puede comenzar a utilizar inmediatamente. Dado que está creando una organización vendedora, los roles típicos que puede asignar son el de administrador de vendedores, vendedor, etc. Consulte el apartado “Roles” en la página 32 para obtener una lista de los roles por omisión.
4. Cree usuarios. Al igual que las organizaciones, creará un perfil para cada usuario que incluya el nombre de usuario, la información de contacto y el rol que se ha asignado a dicho usuario. Cuando asigne roles, los seleccionará de la lista de roles que ha asignado a la organización en el paso anterior.
5. Asigne grupos de políticas a la organización nueva, de modo que los clientes puedan comprar en la tienda gestionada por la organización. Los grupos de políticas típicos necesarios son: grupo de políticas de gestión y administración, grupo de políticas de compra comunes, grupo de políticas B2C y grupo de políticas B2B. Para obtener más información sobre los grupos de políticas, consulte el apartado “Políticas y grupos de control de acceso por omisión”, en la página 217.

Todos los pasos que se han descrito anteriormente los realiza el administrador de sitio desde el menú Gestión de acceso de la Consola de administración de organizaciones.

Nota: En WebSphere Commerce Professional Edition, no puede crear ninguna organización. Ya se habrá creado una organización vendedora para usted.

Definición de una organización compradora

Si va a ejecutar un sitio de empresa a empresa, puede haber más de una organización compradora que pertenezca al sitio. Por el contrario, si va a ejecutar un sitio de empresa a consumidor, se registrarán compradores individuales en la organización por omisión. Cuando haya establecido qué empresas participarán en una relación de compras con su sitio, tendrá que crear una organización compradora para cada empresa. Puede tener tantas organizaciones compradoras como necesite.

Las organizaciones compradoras tienen una estructura similar a la de las organizaciones vendedoras. Al igual que las organizaciones vendedoras, las organizaciones compradoras pueden tener suborganizaciones o divisiones, que representen las diferentes actividades de compra de la organización.

De momento, supongamos que las organizaciones compradoras no tienen ninguna suborganización. Para establecer una organización compradora, deberá realizar lo siguiente:

1. Tal y como ha hecho cuando ha creado una organización vendedora, cree una nueva organización y defina las tareas que se han de aprobar, si es necesario. Una vez más, sólo es necesario que defina las tareas que se han de aprobar para los sitios de empresa a empresa.
2. Asigne roles a la nueva organización compradora. Dado que está creando una organización compradora, los roles típicos que puede asignar son el de administrador de compradores, comprador (parte compradora), aprobador de compradores, etc.
3. Cree usuarios y asígneles roles. Cuando asigne roles, los seleccionará de la lista de roles que ha asignado a la organización compradora en el paso anterior.
4. Repita el procedimiento completo para cada organización compradora que desee añadir al sitio.

Nota: En circunstancias normales, no es necesario que las organizaciones compradores se suscriban a ningún grupo de políticas, ya que heredarán los grupos de políticas a los que se suscribe la organización raíz.

Una vez más, todos los pasos que se han descrito anteriormente se realizan desde el menú Gestión de acceso de la Consola de administración de organizaciones.

Nota: En WebSphere Commerce Professional Edition, todos los clientes pertenecen a la organización por omisión.

¿Qué es el control de acceso?

Cuando haya terminado de definir las organizaciones y los usuarios que participarán en su sitio de comercio electrónico, podrá gestionar sus actividades mediante un conjunto de políticas; este proceso se denomina *control de acceso*. En el apartado siguiente, analizaremos las políticas de control de acceso y su estructura básica.

¿Qué es una política de control de acceso?

Una política de control de acceso es una norma que describe qué grupo de usuarios tiene autorización para realizar determinadas actividades en el sitio. Estas

actividades pueden incluir acciones que van desde el registro y la gestión de subastas hasta la actualización del catálogo de productos y la concesión de aprobaciones en los pedidos, así como cualquiera de los cientos de actividades diferentes que son necesarias para operar y mantener un sitio de comercio electrónico.

Las políticas son las que permiten a los usuarios acceder a su sitio. A menos que se les haya autorizado a llevar a cabo sus responsabilidades, mediante una o varias políticas de control de acceso, los usuarios no pueden acceder a ninguna de las funciones del sitio.

¿Cómo funciona una política de control de acceso?

Las políticas de control de acceso constan de cuatro partes; un grupo de acceso, un grupo de acciones, un grupo de recursos y una relación opcional.

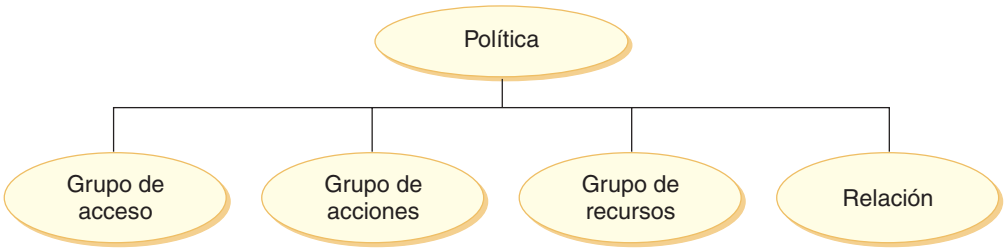
Un *grupo de acceso* es un grupo de usuarios que comparten un acceso común a un conjunto de funciones del sitio. Un grupo de acceso incluye generalmente a los usuarios que comparten atributos comunes como, por ejemplo, el mismo rol, el mismo departamento o el mismo tipo de especialización.

Un *grupo de acciones* es el conjunto de acciones que pueden realizarse en el mismo recurso. En general, los grupos de acciones incluyen las acciones asociadas a un área común de negocio o a un conjunto relacionado de actividades del sitio.

Un *grupo de recursos* incluye los recursos que se controlan mediante la política. Un grupo de recursos puede incluir objetos de negocio como, por ejemplo, un contrato o un conjunto de mandatos relacionados.

En algunos casos, solamente un usuario que tenga una *relación* con un recurso podrá realizar acciones en el mismo. Por ejemplo, solamente aquellos usuarios que creen un contrato podrán modificarlo.

Figura 4. Los cuatro componentes de una política de control de acceso



Estos cuatro componentes juntos definen una política en WebSphere Commerce ya que especifican los usuarios, las acciones que puede realizar, el objeto de negocio o un conjunto de mandatos en los que pueden llevarse a cabo acciones y, opcionalmente, la relación que los usuarios tienen con el grupo de recursos.

Para obtener información detallada acerca de los grupos de acceso, los grupos de acciones, los grupos de recursos y las relaciones, consulte el Capítulo 3, “Conceptos relacionados con la autorización”, en la página 19.

¿Cómo puede comenzar a utilizar el control de acceso?

En algunos casos, no es necesario que haga nada. La introducción de los modelos de negocio también ayuda a proporcionar la estructura de control de acceso básica de un sistema, ya que las políticas por omisión de WebSphere Commerce se han diseñado para proporcionar una estructura básica de control de acceso basada en los usuarios típicos de su sistema y en las actividades que realizan que están asociadas a sus roles dentro de una organización. Las políticas cubren una amplia gama de actividades comunes de negocio, incluidos el registro de miembros, la creación y el proceso de pedidos, la aprobación de flujos de trabajo y el comercio como, por ejemplo, las subastas, la solicitud de presupuesto y los contratos. Una vez definidos las organizaciones y los usuarios, se pueden utilizar las políticas por omisión tal y como se proporcionan o se pueden personalizar según las necesidades individuales de su empresa.

Sin embargo, para poder decidir si desea utilizar las políticas por omisión, o si prefiere personalizarlas, es importante que comprenda cómo se han diseñado en WebSphere Commerce. Si desea obtener una descripción detallada de una política por omisión, consulte el apartado “Análisis detallado de una política” en la página 45.

Capítulo 11. Personalización de las políticas de control de acceso por omisión

Las políticas de control de acceso que proporciona WebSphere Commerce cubren los requisitos básicos que tienen las organizaciones a la hora de regular las acciones y la información que ponen a disposición de los usuarios. Generalmente, las políticas por omisión suelen ser suficientes para las necesidades del sitio. Al mismo tiempo, las políticas por omisión se pueden personalizar fácilmente, lo que le permite adaptarlas a sus propios requisitos.

La política `SiteAdministratorsCanDoEverything` es una política especial por omisión que otorga acceso de superusuario a los administradores que tienen el rol de administrador de sitio. En esta política, un administrador de sitio puede realizar cualquier acción en cualquier recurso, incluso si estas acciones o recursos no se han definido. Es importante recordarlo cuando se asigna este rol a los usuarios.

Este capítulo proporciona información acerca de cómo realizar cambios básicos en las políticas de control de acceso por omisión que se incluyen con WebSphere Commerce. Comenzaremos introduciendo determinados conceptos y relaciones que necesita comprender.

Nota: Si encuentra algún término o concepto con el que no está familiarizado, consulte el Capítulo 3, "Conceptos relacionados con la autorización", en la página 19 para obtener más información.

Identificación de las políticas afectadas por un cambio

En el Capítulo 3, "Conceptos relacionados con la autorización", en la página 19, se ha explicado que las políticas suelen estar relacionadas con otras políticas. También se ha descrito cómo comenzar por una política a nivel de recursos e identificar las políticas basadas en roles asociadas a la misma. En este capítulo describiremos detalladamente cómo las políticas se relacionan entre sí y por qué es necesario conocer sus relaciones antes de modificar una política existente o de crear una nueva. En muchos casos, deberá cambiar varias políticas para poder implementar un cambio.

Descripción de la relación entre las políticas basadas en roles y las políticas a nivel de recursos

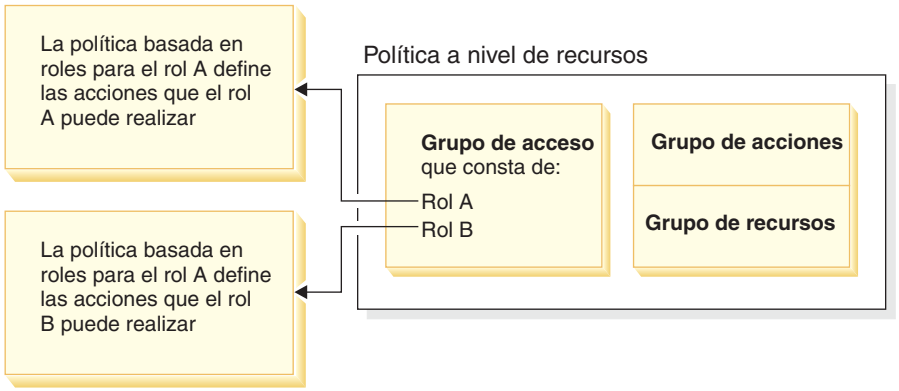
En WebSphere Commerce, cada acción que puede llevar a cabo un usuario se asigna a uno o varios roles mediante las políticas basadas en roles, como se describe a continuación:

- Cada rol por omisión tiene un grupo de acceso correspondiente. Por ejemplo, el grupo de acceso para el rol de vendedor es `Vendedores`.
- Generalmente, cada grupo de acceso basado en rol tiene asociadas dos políticas basadas en roles:
  - Una política que define los mandatos de controlador que puede ejecutar el rol.
  - Una política que define las acciones de vista que puede ejecutar el rol. Las acciones de vista se correlacionan con las vistas de la tabla `VIEWREG`. Por ejemplo,`OperationalReportsHomeRHSView` muestra una página Web con la lista de informes operativos a los que tiene acceso el vendedor.

Algunos mandatos de controlador solamente tienen una política basada en roles pero ninguna política a nivel de recursos. Esto es así si el mandato no funciona en ningún recurso protegible. Por ejemplo, el mandato `SetCurrencyPreferenceCmd` no necesita una política a nivel de recursos ya que solamente puede modificar la preferencia de moneda del usuario que ejecuta el mandato. Si pudiera modificar la preferencia de moneda de otro usuario, entonces el objeto de usuario tendría que estar protegido y se necesitaría una política a nivel de recursos.

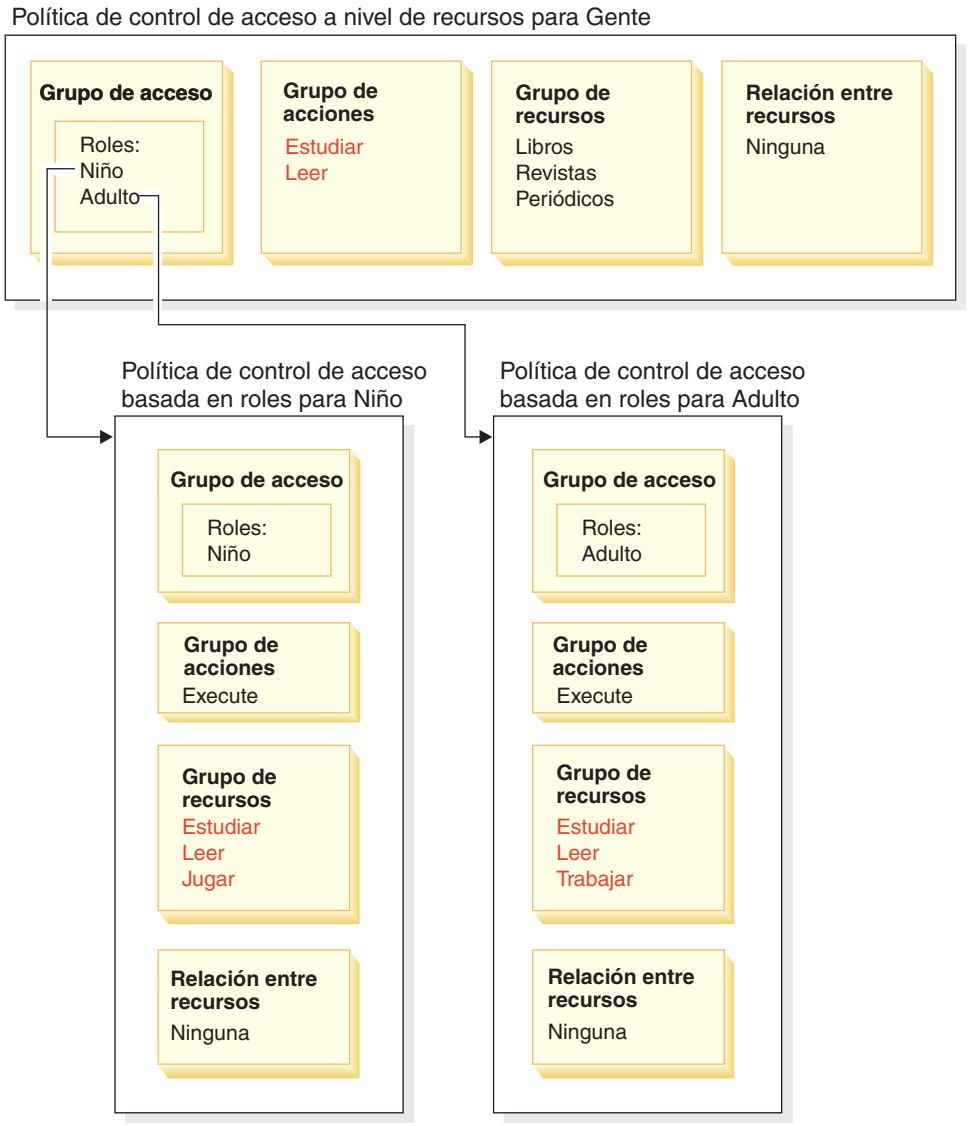
Las políticas a nivel de recursos para mandatos de controlador están relacionadas directamente con determinadas políticas basadas en roles para mandatos de controlador. En la política a nivel de recursos, el mandato del controlador forma parte del grupo de acciones pero en la política basada en roles, el mandato de controlador forma parte del grupo de recursos. La figura siguiente ilustra esta relación. La política a nivel de recursos incluye los roles A y B en su grupo de acceso, el cual hace que se activen las políticas basadas en roles para los roles A y B. Mientras que la política a nivel de recursos autoriza a los usuarios que poseen los roles A o B a realizar determinadas acciones en un conjunto de recursos específicos, las políticas basadas en roles asociadas autorizan a los usuarios que poseen los roles A y B a realizar dichas acciones en general.

Figura 5. Relación entre una política a nivel de recursos y las políticas basadas en roles asociadas



La figura siguiente muestra una política a nivel de recursos de ejemplo que autoriza a los usuarios del grupo de acceso `Gente` a leer o estudiar determinados recursos, principalmente, libros, revistas y periódicos. Esta política se ha formulado correctamente ya que las políticas basadas en roles de los roles `niño` y `adulto` también les autorizan a leer o estudiar libros, revistas y periódicos.

Figura 6. Una política a nivel de recursos y las políticas basadas en roles que le afectan.



Tenga en cuenta que en las políticas basadas en roles para mandatos de controlador:

- El grupo de acciones contiene solamente una acción: `Execute`.
- El grupo de recursos contiene los mandatos de controlador que se pueden ejecutar.

Del mismo modo, en las políticas basadas en roles para vistas:

- El grupo de acciones contiene solamente las vistas que se pueden ejecutar.
- El grupo de recursos contiene solamente un recurso: `com.ibm.commerce.command.ViewCommand`.

Por otro lado, en las políticas a nivel de recursos:

- El grupo de acciones contiene el conjunto de acciones que se puede realizar en los recursos del grupo de recursos.

- El grupo de recursos contiene una lista de los recursos de negocio reales en los que pueden realizarse acciones.

Una política a nivel de recursos solamente puede autorizar a los usuarios que tienen un rol determinado a realizar acciones que ya ha autorizado la política basada en roles correspondiente. Por ejemplo, en el ejemplo anterior, el rol de `niño` tiene autorización para realizar las acciones siguientes:

- Estudiar
- Leer
- Jugar

Suponga que ahora se modifica la política a nivel de recursos para que incluya una acción nueva llamada `trabajar`. Los usuarios que tienen el rol de `adulto` podrán realizar la acción `trabajar`. Sin embargo, los usuarios que tienen el rol de `niño` no podrán hacerlo. El motivo resulta aparente cuando comprueba las políticas basadas en roles de estos dos roles. La política del `adulto` lista la acción `trabajar` en su grupo de recursos. La política del `niño` no. Incluso si tanto el `niño` como el `adulto` tienen la autorización correcta de la política a nivel de recursos, la política basada en roles para el `niño` no le autoriza a realizar la acción `trabajar`.

Debido al modo en que las políticas a nivel de recursos están vinculadas con las políticas basadas en roles, el mejor modo de realizar un seguimiento de todas las políticas afectadas por un cambio determinado es retroceder a partir de la política a nivel de recursos. El primer paso es analizar el grupo de acceso de la política a nivel de recursos y determinar si contiene algún rol. Puede ver la lista completa de roles por omisión seleccionando en la Consola de administración, Gestión de acceso > Roles.

Si el grupo de acceso de la política a nivel de recursos incluye roles, revise las políticas basadas en roles para ver si es necesario modificarlas. Si va a añadir una acción al grupo de acciones de una política a nivel de recursos, debe asegurarse de que las políticas basadas en roles relevantes también autoricen la nueva acción. Sin embargo, si va a suprimir una acción de una política a nivel de recursos y ninguna otra política a nivel de recursos hace referencia a esta acción, es mejor que suprima el recurso correspondiente.

Descripción del modelo de política

Para que un usuario pueda realizar una acción, debe haber una política que lo autorice. Sin embargo, WebSphere Commerce permite que los usuarios realicen determinadas acciones si **cualquier** política proporciona la autorización necesaria. Por lo tanto, si define una política nueva que sea más restrictiva que la política por omisión, debe suprimir o modificar la política por omisión que tiene más margen de acción para impedir que prevalezca sobre la nueva política.

Por ejemplo, suponga que la política por omisión A autoriza a todos los usuarios registrados a someter ofertas de subasta. Y desea cambiar esta política de modo que las ofertas de subasta estén limitadas a los usuarios que tienen el rol de comprador. Si simplemente define una nueva política que autorice a los compradores a crear ofertas de subasta, entonces la nueva política no tendrá efecto. La política por omisión A, continuará permitiendo a los usuarios registrados a realizar ofertas de subasta. Para que la nueva política entre en vigor, deberá suprimir la política por omisión que da más margen de acción.

La tabla siguiente resume los cambios adicionales que deberá realizar cuando cree, suprima o cambie una política a nivel de recursos.

Tabla 9. Cambios adicionales que son necesarios cuando se cambia una política a nivel de recursos que utiliza roles.

Cambiar a una política a nivel de recursos	**El cambio es necesario si el grupo de acceso a nivel de recursos utiliza roles.**
Añadir una acción al grupo de acciones de la política.	Asegurarse de que las políticas basadas en roles aplicables incluyen la acción en sus grupos de recursos.
Suprimir una acción del grupo de acciones de la política.	No es necesario realizar ningún cambio adicional. Para mayor coherencia, es mejor suprimir esta acción de los grupos de recursos correspondientes de las políticas basadas en roles. Esto solamente debe llevarse a cabo si ningún otro grupo de acciones hace referencia a esta acción. Si otros grupos de acciones hacen referencia a esta acción, probablemente hay políticas basadas en roles que todavía necesitan tener esta acción en su grupo de recursos.
Utilizar un grupo de acciones diferente.	Asegurarse de que las políticas basadas en roles aplicables incluyen en sus grupos de recursos las acciones del nuevo grupo de acciones.
Añadir un rol al grupo de acciones de la política.	Asegurarse de que la política basada en roles correspondiente al nuevo rol, hace referencia a un grupo de recursos que incluye las acciones especificadas en la política a nivel de recursos.
Suprimir un rol del grupo de acciones de la política.	No es necesario realizar ningún cambio adicional. Por coherencia, es mejor modificar la política basada en roles correspondiente de modo que ya no haga referencia a estas acciones en su grupo de recursos.
Utilizar un grupo de acceso diferente.	Asegurarse de que las políticas basadas en roles incluyen en sus grupos de recursos las acciones del grupo de acciones de la política a nivel de recursos.
Crear una política nueva.	Comprobar si existe una política que autorice las mismas acciones. Suprimirla, si es necesario.
Suprimir la política.	Impedir que los usuarios lleven a cabo las acciones de dicha política, suprimir cualquier otra política que autorice las mismas acciones.

Determinar si una política está basada en roles o es una política a nivel de recursos

Las políticas basadas en roles también se conocen como políticas a nivel de mandatos ya que autorizan a los usuarios con un rol determinado a ejecutar un conjunto de mandatos. Las políticas a nivel de recursos autorizan a un grupo de usuarios a ejecutar un conjunto de mandatos en un conjunto determinado de recursos. Por ejemplo, una política basada en roles puede dar su autorización para que los niños coman. Mientras que una política a nivel de recursos puede dar su autorización para que los niños coman arroz.

Normalmente, se puede determinar si una política está basada en roles o si se trata de una política a nivel de recursos simplemente observando su nombre.

Políticas basadas en roles

Las políticas que definen los mandatos del controlador que puede ejecutar un rol, adoptan el siguiente convenio de denominación:

<GrupoAccesoparaRolXYZ> Execute <GrupoRecursosMdtXYZ>

Por ejemplo: `ProductManagersExecuteProductManagersCmdResourceGroup`.

En las políticas basadas en roles para mandatos del controlador, el grupo de acciones contiene una sola entrada llamada `Execute` y el grupo de recursos contiene una lista de mandatos de WebSphere Commerce que los usuarios que poseen este rol pueden ejecutar.

Las políticas que definen las vistas que un rol puede ejecutar adoptan el siguiente convenio de denominación:

<GrupoAccesoparaRolXYZ> Execute <VistasXYZ>

Por ejemplo: `SalesManagersExecuteSalesManagersViews`.

El grupo de recursos contiene solamente un recurso llamado `com.ibm.commerce.command.ViewCommand`.

Políticas a nivel de recursos

Las políticas que definen quién puede realizar acciones en los recursos de datos (los objetos de negocio que se pueden crear o manipular) adoptan este convenio de denominación:

<GrupoAccesoXYZ> Execute <MandatosXYZ> On <RecursoXYZ>

Por ejemplo: `AllUsersExecuteOrderProcessOnOrderResource`.

En las políticas a nivel de recursos, el grupo de acciones contiene mandatos de WebSphere Commerce y el grupo de recursos identifica los recursos de negocio específicos en los que se pueden realizar acciones.

Una excepción son las políticas que autorizan la creación de una entidad como, por ejemplo, un pedido, una oferta de subasta o una RFQ. Estas políticas no actúan en la entidad propiamente dicha, debido a que ésta todavía no se ha creado. Sino que actúan en la entidad que las contiene. Por ejemplo, una subasta se crea dentro del contexto de una tienda y un usuario se crea dentro del contexto de una organización. La mayor parte de los recursos se crean dentro del contexto de una tienda. Por consiguiente, estas políticas tienen nombres como, por ejemplo:

<GrupoAccesoXYZs> Execute <MandatosXYZ> On <RecursoEntidadTienda>

Por ejemplo:
`AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource`

Las políticas que definen quién puede ver un recurso de bean de datos (los beans de datos contienen información acerca de los recursos de datos como, por ejemplo, una oferta de subasta o un pedido y se utilizan generalmente en los archivos JSP), adoptan el siguiente convenio de denominación:

<GrupoAccesoXYZs> Display <GrupoRecursosBeanDatosXYZ>

Por ejemplo: `MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup`.

Sugerencias para cambiar las políticas por omisión

Recuerde lo siguiente cuando deba modificar las políticas por omisión:

- La mayor parte de los grupos de acceso se definen mediante roles de usuario como, por ejemplo, Comprador o Gestor de productos. Para comprender mejor estos roles y las acciones que permiten realizar, consulte el apartado "Roles" en la página 32.
- Antes de cambiar una política para utilizar un grupo de acceso diferente, revise la definición de dicho grupo de acceso para asegurarse de que cumple con sus requisitos. Para hacerlo, en la Consola de administración de organizaciones seleccione **Gestión de acceso > Grupos de acceso**.
- Dependiendo del valor que seleccione para Vista, la página de políticas mostrará las políticas que son propiedad de la organización seleccionada. No diferencia entre las políticas a nivel de sitio y las políticas específicas de una organización determinada.
- Cambie el nombre de las políticas por omisión que modifique de modo que el nombre refleje lo que hace la política, y así podrá identificar las políticas por omisión que ha modificado. Se le recomienda que utilice un convenio de denominación para sus políticas personalizadas. Si resulta adecuado, debe modificar también la descripción de la política y el nombre de visualización.

Nota: El menú de política de control de acceso se ha trasladado a la Consola de administración de organizaciones. La Consola de administración de organizaciones solamente puede realizar modificaciones sencillas en las definiciones de políticas de control de acceso y en las definiciones de grupos de acceso. La solución óptima es actualizar los datos mediante archivos XML. Las operaciones siguientes solamente se pueden hacer a través de XML:

1. Definir acciones, recursos, atributos, relaciones y grupos de relaciones nuevos.
2. Definir grupos de recursos implícitos complejos y grupos de acceso implícitos complejos.
3. Asignar una política nueva a un grupo de políticas.

Después de modificar la política

Después de crear una política nueva se debe asignar a un grupo de políticas para que pueda entrar en vigor. La nueva política se debe asignar al grupo cuya finalidad es la misma que la de la política. Para obtener más información sobre los nombres de grupos de políticas, consulte el apartado "Políticas y grupos de control de acceso por omisión", en la página 217.

Cada vez que crea o modifica una política de control de acceso, debe realizar determinadas pruebas para verificar que la política funciona correctamente. Cuando ha comprobado todas las políticas nuevas y modificadas que hay actualmente en la base de datos, es aconsejable extraer esta información en archivos XML. Estos archivos tienen el mismo formato que los archivos relacionados de políticas de control de acceso iniciales: `defaultAccessControlPolices.xml`, `defaultAccessControlPolicies_entorno_nacional.xml` y `ACUserGroup_entorno_nacional.xml`. Este paso es necesario porque los cambios realizados mediante la Consola de administración únicamente afectan a la información de políticas que está almacenada en la base de datos. Los archivos

XML que se utilizaban para cargar las políticas de control de acceso por omisión y sus componentes durante la creación de la instancia no se actualizan automáticamente.

Debe mantener la coherencia entre los archivos XML y la información de control de acceso en las bases de datos por diversos motivos:

- Cuando crea una instancia de WebSphere Commerce, las definiciones del grupo de políticas y del grupo de acceso se cargan desde los archivos XML.
- Los archivos XML son un método práctico de ver y editar directamente las políticas y sus componentes, por lo que mantener actualizados estos archivos resulta esencial.

Comprobación de los cambios realizados en las políticas

Para cada política, asegúrese de lo siguiente:

- Un usuario que pertenece al grupo de acceso de la política puede realizar las acciones especificadas en los recursos especificados. Si ha suprimido la autorización para realizar una acción, también debe asegurarse de que el usuario ya no puede realizar la acción.
- Un usuario que no pertenece al grupo de acceso de la política no puede realizar las acciones especificadas en los recursos especificados.

Por ejemplo, suponga que implementa el escenario de personalización 1 para una subasta del Capítulo 5, en el cual suprime la posibilidad de que los administradores de la subasta puedan cerrar las ofertas de subasta. Para comprobar si este cambio está funcionando correctamente, debe iniciar la sesión como un usuario perteneciente al grupo de acceso `administrador de subasta` y realizar las acciones siguientes:

- Modificar una subasta
- Suprimir una subasta.

También debe comprobar si un administrador de subasta no puede cerrar las ofertas de subasta.

A continuación, inicie la sesión como un usuario perteneciente al grupo `administrador de subasta` e intente realizar las mismas acciones. Si la política funciona correctamente no podrá realizar las acciones.

Extracción de los cambios realizados en las políticas a archivos XML

Cuando haya finalizado y comprobado los cambios en las políticas, debe actualizar los archivos XML para que estén sincronizados con la información de políticas contenida en las bases de datos. Consulte el Capítulo 13, “Personalización de las políticas de control de acceso mediante XML”, en la página 143 para obtener una descripción de los diferentes archivos XML relacionados con las políticas de control de acceso y los grupos de acceso. También incluye descripciones sobre cómo extraer de las bases de datos los cambios realizados en las políticas y pasarlos a los archivos XML, y cómo cargar la información de políticas desde los archivos XML en las bases de datos.

Capítulo 12. Personalización de las políticas de control de acceso mediante la GUI

Los escenarios que se muestran a continuación le permiten aplicar lo que ha aprendido sobre las políticas de control de acceso para realizar cambios básicos en las políticas por omisión mediante la GUI. Si desea realizar cambios más sofisticados, tendrá que utilizar XML. Consulte el Capítulo 13, "Personalización de las políticas de control de acceso mediante XML", en la página 143.

Para todos esos escenarios, se presupone que un administrador de sitio está modificando las políticas para la organización raíz. Cuando realice los pasos de algunos de estos escenarios, podrá seguir la misma metodología para realizar cambios que no se describen de forma específica en este manual.

Los escenarios están organizados por área de negocio. Dentro de cada área de negocio, los escenarios se presentan según el orden de mayor complejidad.

Tabla 10. Tabla de contenido de los escenarios

Área de negocio	**Comienza en**
Subastas	"Escenario de subastas 1: suprimir la posibilidad de que los administradores de subastas puedan cerrar las ofertas de subasta" en la página 114
Contratos	"Escenario de contratos 1: suprimir la posibilidad de que los gestores de contratos puedan añadir o suprimir adjuntos de contratos" en la página 118
Pedidos	"Escenario de pedidos 1: permitir que solamente los compradores puedan crear pedidos" en la página 120
Miembros	"Escenario de miembros 1: suprimir la posibilidad de que el usuario pueda autorregistrarse" en la página 126
Cupones	"Escenario de cupones 1: permitir que solamente los compradores puedan canjear cupones" en la página 131
Compras	"Escenario de compras 1: permitir que los jefes de compras gestionen el carro de la compra para los pedidos creados por su organización" en la página 135
Inventario	"Escenario de inventario 1: permitir que los administradores del centro de despacho de pedidos puedan actualizarlos pero no suprimirlos" en la página 138
Business intelligence	"Escenario de Business intelligence 1: permitir que los auditores vean los informes de business intelligence" en la página 140

Si está buscando un escenario que describa un tipo de cambio determinado, consulte la Tabla 11 en la página 114, que muestra una referencia cruzada de los escenarios según el tipo de personalización descrito.

Tabla 11. Escenarios de personalización organizados por tipo de personalización

Personalización	Vea la página
Añadir un rol a un grupo de acceso de política	133
Cambiar un grupo de acceso de política	136,138
Cambiar una relación de recursos de una política	122,135
Cambiar una política para que utilice un grupo de acceso diferente	116,120,122,127,131,133
Crear un nuevo grupo de acceso y utilizarlo en una política	125,128
Crear un grupo de acciones nuevo y utilizarlo en una política	129,136
Crear una política a nivel de recursos nueva	119,136
Crear una política basada en roles nueva	128,140
Crear un nuevo rol y utilizarlo en una política a nivel de recursos	128,140
Suprimir una política	115,127
Suprimir una acción de un grupo de acciones de una política	3,118

Escenario de subastas 1: suprimir la posibilidad de que los administradores de subastas puedan cerrar las ofertas de subasta

Por omisión, los administradores de subasta pueden modificar o suprimir las subastas de la tienda y también cerrar las ofertas de subasta. En determinados casos, es posible que no desee otorgar a los administradores de la subasta la autorización para cerrar las ofertas de subasta, ya sea porque desea que esta acción la controlen otros o porque no necesita esta acción para la tienda.

En este escenario, suprimirá la autorización que tienen los administradores de subasta de cerrar las ofertas de subasta. Para realizar este cambio, efectúe lo siguiente:

1. Utilice el Apéndice para encontrar la política a nivel de recursos que define las acciones que pueden realizar los administradores de subasta.
2. Determine el nombre del grupo de acciones de la política.
3. Suprima la acción de cerrar las ofertas de subasta del grupo de acciones de la política.

Pasos que debe realizar

Identificar la política cuyo grupo de acciones debe modificarse

1. Vaya al apartado de Subastas en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es:

   ```
   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
   ```

2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. Localice la política en la lista.

5. Anote el nombre del grupo de acciones de la política— `AuctionManage`. Este es el grupo de acciones que debe cambiar para suprimir la acción de cerrar las ofertas de subasta.

Suprimir la acción de cerrar las ofertas de subasta del grupo de acciones de la política

1. Pulse **Gestión de acceso > Grupo de acciones**.
2. En la lista de grupos de acciones, seleccione **AuctionManage**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones.
4. En la lista Acciones seleccionadas, seleccione **com.ibm.commerce.negotiation.commands.CloseBiddingCmd**.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Actualizar el registro de políticas con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de subastas 2: suprimir la posibilidad de que los gestores de subastas puedan retractar las ofertas de subasta

Por omisión, los gestores de subastas de una tienda pueden retractar las ofertas que se han sometido en sus subastas. Es posible que en algunos casos desee que esta autorización no la posea nadie. Para realizar este cambio, debe encontrar la política a nivel de recursos que define quién puede retractar las ofertas de subasta y suprimirla.

En el escenario de subastas 1, cerrar las ofertas de subasta, era una de las diferentes acciones incluidas en la política. Por consiguiente, únicamente tenía que suprimir la acción del grupo de acciones de la política. Sin embargo, en este escenario toda una política controla la retracción de las ofertas de subasta. Por lo tanto, debe suprimir una política y no simplemente una acción.

Para suprimir la política, deberá realizar lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que cubre la retracción de las ofertas de subasta por parte de los gestores de subastas.
- Suprima la política.

Nota: Antes de suprimir la política, anote su nombre, el nombre del grupo de acceso, el nombre del grupo de recursos y un nombre de grupo de acciones para que pueda volver a crearla en el escenario siguiente.

Pasos que debe realizar

1. Vaya al apartado de Subastas en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es:

   `AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.

4. En la lista de políticas, seleccione lo siguiente:
   AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
5. Pulse **Suprimir**.

Actualizar el registro de políticas con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.
5. Repita los pasos 3 y 4 para el **Registro de grupos de políticas de control de acceso**.

Escenario de subastas 3: limitar las ofertas de subasta a los compradores

Por omisión, todos los usuarios registrados pueden realizar ofertas para los productos que están en subasta en una tienda, independientemente de la posición que tengan en la organización. En algunos casos, es posible que desee limitar las ofertas de subasta a un grupo de usuarios limitado, por ejemplo, los que tienen asignado el rol de `comprador` en WebSphere Commerce.

En este escenario, cambiará una política a nivel de recursos y también la política basada en roles asociada. Para limitar las ofertas de subasta a los miembros de una organización compradora que tienen el rol de `comprador`, deberá realizar lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que especifica quién puede crear una oferta de subasta.
- Cambie el grupo de acceso de la política de modo que dejen de ser todos los usuarios registrados y pasen a ser aquellos que tienen el rol de `comprador`.
- Cambie el nombre de la política, la descripción y el nombre de visualización.
- Identifique el mandato para crear ofertas de subasta.
- Utilice el Apéndice para buscar la política basada en roles para los compradores (parte compradora). Esta política define los mandatos que pueden ejecutar los usuarios que tienen el rol de comprador (parte compradora). Debe actualizar este grupo de recursos de la política para que los compradores puedan ejecutar el mandato para crear ofertas de subasta.
- Actualice este grupo de recursos de la política basada en roles para que incluya el mandato para crear ofertas de subasta.

Pasos que debe realizar

Identificar la política a nivel de recursos

1. Vaya al apartado de Subastas en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es:
   `RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource`.
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. En la lista de políticas, seleccione **RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource**.

5. Anote el nombre del grupo de acciones de la política— `BidCreate`. Este es el grupo de acciones que debe visualizar para buscar el nombre del mandato con el que se crean las ofertas de subasta.

Cambiar el grupo de acceso de la política

1. Pulse **Cambiar** para visualizar la página Cambiar política.
2. En Grupo de usuarios, pulse **Buscar** y seleccione **Compradores (parte compradora)**.
3. Pulse **Aceptar**.
4. Cambie el nombre de la política, el nombre de visualización y la descripción de la política, editando el texto.
5. Pulse **Aceptar**.

Identificar el mandato para crear ofertas de subasta

1. Pulse **Gestión de acceso > Grupos de acciones**.
2. En la lista de grupos de acciones, seleccione **BidCreate**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones. Anote el nombre del mandato para crear ofertas de subasta: `com.ibm.commerce.negotiation.commands.BidSubmitCmd`. Debe añadir este mandato al grupo de recursos que contiene la lista de mandatos que puede ejecutar un comprador.

Identificar la política basada en roles y el grupo de recursos para compradores (parte compradora)

1. Busque en el apartado de políticas basadas en roles del Apéndice la política basada en roles para compradores (parte compradora). La política es:
   `Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup`.
2. Pulse **Gestión de acceso** > **Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. Anote el nombre del grupo de recursos: `Buyers(buy-side)CommandsResourceGroup`. Ahora ya tiene el nombre del grupo de recursos que necesita actualizar.

Actualizar el grupo de recursos de la política basada en roles para incluir el mandato para crear ofertas de subasta

1. Pulse **Gestión de acceso > Grupos de recursos**.
2. Seleccione **Buyers(buy-side)CommandsResourceGroup**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de recursos.
4. Pulse **Siguiente** para visualizar la página Detalles.
5. En la lista Recursos disponibles, seleccione **com.ibm.commerce.negotiation.commands.BidSubmitCmd**. Este es el mandato para crear ofertas de subasta.
6. Pulse **Añadir** para añadir el mandato al grupo de recursos.
7. Pulse **Finalizar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración >Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.

4. Pulse **Actualizar**.

Escenario de contratos 1: suprimir la posibilidad de que los gestores de contratos puedan añadir o suprimir adjuntos de contratos

Por omisión, los gestores de contratos de una tienda pueden añadir o suprimir adjuntos a los contratos que gestionan. En algunos casos, es posible que no desee que los gestores de contratos posean esta autorización.

En este escenario, cambiará una política a nivel de recursos que define las acciones que puede llevar a cabo un gestor de contratos. Para suprimir la autorización que tienen los gestores de contratos para añadir o suprimir adjuntos de contratos, deberá realizar lo siguiente:

- Utilice el Apéndice para encontrar la política a nivel de recursos que define las acciones que pueden realizar los gestores de contratos.
- Determine el nombre del grupo de acciones de la política.
- Suprima las acciones para añadir adjuntos y suprimir adjuntos de la lista de acciones del grupo de acciones de la política.

Pasos que debe realizar

Identificar la política a nivel de recursos y el grupo de acciones

1. Vaya al apartado de Contratos en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es:
   `ContractManagersForOrgExecuteContractManageCommandsOnContractResource`
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. Localice la política en la lista.
5. Anote el nombre del grupo de acciones de la política— `ContractManage`. Este es el grupo de acciones que debe cambiar para suprimir la acción de añadir y suprimir adjuntos.

Suprimir las acciones para añadir y suprimir adjuntos del grupo de acciones de la política

1. Pulse **Gestión de acceso** > **Grupo de acciones**.
2. En la lista de grupos de acciones, seleccione **ContractManage**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de recursos.
4. En la lista Acciones seleccionadas, seleccione las acciones siguientes:
   com.ibm.commerce.contract.commands.ContractAttachmentAddCmd
   com.ibm.commerce.contract.commands.ContractAttachmentDeleteCmd.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de contratos 2: permitir que los operadores de contratos y los administradores de contratos desplieguen contratos

Por omisión, los operadores de contratos de una tienda pueden desplegar contratos. En algunos casos, es posible que desee que los administradores de contratos posean también esta autorización.

El diseño flexible de las políticas de control de acceso ofrecen varios métodos para implementar este cambio:

- Puede crear un nuevo grupo de acceso que contenga tanto los operadores de contratos como los administradores de contratos y asignar el nuevo grupo de acceso a la política que define quién puede desplegar contratos.
- Puede añadir las acciones de `desplegar contrato` a la política que especifica las acciones que puede realizar un administrador de contratos.
- Puede crear una política nueva que permita a los administradores de contratos desplegar contratos.

Este escenario describe el tercer método. Muestra cómo crear una política a nivel de recursos que autoriza a los administradores de contratos a desplegar contratos.

Para crear esta política, efectúe lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que autoriza a los operadores de contrato a desplegar contratos.
- Anote el nombre del grupo de acciones de esta política.
- Anote el nombre del grupo de recursos de esta política.
- Defina una política nueva para el grupo de acceso `administrador de contratos`, especificando el grupo de acciones y el grupo de recursos de la política que autoriza a los operadores de contratos a desplegar contratos.

Pasos que debe realizar

Identificar el grupo de acciones y el grupo de recursos que deben utilizarse en la política nueva

1. Vaya al apartado Contratos del Apéndice y busque la política a nivel de recursos que autoriza a los operadores de contrato a desplegar contratos. La política es:
   `ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource`
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. Localice la política en la lista.
5. Anote el nombre del grupo de acciones de la política— `ContractDeploy`. Este es el grupo de acciones que debe utilizar para definir la nueva política.
6. Anote el nombre del grupo de recursos— `ContractDataResourceGroup`. Este es el grupo de recursos que debe utilizar para definir la nueva política.

Definir la nueva política

1. Pulse **Nueva** para que se visualice la página Nueva política.
2. En Nombre, especifique:
   `ContractAdministratorsForOrgExecuteContractDeployCommandsOnContractResource`

3. Como Nombre de visualización, especifique una breve descripción de la política en su idioma local.
4. Como Descripción, especifique una descripción más completa de lo que lleva a cabo la política, en su idioma local.
5. Para Grupo de usuarios, pulse **Buscar** y seleccione **ContractAdministratorForOrg**.
6. Pulse **Aceptar**.
7. Para Grupo de recursos, seleccione **ContractDataResourceGroup**.
8. Para Grupo de acciones, seleccione **ContractDeploy**.
9. Para Tipo de política, seleccione **Política de plantilla agrupable** para designar la política como una política de plantilla.
10. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Nota: Esta política nueva se debe asignar a un grupo de políticas para que entre en vigor. La asignación de políticas debe realizarse mediante XML. Consulte la documentación correspondiente para obtener más información.

Escenario de pedidos 1: permitir que solamente los compradores puedan crear pedidos

Por omisión, todos los usuarios registrados pueden crear pedidos de los productos, independientemente de la posición que tengan en la organización. En algunos casos, es posible que desee limitar la posibilidad de crear pedidos a un grupo de usuarios limitado, por ejemplo, los empleados de la organización compradora. Generalmente, estos empleados tienen asignado el rol de comprador (parte compradora).

Para que sólo puedan crear pedidos los usuarios con el rol de `Comprador`, debe realizar lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que especifica quién puede crear un pedido.
- Cambie el grupo de acceso de la política de todos los usuarios a solamente los que tienen el rol de `comprador`.
- Actualice el nombre de la política, el nombre de visualización y la descripción.
- Identifique el mandato para crear pedidos.
- Utilice el Apéndice para buscar la política basada en roles para el comprador (parte compradora). Esta política define los mandatos que pueden ejecutar los usuarios que tienen el rol de comprador (parte compradora). Debe actualizar este grupo de recursos de la política para que los compradores puedan ejecutar el mandato para crear pedidos.
- Actualice este grupo de recursos de la política basada en roles para que incluya el mandato para crear pedidos.

Pasos que debe realizar

Identificar la política a nivel de recursos

1. Vaya al apartado de Pedidos en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es: `AllUsersExecuteOrderCreateCommandsOnStoreResource`.
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. En la lista de políticas, seleccione: **AllUsersExecuteOrderCreateCommandsOnStoreResource.** Anote el nombre del grupo de acciones de la política— `OrderCreateCommands`. Este es el grupo de acciones que debe visualizar para buscar los nombres de los mandatos con los que se crea un pedido.

Cambiar el grupo de acceso

1. Pulse **Cambiar** para visualizar la página Cambiar política.
2. En Grupo de usuarios, pulse **Buscar** y seleccione **Compradores (parte compradora)**.
3. Pulse **Aceptar**.
4. Actualice el nombre de la política, el nombre de visualización y la descripción, de modo que quede reflejado el cambio del grupo de acceso.
5. Pulse **Aceptar**.

Identificar el mandato para crear pedidos

1. Pulse **Gestión de acceso > Grupos de acciones**.
2. En la lista de grupos de acciones, seleccione **OrderCreateCommands**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones. Anote los nombres de los mandatos para crear pedidos:

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

   Debe añadir estos mandatos al grupo de recursos que contiene la lista de mandatos que puede ejecutar un comprador.

   Nota: El mandato `com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd`, no es necesario.

Identificar la política basada en roles para compradores (parte compradora)

1. Busque en el apartado de políticas basadas en roles del Apéndice la política basada en roles para compradores (parte compradora). La política es: `Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup`.
2. Pulse **Gestión de acceso** > **Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. Localice la política en la lista.

5. Anota el nombre del grupo de recursos— `Buyers(buy-side)CommandsResourceGroup`. Este es el grupo de recursos que debe actualizar.

Actualizar el grupo de recursos de la política basada en roles para incluir el mandato para crear pedidos

1. Pulse **Gestión de acceso > Grupos de recursos**.
2. En la lista de grupos de recursos, seleccione **Buyers(buy-side)CommandsResourceGroup**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de recursos.
4. Pulse **Siguiente** para visualizar la página Detalles.
5. En la lista Recursos disponibles, seleccione los mandatos siguientes para crear pedidos:

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

6. Pulse **Añadir.**
7. Pulse **Terminar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de pedidos 2: permitir que únicamente los administradores de compradores puedan modificar los pedidos

Nota: Este escenario no se aplica a WebSphere Commerce Professional Edition.

Por omisión, todos los usuarios pueden modificar los pedidos que han creado, independientemente de la posición que tengan en la organización. En algunos casos, es posible que desee que solamente el administrador de compradores de la organización tenga autorización para modificar los pedidos.

En este escenario, cambiará una política a nivel de recursos y también una política basada en roles. Para que solamente los administradores de compradores puedan modificar los pedidos pertenecientes a los miembros de una organización compradora, realice lo siguiente:

- Consulte el Apéndice para buscar la política a nivel de recursos que especifica quién puede modificar un pedido.
- Cambie el grupo de acceso de la política de modo que dejen de ser todos los usuarios y pasen a ser aquellos que tienen el rol de `administrador de compradores`.
- Suprima la especificación de la relación de recursos para permitir que los administradores de compradores puedan modificar los pedidos pertenecientes a otros usuarios.
- Actualice el nombre de la política, el nombre de visualización y la descripción.

- Identifique los mandatos para modificar pedidos.
- Utilice el Apéndice para buscar la política basada en roles para el administrador de compradores. Esta política define los mandatos que pueden ejecutar los usuarios que tienen el rol de administrador de compradores. Debe actualizar este grupo de recursos de la política para que los administradores de compradores puedan ejecutar el mandato para modificar pedidos.
- Actualice este grupo de recursos de la política basada en roles para que incluya los mandatos para modificar pedidos.

Pasos que debe realizar

Identificar la política a nivel de recursos

1. Vaya al apartado de Pedidos en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es: `AllUsersExecuteOrderWriteCommandsOnOrderResource`.
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. En la lista de políticas, seleccione **AllUsersExecuteOrderWriteCommandsOnOrderResource**.
5. Anote el nombre del grupo de acciones de la política— `OrderWriteCommands`. Debe visualizar este grupo de acciones para buscar el nombre del mandato para crear un pedido.

Cambiar el grupo de acceso

1. Pulse **Cambiar** para visualizar la página Cambiar política.
2. En Grupo de usuarios, pulse **Buscar** y seleccione **Administradores de compradores**.
3. Pulse **Aceptar**.
4. Para Relación, seleccione **Ninguna**.
5. Actualice el nombre de la política, el nombre de visualización y la descripción, de modo que quede reflejado el cambio del grupo de acceso.
6. Pulse **Aceptar**.

Identificar los mandatos para modificar pedidos

1. Pulse **Gestión de acceso > Grupos de acciones**.
2. En la lista de grupos de acciones, seleccione **OrderWriteCommands**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones. Anote los nombres de los mandatos para modificar pedidos:

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

   Debe añadir estos mandatos al grupo de recursos que contiene la lista de mandatos que puede ejecutar un comprador.

   Nota: Cuando añada el mandato, `com.ibm.commerce.order.commands.OrderCopyCmd-Write` al grupo de

recursos, aparecerá debajo de los Recursos disponibles como `com.ibm.commerce.order.commands.OrderCopyCmd`.

Identificar la política basada en roles para el rol de administrador de compradores

1. Busque en el apartado de políticas basadas en roles del Apéndice la política basada en roles para administradores de compradores. La política es: `BuyerAdministratorsExecuteBuyersAdministratorsCommands`.
2. Pulse **Gestión de acceso** > **Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. Localice la política en la lista.
5. Anote el nombre del grupo de recursos— `BuyersAdministratorsCommmandsResourceGroup`.

   Este es el nombre del grupo de recursos que debe actualizar.

Actualizar el grupo de recursos de la política basada en roles para incluir los mandatos para modificar pedidos

1. Pulse **Gestión de acceso > Grupos de recursos**.
2. Seleccione **BuyersAdministratorsCommandsResourceGroup**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de recursos.
4. Pulse **Siguiente** para visualizar la página Detalles.
5. En la lista Recursos disponibles, seleccione los mandatos siguientes para modificar pedidos:

   ```
   com.ibm.commerce.order.commands.OrderCancelCmd
   com.ibm.commerce.order.commands.OrderCopyCmd
   com.ibm.commerce.order.commands.OrderUnlockCmd
   com.ibm.commerce.orderitems.commands.OrderItemAddCmd
   com.ibm.commerce.orderitems.commands.OrderItemDeleteCmd
   com.ibm.commerce.orderitems.commands.OrderItemMoveCmd
   com.ibm.commerce.orderitems.commands.OrderItemUpdate.Cmd
   com.ibm.commerce.orderquotation.commands.OrderItemSelectCmd
   ```
6. Pulse **Añadir** para añadir el mandato al grupo de recursos.
7. Pulse **Terminar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de pedidos 3: permitir que los aprobadores de las RMA puedan aprobar todas las RMA

Por omisión, los aprobadores de las RMA (autorización de devolución de artículos) de una tienda solamente pueden aprobar las RMA de sus propias tiendas. En algunos casos, es posible que desee permitir que los aprobadores de las RMA puedan aprobar las RMA de cualquier tienda. Esto puede ser así si algunas tiendas son propiedad de la misma organización o si la misma persona maneja las aprobaciones de las RMA de varias tiendas.

En este escenario, creará un nuevo grupo de acceso y lo utilizará en una política a nivel de recursos nueva. Para que todos los aprobadores de las RMA puedan aprobar las RMA de cualquier tienda, deberá realizar lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que permite a los aprobadores de las RMA de una organización aprobar las RMA de su organización.
- Anote el nombre del grupo de recursos y del grupo de acciones que se utilizan en esta política.
- Visualice el grupo de acceso de la política, `RMAApproversForOrg`, y anote los roles que incluye. El grupo de acceso se define utilizando como criterio de selección las organizaciones y los roles. Para otorgar autorización a los usuarios para llevar a cabo una acción en varias organizaciones, el grupo de acceso debe definirse sin criterios de organización.
- Cree un nuevo grupo de acceso, `RMAApprovers`, que utilice los mismos roles pero que no incluya criterios de organización.
- Cree una nueva política utilizando:
  - El nuevo grupo de acceso, `RMAApprovers`
  - El grupo de acciones de la política existente
  - El grupo de recursos de la política existente

Pasos que debe realizar

Identificar el grupo de acciones y el grupo de recursos que deben utilizarse en la política nueva

1. Vaya al apartado Pedidos del Apéndice y busque la política a nivel de recursos que autoriza a `RMAApproversForOrg` a aprobar las RMA de sus tiendas. La política es: `RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource`
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. Localice la política en la lista.
5. Anote el nombre del grupo de acciones de la política— `RMAApproveCommands`. Este es el grupo de acciones que utilizará para definir la nueva política.
6. Anote el nombre del grupo de recursos— `RMADataResourceGroup`. Este es el grupo de recursos que utilizará para definir la nueva política.
7. Anote el nombre del grupo de acceso— `RMAApproversForOrg`. Visualice este grupo de acceso para ver los roles que se han de incluir en el nuevo grupo de acceso.

Identificar los roles que se han de utilizar en el nuevo grupo de acceso

1. Pulse **Gestión de acceso > Grupos de acceso**.
2. En la lista de grupos de acceso, seleccione **RMAApproversForOrg**.
3. Pulse **Cambiar**.
4. Pulse **Criterios** para que se visualice la página Criterios.
5. En Roles y organizaciones seleccionados, anote los roles que se utilizan en el grupo de acceso:
   - `Supervisor de servicio al cliente`
   - `Vendedor`
   - `Director de ventas`

- Director de operaciones

6. Pulse **Cancelar** para regresar a la lista de grupos de acceso.

Definir el nuevo grupo de acceso

1. Pulse **Nuevo** para visualizar la página Detalles del nuevo grupo de acceso.
2. En Nombre, especifique RMAApprovers.
3. En Descripción, escriba una descripción del grupo de acceso.
4. En Organización padre, seleccione Organización raíz.
5. Pulse **Siguiente** para visualizar la página Criterios del nuevo grupo de acceso.
6. Pulse **Basándose en organizaciones y roles**.
7. En la lista de roles, seleccione los roles siguientes:
   - **Supervisor de servicio al cliente**
   - **Vendedor**
   - **Director de ventas**
   - **Director de operaciones**
8. Pulse **Finalizar**.

Definir la nueva política

1. Pulse **Gestión de acceso > Políticas**.
2. Pulse **Nueva** para que se visualice la página Nueva política.
3. En Nombre, especifique:
   RMAApproversExecuteRMAApproveCommandsOnRMAResource
4. Como Nombre de visualización, especifique una breve descripción de la política en su idioma local.
5. Como Descripción, especifique una descripción más completa de lo que lleva a cabo la política, en su idioma local.
6. Para Grupo de usuarios, pulse **Buscar** y seleccione **RMAApprovers**.
7. Pulse **Aceptar**.
8. Para Grupo de recursos, seleccione **RMADataResourceGroup**.
9. Para Grupo de acciones, seleccione **RMAApproveCommands**.
10. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de miembros 1: suprimir la posibilidad de que el usuario pueda autorregistrarse

Por omisión, los usuarios se pueden autorregistrar si pertenecen a una organización registrada. Los administradores de los miembros también tienen autorización para registrar a los usuarios que pertenecen a su organización. En los sitios en que se necesita un control de acceso estricto, es posible que sea necesario eliminar la posibilidad del autorregistro y solicitar a los usuarios que se registren mediante los administradores de miembros.

Nota: En WebSphere Commerce Professional Edition, solamente hay tres organizaciones, la organización raíz, la organización por omisión y la organización vendedora.

En este escenario, se suprimirá la política a nivel de recursos que permite a los usuarios el autorregistro pero se dejará intacta una política que permite a los administradores de miembros registrar a los usuarios de su organización.

Para suprimir la política a nivel de recursos que permite a los usuarios el autorregistro, efectúe lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que autoriza el autorregistro de los usuarios.
- Suprima la política.

Pasos que debe realizar

Suprimir la política

1. Vaya al apartado Miembros del Apéndice y busque la política a nivel de recursos que autoriza el autorregistro de los usuarios. La política es: `GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource`.
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. En la lista de políticas, seleccione **GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource**
5. Pulse **Suprimir**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.
5. Repita los pasos 3 y 4 para el **Registro de grupos de políticas de control de acceso**.

Escenario de miembros 2: permitir que solamente los usuarios registrados y los usuarios aprobados puedan cambiar su información de dirección

Por omisión, los usuarios pueden modificar su información de dirección si el registro se ha aprobado o está pendiente de aprobación. En algunos casos, es posible que desee que solamente los usuarios registrados y aprobados puedan gestionar sus direcciones.

En este escenario, cambiará el grupo de acceso de la política a nivel de recursos que autoriza a los usuarios a gestionar la información de dirección, para lo que debe realizar lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que permite a los usuarios gestionar su información de dirección.
- Cambie el grupo de acceso de la política.

Dado que el grupo de acceso RegisteredApprovedUsers no contiene ningún rol, no es necesario que actualice una política basada en roles para este cambio.

Pasos que debe realizar

Cambiar el grupo de acceso de la política a nivel de recursos

1. Vaya al apartado Miembros del Apéndice y busque la política a nivel de recursos que permite que los usuarios gestionen la información de dirección. La política es—NonRejectedUsersExecuteAddressManageCommandsOnUserResource.

   Nota: Los usuarios que no han sido rechazados son aquellos usuarios cuyo registro no se ha rechazado. Su registro ha sido aprobado o está pendiente de aprobación.
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. En la lista de políticas, seleccione **NonRejectedUsersExecuteAddressManageCommandsOnUserResource.**
5. Pulse **Cambiar** para visualizar la página Cambiar política.
6. Para Grupo de usuarios, pulse **Buscar** y seleccione **RegisteredApprovedUsers**.
7. Pulse **Aceptar**.
8. Actualice el nombre de la política, el nombre de visualización y la descripción, de modo que quede reflejado el cambio del grupo de acceso.
9. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de miembros 3: permitir que los responsables del registro de miembros puedan registrar usuarios

Por omisión, los administradores de miembros de una organización tienen autorización para registrar a los miembros de su organización. El grupo de acceso, MemberAdministratorsForOrg, incluye varios roles como, por ejemplo, administrador de compradores y administrador de vendedores, que pueden realizar diferentes tareas de administración. En algunos casos, es posible que desee crear un rol diferente que tenga autorización solamente para registrar a los miembros de la organización.

A continuación se muestra una visión general de los pasos que debe realizar:

- Cree un nuevo rol y, para este rol, cree un nuevo grupo de acceso, un nuevo grupo de recursos y una nueva política basada en roles.
- Modifique una política a nivel de recursos existente para utilizar el nuevo rol.

En este escenario, realice lo siguiente:

- Defina un nuevo rol llamado Member Registrar.

- Defina un nuevo grupo de acceso llamado `MemberRegistrars`, que incluirá el rol de responsable del registro de miembros.
- Utilice el Apéndice para buscar la política a nivel de recursos que permita que los administradores de miembros registren miembros.
- Anote el nombre de la acción en este grupo de acciones. Debe crear un nuevo grupo de recursos con esta acción y utilizarlo en la política basada en roles para el nuevo rol. Recuerde que en las políticas basadas en roles para acciones, el grupo de acciones contiene una sola acción de ejecución. El grupo de recursos contiene las acciones (mandatos) que se pueden ejecutar.
- Defina un grupo de recursos nuevo llamado `UserAdminRegistrationCommands`, que incluya el mandato para registrar miembros. Este grupo de recursos lo utilizará en la política basada en roles para el rol de responsable del registro de miembros.
- Defina una política basada en roles nueva para los responsables del registro de miembros, que utilizará el grupo de acceso MemberRegistrars y el grupo de recursos MemberRegistrationCommands.
- Modifique la política a nivel de recursos que define quién puede registrar a los miembros y cambiar su grupo de acceso de MembershipAdministrators a MemberRegistrars.

Pasos que debe realizar

Definir el nuevo rol

1. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Roles**.
2. En la página Roles, pulse **Nuevo**.
3. En Nombre, especifique Member Registrar.
4. En Descripción, especifique una descripción del rol de responsable del registro de miembros en su idioma local.
5. Pulse **Aceptar**.

Definir un nuevo grupo de acceso que contenga el rol de responsable del registro de miembros

1. Pulse **Gestión de acceso > Grupos de acceso**.
2. En la página Grupos de acceso, pulse **Nuevo** para visualizar la página Detalles del nuevo grupo de acceso.
3. En Nombre, especifique: MemberRegistrars.
4. En Organización padre, seleccione **Organización raíz**.
5. En Descripción, especifique una descripción del grupo de acceso en su idioma local.
6. Pulse **Siguiente** para visualizar la página Criterios del nuevo grupo de acceso.
7. Pulse **Basándose en organizaciones y roles**.
8. En la lista Rol, seleccione **Member Registrar**.
9. Pulse **Para organización** para especificar que el rol debe desempeñarse en la propia organización del usuario o en sus antecesoras.
10. Pulse **Terminar**.

Identificar acciones para utilizarlas en el grupo de recursos para la política basada en roles del responsable del registro de miembros

1. Vaya al apartado Miembros del Apéndice y busque la política a nivel de recursos que autoriza a los administradores de miembros a registrar usuarios. La política es:

   `CSAMembershipAdministratorsForOrgExecuteUserAdminRegistrationCommandsOn OrganizationResource`
2. Pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. Localice la política en la lista.
5. Anote el nombre del grupo de acciones de la política— `UserAdminRegistration`. Este es el grupo de acciones que debe visualizar para identificar las acciones para registrar miembros.
6. Pulse **Gestión de acceso > Grupos de acciones**.
7. En la lista de grupos de acciones, seleccione **UserAdminRegistration**.
8. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones.
9. Anote el nombre del mandato para registrar miembros: `com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd`.

Definir el nuevo grupo de recursos que se ha de utilizar en la política basada en roles para los responsables del registro de miembros

1. Pulse **Gestión de acceso > Grupo de recursos** para visualizar la página Grupo de recursos.
2. Pulse **Nuevo** para visualizar la página General para el nuevo grupo de recursos.
3. En Nombre, especifique `UserAdminRegistrationCommands`.
4. Como Nombre de visualización, especifique una breve descripción del grupo de políticas en su idioma local.
5. Como Descripción, especifique una descripción más completa del grupo de recursos, en su idioma local.
6. En Tipo, seleccione **Grupo de recursos explícitos**.
7. Pulse **Siguiente**.
8. Pulse **Siguiente** para visualizar la página Detalles del nuevo grupo de recursos.
9. En la lista de Recursos disponibles, seleccione lo siguiente:

   com.ibm.commerce.usermanagement.commands.
   UserRegistrationAdminAddCmd
10. Pulse **Añadir**.
11. Pulse **Terminar**.

Definir una política basada en roles para el rol de responsable del registro de miembros

1. Pulse **Gestión de acceso** > **Políticas**.
2. En la página Políticas, pulse **Nueva**.
3. En Nombre, especifique **MemberRegistrarsExecuteUserAdminRegistrationCommands**.

4. Como Nombre de visualización, especifique una breve descripción de la política en su idioma local.
5. Como Descripción, especifique una descripción más completa de lo que lleva a cabo la política, en su idioma local.
6. Para Grupo de usuarios, pulse **Buscar** y seleccione **MemberRegistrars**.
7. Pulse **Aceptar**.
8. Para Grupo de recursos, seleccione **UserAdminRegistrationCommands**.
9. Para Grupo de acciones, seleccione **ExecuteCommandActionGroup**.
10. Pulse **Aceptar**.

Nota: Después de crear una política nueva, se debe asignar a un grupo de políticas para que entre en vigor. Esto debe realizarse mediante XML. Para obtener más información, consulte el Capítulo 13, "Personalización de las políticas de control de acceso mediante XML", en la página 143.

Modificar la política a nivel de recursos de modo que utilice el nuevo grupo de acceso

Después de modificar la política a nivel de recursos, sólo los usuarios que tengan el rol Member Registrar en la misma organización que el recurso podrán registrar al usuario. Los usuarios que desempeñen el rol en cualquier otra organización no podrán realizarlo.

1. En la lista de políticas, seleccione lo siguiente:

   CSAMembershipAdministratorsForOrgExecuteUserAdmin RegistrationCommandsOnOrganizationResource
2. Pulse **Cambiar** para visualizar la página Cambiar política.
3. Actualice el nombre de la política, el nombre de visualización y la descripción de modo que refleje el cambio del grupo de acceso.
4. Para Grupo de usuarios, pulse **Buscar** y seleccione **MemberRegistrars**.
5. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de cupones 1: permitir que solamente los compradores puedan canjear cupones

Por omisión, todos los usuarios pueden canjear cupones. En algunos casos, es posible que desee limitar el canje de cupones a los usuarios que tienen asignado el rol de `Comprador` en WebSphere Commerce.

En este escenario, cambiará una política a nivel de recursos y también la política basada en roles asociada. Para limitar el canje de cupones a los usuarios que tienen el rol de `Comprador`, efectúe lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que especifica quién puede canjear un cupón.
- Cambie el grupo de acceso de la política de todos los usuarios a solamente los que tienen el rol de `Comprador`.

- Identifique el mandato para canjear cupones.
- Utilice el Apéndice para buscar la política basada en roles para el comprador (parte compradora). Esta política define los mandatos que pueden ejecutar los usuarios que tienen el rol de comprador (parte compradora). Debe actualizar este grupo de recursos de la política para que los compradores puedan ejecutar el mandato para canjear cupones.
- Actualice este grupo de recursos de la política basada en roles para que incluya el mandato para canjear cupones.

Pasos que debe realizar

Identificar la política a nivel de recursos y su grupo de acciones

1. Vaya al apartado de Cupones en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es:

   `AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource`
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. En la lista de políticas, seleccione lo siguiente:

   `AllUsersExecuteCouponRedemptionCommandsOnCoupon WalletResource`
5. Anote el nombre del grupo de acciones de la política— `CouponRedemption`. Este es el grupo de acciones que debe visualizar para buscar el nombre del mandato con el que se canjean los cupones.

Cambiar el grupo de acceso

1. Pulse **Cambiar** para visualizar la página Cambiar política.
2. En Grupo de usuarios, pulse **Buscar** y seleccione **Compradores (parte compradora)**.
3. Pulse **Aceptar**.
4. Actualice el nombre de la política, el nombre de visualización y la descripción, de modo que quede reflejado el cambio del grupo de acceso.
5. Pulse **Aceptar**.

Identificar los mandatos para canjear cupones

1. Pulse **Gestión de acceso > Grupos de acciones**.
2. En la lista de grupos de acciones, seleccione **CouponRedemption**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones. Anote los nombres de los mandatos para canjear cupones:

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

   Debe añadir estos mandatos al grupo de recursos que contiene la lista de mandatos que puede ejecutar un comprador.

Identificar la política basada en roles para compradores (parte compradora)

1. Busque en el apartado de políticas basadas en roles del Apéndice la política basada en roles para compradores (parte compradora). La política es:

   `Buyers(buy-side)ExecuteBuyers(buy-side)CommandsResourceGroup`
2. Pulse **Gestión de acceso** > **Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.

4. Localice la política en la lista.
5. Anote el nombre del grupo de recursos: `Buyers(buy-side)CommandsResourceGroup`. Este es el nombre del grupo de recursos que debe actualizar.

Actualizar el grupo de recursos de la política basada en roles para incluir el mandato para crear ofertas de subasta

1. Pulse **Gestión de acceso > Grupos de recursos**.
2. Seleccione **Buyers(buy-side)CommandsResourceGroup**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de recursos.
4. Pulse **Siguiente** para visualizar la página Detalles.
5. En la lista Recursos disponibles, seleccione **com.ibm.commerce.couponredemption.commands.CouponDSSCmd com.ibm.commerce.couponredemption.commands.UseCouponIdCmd**. Esos son los mandatos para canjear cupones.
6. Pulse **Añadir** para añadir los mandatos al grupo de recursos.
7. Pulse **Finalizar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de cupones 2: permitir que los administradores de cupones y los gestores de operaciones puedan crear promociones de cupones electrónicos

Por omisión, los administradores de cupones de una tienda pueden crear promociones de cupones electrónicos para la tienda. En algunos casos, es posible que desee que los gestores de operaciones posean también esta autorización.

El diseño flexible de las políticas de control de acceso ofrecen varios métodos para implementar este cambio:

- Puede añadir el rol de Director de operaciones al grupo de acceso de la política que especifica quién puede crear promociones de cupones electrónicos.
- Puede crear una política nueva que permita a los gestores de operaciones crear promociones de cupones electrónicos.

Este escenario describe el primer método. Muestra cómo puede añadir el rol de Director de operaciones a la política a nivel de recursos que autoriza a los administradores de cupones a crear cupones.

Para realizar este cambio, realice lo siguiente:

- Consulte el Apéndice para buscar la política a nivel de recursos que especifica quién puede crear promociones de cupones electrónicos.
- Cambie el grupo de acceso de la política de modo que incluya a los usuarios que tienen el rol de `Gestor de operaciones`.
- Visualice el grupo de acciones de la política a nivel de recursos para identificar el mandato para crear promociones de cupones electrónicos.

- Utilice el Apéndice para buscar la política basada en roles para un Director de operaciones. Esta política define los mandatos que pueden ejecutar los usuarios que tienen el rol de Director de operaciones. Debe actualizar este grupo de recursos de la política para que los administradores de tienda puedan ejecutar el mandato para crear promociones de cupones electrónicos.
- Actualice este grupo de recursos de la política basada en roles para que incluya el mandato para crear promociones de cupones electrónicos.

Pasos que debe realizar

Identificar el grupo de acciones y el grupo de acceso para la política a nivel de recursos

1. Vaya al apartado de Subastas en el Apéndice e identifique la política a nivel de recursos que debe modificarse. La política es:

   CouponAdministratorsForOrgExecuteCouponPromotionCreateCommands OnStoreEntityResource
2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. Localice la política en la lista.
5. Anote el nombre del grupo de acciones de la política —CouponPromotionCreate. Este es el grupo de acciones que debe visualizar para buscar el nombre del mandato para crear promociones de cupones electrónicos.
6. Anote el nombre del grupo de acceso de la política— CouponAdministratorsForOrg. Este es el grupo de acceso que debe actualizar para incluir el rol de administrador de tienda.

Cambiar el grupo de acceso

1. Pulse **Gestión de acceso > Grupos de acceso**.
2. En la lista de grupos de acceso, seleccione **CouponAdministratorsForOrg**
3. Pulse **Cambiar** para visualizar la página Detalles.
4. Pulse **Criterios** para visualizar la página Criterios.
5. En la lista Rol, seleccione **Gestor de operaciones**.
6. Pulse **Para organización** para especificar que el rol debe desempeñarse en la propia organización del recurso o en sus antecesoras.
7. Pulse **Añadir**.
8. Pulse **Aceptar**.

Identificar los mandatos para crear promociones de pedidos

1. Pulse **Gestión de acceso > Grupos de acciones**.
2. En la lista de grupos de acciones, seleccione **CouponPromotionCreate**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones. Anote el nombre del mandato para crear promociones de cupones electrónicos—com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd. Debe añadir este mandato al grupo de recursos que contiene la lista de mandatos que puede ejecutar un Gestor de operaciones.

Identificar la política basada en roles para gestores de operaciones

1. Busque en el apartado de políticas basadas en roles del Apéndice la política basada en roles para Gestores de operaciones. La política es: OperationsManagersExecuteOperations ManagersCmdResourceGroup.

2. Pulse **Gestión de acceso** > **Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. Localice la política en la lista.
5. Anote el nombre de su grupo de recursos— `OperationsManagersCmdResourceGroup`. Este es el nombre del grupo de recursos que debe actualizar.

Actualizar el grupo de recursos de la política basada en roles para incluir el mandato para crear promociones de cupones electrónicos

1. Pulse **Gestión de acceso > Grupos de recursos**.
2. Seleccione **OperationsManagersCmdResourceGroup**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de recursos.
4. Pulse **Siguiente** para visualizar la página Detalles.
5. En la lista Recursos disponibles, seleccione `com.ibm.commerce.tools.ecoupon.ECouponPromotionSaveCmd`. Este es el mandato para crear promociones de cupones electrónicos.
6. Pulse **Añadir**.
7. Pulse **Finalizar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de compras 1: permitir que los jefes de compras gestionen el carro de la compra para los pedidos creados por su organización

Nota: Este escenario no se aplica a WebSphere Commerce Professional Edition.

Por omisión, los jefes de compras tienen autorización para gestionar el carro de la compra cuando han creado el pedido. En algunos casos, es posible que desee ampliar la autorización de los jefes de compras para permitirles que gestionen el carro de la compra de los pedidos creados por los miembros de su organización.

Para realizar este cambio, realice lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que autoriza a los administradores del carro de la compra a gestionar sus carros de la compra.
- Cambie la relación de recursos de esta política de `creador` a `misma entidad de organización que el creador`.

Pasos que debe realizar

Cambiar la relación de recursos para la política a nivel de recursos

1. Vaya al apartado Compras del Apéndice y busque la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de los pedidos. La política es:

ProcurementShoppingCartManagersExecuteProcurementShopping
CartManageOnOrderResource

2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. En la lista de políticas, seleccione lo siguiente:

   ProcurementShoppingCartManagersExecuteProcurementShopping CartManageOnOrderResource
5. Pulse **Cambiar** para visualizar la página Cambiar política.
6. Para Relación, seleccione **sameOrganizationalEntityAsCreator**.
7. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de compras 2: permitir que los administradores de compradores del sistema de compras sometan el carro de la compra de los pedidos creados por su organización

Nota: Este escenario no se aplica a WebSphere Commerce Professional Edition.

Por omisión, los jefes de compras tienen autorización para guardar o someter el carro de la compra si crean ellos el pedido. En algunos casos, es posible que desee dividir la responsabilidad de estas dos tareas. También puede permitir que los jefes de compra puedan guardar los carros de la compra que contienen pedidos creados por ellos pero otorgar a los administradores de compradores de la misma organización que el creador del pedido la autorización para someter el carro de la compra de pedidos. Esto puede resultar útil si desea que el administrador de compradores revise las compras planificadas antes de que se sometan.

Para realizar este cambio, realice lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que autoriza a los administradores del carro de la compra y a los administradores de los centros a gestionar los centros de formalización de pedidos.
- Suprima la acción que permite someter un carro de la compra del grupo de acciones de la política.
- Defina un nuevo grupo de acciones que contenga el mandato para someter un carro de la compra del sistema de compras. Utilizará este grupo de acciones para definir la nueva política a nivel de recursos que autoriza a los administradores de compradores a someter los carros de la compra si están en la misma organización que el creador del pedido.
- Cree una nueva política a nivel de recursos que autorice a los administradores de compradores a someter los carros de la compra si están en la misma organización que el creador del pedido.

Pasos que debe realizar

Identificar el grupo de acciones de la política a nivel de recursos y el grupo de recursos

1. Vaya al apartado Compras del Apéndice y busque la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de los pedidos. La política es:

   ```
   ProcurementShoppingCartManagersExecuteProcurement
   ShoppingCartManageOnOrderResource
   ```

2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. Localice la política en la lista de políticas.
4. Anote el nombre del grupo de acciones— `ProcurementShoppingCartManage`. Actualizará este grupo de acciones para suprimir la acción para someter los carros de la compra.
5. Anote el nombre del grupo de recursos— `OrderDataResourceGroup`. Utilizará este grupo de recursos para definir la nueva política a nivel de recursos.

Actualizar el grupo de acciones de la política a nivel de recursos

1. Pulse **Gestión de acceso > Grupos de acciones**.
2. En la lista de grupos de acciones, seleccione **ProcurementShoppingCartManage**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones.
4. En la lista Acciones seleccionadas, seleccione **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**. Creará un nuevo grupo de acciones con esta acción y utilizará el grupo de acciones de la nueva política a nivel de recursos.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

Definir un grupo de acciones nuevo

1. Pulse **Gestión de acceso > Grupos de acciones**.
2. Pulse **Nuevo** para visualizar la página Nuevo grupo de acciones.
3. En Nombre, especifique `ProcurementShoppingCartSubmit`.
4. Como Nombre de visualización, especifique una breve descripción del grupo de acciones en su idioma local.
5. Como Descripción, especifique una descripción más completa de lo que lleva a cabo la acción, en su idioma local.
6. En la lista Acciones disponibles, seleccione **com.ibm.commerce.me.commands.SubmitShoppingCartCmd**.
7. Pulse **Añadir**.
8. Pulse **Aceptar**.

Definir la nueva política

1. Pulse **Gestión de acceso > Políticas**.
2. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
3. Pulse **Nueva** para que se visualice la página Nueva política.
4. En Nombre, especifique:

   ```
   ProcurementBuyerAdministratorsExecuteProcurementShoppingCartSubmitCommands
   OnOrderResource
   ```

5. Como Nombre de visualización, especifique una breve descripción de la política en su idioma local.
6. Como Descripción, especifique una descripción más completa de lo que lleva a cabo la política, en su idioma local.
7. Para Grupos de usuarios, pulse **Buscar** y seleccione **ProcurementBuyerAdministrators**.
8. Pulse **Aceptar**.
9. Para Grupo de recursos, seleccione **OrderDataResourceGroup**.
10. Para Grupo de acciones, seleccione **ProcurementShoppingCartSubmit**.
11. Para Relación, seleccione **sameOrganizationalEntityAsCreator**.
12. Para Tipo de política, seleccione **Política de plantilla agrupable** para designar la política como una política de plantilla.
13. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con el cambio

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Nota: Después de crear la política nueva, se debe asignar a un grupo de políticas para que entre en vigor. Esto debe realizarse mediante XML. Consulte el Capítulo 13, “Personalización de las políticas de control de acceso mediante XML”, en la página 143 para obtener más información.

Escenario de inventario 1: permitir que los administradores del centro de despacho de pedidos puedan actualizarlos pero no suprimirlos

Por omisión, los administradores del centro de despacho de pedidos tienen autorización para actualizar o suprimir los centros de despacho de pedidos asociados a la tienda. En algunos casos, es posible que desee que los administradores de los centros de formalización de pedidos puedan actualizar los centros de formalización de pedidos pero no suprimirlos.

Para realizar este cambio, realice lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que autoriza a los administradores de los centros de formalización de pedidos a gestionar los centros de formalización de pedidos.
- Suprima la acción que permite suprimir un centro de despacho de pedidos del grupo de acciones de la política.

Pasos que debe realizar

Suprimir la acción para suprimir un centro de despacho de pedidos

1. Vaya al apartado Compras del Apéndice y busque la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de los pedidos. La política es:

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenter
   ManageCommandsOnFulfillmentResource
   ```

2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. Localice la política en la lista de políticas.
4. Anote el nombre del grupo de acciones— `FulfillmentCenterManage`. Deberá Actualizar este grupo de acciones para suprimir la acción de suprimir los centros de formalización de pedidos.
5. Pulse **Gestión de acceso > Grupos de acciones**.
6. En la lista de grupos de acciones, seleccione **FulfillmentCenterManage**.
7. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones.
8. En la lista Acciones seleccionadas, seleccione **com.ibm.commerce.inventory.commands.FulfillmentCenterDeleteCmd**.
9. Pulse **Eliminar**.
10. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de inventario 2: permitir que solamente los directores de logística, los directores de operaciones y los representantes de cuentas puedan crear, actualizar o suprimir los centros de despacho de pedidos

Por omisión, los administradores del centro de despacho pedidos tienen autorización para crear, actualizar o suprimir los centros de formalización de pedidos asociados a la tienda. El grupo de acceso del centro de despacho de pedidos incluye los roles: Vendedor, Director de logística, Director de operaciones y Representante de cuentas. Es posible que en algunos casos desee que los vendedores no tengan autorización para ser administradores del centro de despacho de pedidos.

Para realizar este cambio, realice lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que autoriza a los administradores de los centros de formalización de pedidos a gestionar los centros de formalización de pedidos.
- Suprima el rol de vendedor de la definición del grupo de acceso de `administradores del centro de despacho de pedidos`.

Pasos que debe realizar

Suprimir el rol de vendedor del grupo de acceso

1. Vaya al apartado Compras del Apéndice y busque la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de los pedidos. La política es:

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage
   CommandsOnFulfillmentResource
   ```

2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Grupos de acceso**.

3. En la lista de grupos de acceso, seleccione **FulfillmentCenterManagersForOrg**.
4. Pulse **Cambiar** para visualizar la página Cambiar grupo de acceso.
5. Pulse **Gestión de acceso > Grupos de acceso**.
6. Pulse **Cambiar** para visualizar la página Detalles.
7. Pulse **Criterios** para visualizar la página Criterios.
8. En la lista Rol, seleccione **Vendedor**.
9. Pulse **Eliminar**.
10. Pulse **Aceptar**.

Actualizar el registro de políticas de control de acceso con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Escenario de Business intelligence 1: permitir que los auditores vean los informes de business intelligence

Por omisión, los que pueden visualizar los informes de business intelligence pueden ver este tipo de informes de su tienda. En algunos casos, es posible que desee crear un nuevo rol denominado `auditor` y autorizar a los usuarios que posean este rol a visualizar los informes de business intelligence de una tienda.

A continuación se muestra una visión general de los pasos que debe realizar:

- Cree un nuevo rol, (`Auditor`) y cree para el mismo un grupo de acceso nuevo `Auditors`, un grupo de recursos nuevos y una política nueva basada en roles.
- Añada un rol al grupo de acceso de la política a nivel de recursos.
- Añada el rol `Auditor` al grupo de acceso de la política a nivel de recursos que define quién puede ver los informes de business intelligence de sus tiendas.

En este escenario, realice lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que permite ver los informes de business intelligence a los visualizadores de este tipo de informes.
- Anote el nombre de la acción en este grupo de acciones. Debe crear un nuevo grupo de recursos con esta acción y utilizarlo en la política basada en roles para el nuevo rol. Recuerde que en las políticas basadas en roles para acciones, el grupo de acciones contiene una sola acción de ejecución. El grupo de recursos contiene las acciones (mandatos) que se pueden ejecutar.
- Defina un grupo de recursos nuevo llamado `AuditorCommands`, que incluya los mandatos para ver informes de business intelligence. Este grupo de recursos lo utilizará en la política basada en roles para el rol de auditor.
- Defina una política basada en roles nueva para los auditores, que utilizará el grupo de acceso Auditors y el grupo de recursos AuditorCommands.
- Añada el rol de auditor al grupo de acceso de la política a nivel de recursos que define quién puede ver los informes de business intelligence de sus tiendas.

Pasos que debe realizar

Definir el nuevo rol de auditor

1. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Roles**.
2. En la página Roles, pulse **Nuevo**.
3. En Nombre, especifique Auditor.
4. En Descripción, especifique una descripción del rol de auditor en su idioma local.
5. Pulse **Aceptar**.

Definir un nuevo grupo de acceso para el auditor

1. Pulse **Gestión de acceso > Grupos de acceso**.
2. En la página Grupos de acceso, pulse **Nuevo** para visualizar la página Detalles del nuevo grupo de acceso.
3. En Nombre, especifique—Auditors.
4. En Descripción, especifique una descripción del grupo de acceso en su idioma local.
5. En Organización padre, seleccione **Organización raíz**.
6. Pulse **Siguiente** para visualizar la página Criterios del nuevo grupo de acceso.
7. Pulse **Basándose en organizaciones y roles**.
8. En la lista Rol, seleccione **Auditor**.
9. Pulse **Añadir**.
10. Pulse **Terminar**.

Identificar acciones para utilizarlas en el grupo de recursos para la política basada en roles del auditor

1. Vaya al apartado Business Intelligence del Apéndice y busque la política a nivel de recursos que autoriza a los auditores a visualizar informes de business intelligence. La política es:

   ```
   IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport
   CommandsOnStoreEntityResource
   ```

2. En la Consola de administración de organizaciones, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas que posee.
4. Localice la política en la lista.
5. Anote el nombre del grupo de acciones de la política— `ViewBusinessIntelligenceReport`. Este es el grupo de acciones que debe visualizar para identificar las acciones para registrar miembros.
6. Pulse **Gestión de acceso > Grupos de acciones**.
7. En la lista de grupos de acciones, seleccione **ViewBusinessIntelligenceReport**.
8. Pulse **Cambiar** para visualizar la página Cambiar grupo de acciones.
9. Anote el nombre del mandato para visualizar informes de business intelligence—`com.ibm.commerce.bi.commands.BIShowReportCmd`.

Definir el nuevo grupo de recursos que se ha de utilizar en la política basada en roles para el rol de auditor

1. Pulse **Gestión de acceso > Grupo de recursos** para visualizar la página Grupo de recursos.

2. Pulse **Nuevo** para visualizar la página General para el nuevo grupo de recursos.
3. En **Nombre**, especifique AuditorCommands.
4. Como **Nombre de visualización**, especifique una descripción del grupo de recursos en el idioma local.
5. Como **Descripción**, especifique una descripción más completa del grupo de recursos en su idioma local.
6. Pulse **Siguiente**.
7. En Tipo, seleccione **Grupo de recursos explícitos**.
8. Pulse **Siguiente** para visualizar la página Detalles del nuevo grupo de recursos.
9. En la lista Recursos disponibles, seleccione **com.ibm.commerce.bi.commands.BIShowReportCmd**.
10. Pulse **Añadir**.
11. Pulse **Terminar**.

Definir la política basada en roles para el rol de auditor

1. Pulse **Gestión de acceso > Políticas**.
2. En la página Políticas, pulse **Nueva**.
3. En Nombre, especifique **AuditorsExecuteAuditorCommands**.
4. Como Nombre de visualización, especifique una breve descripción de la política en su idioma local.
5. Como Descripción, especifique una descripción más completa de lo que lleva a cabo la política, en su idioma local.
6. Para Grupo de usuarios, pulse **Buscar** y seleccione **Auditors**.
7. Pulse **Aceptar**.
8. Para Grupo de recursos, seleccione **AuditorCommands**.
9. Para Grupo de acciones, seleccione **ExecuteCommandActionGroup**.
10. Pulse **Aceptar**.

Añadir el rol de auditor al grupo de acceso de la política a nivel de recursos

1. Pulse **Gestión de acceso > Grupos de acceso.**
2. En la lista de grupos de accesos, seleccione **IntelligenceReportViewersForOrg**.
3. Pulse **Cambiar** para visualizar la página Cambiar grupo de acceso.
4. Pulse **Criterios** para visualizar la página Criterios del grupo de acceso.
5. En la lista Rol, seleccione **Auditor**.
6. Pulse **Para organización** para especificar que el rol debe desempeñarse en la propia organización del recurso o en sus antecesoras.
7. Pulse **Añadir**.
8. Pulse **Aceptar**.

Actualizar el registro de políticas con los cambios

1. Conéctese a la consola de administración.
2. Pulse **Configuración > Registro**.
3. En la lista de registros, seleccione **Políticas de control de acceso**.
4. Pulse **Actualizar**.

Capítulo 13. Personalización de las políticas de control de acceso mediante XML

La Consola de administración de WebSphere Commerce permite realizar cambios sencillos para acceder a las políticas de control de acceso y a sus componentes. Para realizar cambios más sofisticados, debe editar los archivos XML directamente y luego cargarlos en la base de datos.

Antes de comenzar a realizar los cambios en los archivos XML para modificar el control de acceso, debe leer el capítulo sobre control de acceso de la publicación *WebSphere Commerce, Guías de programación y aprendizaje*. Este capítulo proporciona una visión general técnica del control de acceso y describe cómo crear mandatos personalizados, beans de entidad y plantillas JSP que se pueden proteger mediante las políticas de control de acceso.

Cuando haya finalizado la personalización del código siguiendo las indicaciones que se proporcionan en la publicación *WebSphere Commerce, Guías de programación y aprendizaje*, puede editar los archivos XML de control de acceso para establecer las protecciones que necesita.

Cambios que sólo pueden realizarse editando y cargando los archivos XML

Los cambios siguientes solamente pueden realizarse editando y cargando los archivos XML adecuados:

- Crear o modificar una acción
- Crear o modificar una relación
- Crear o modificar un grupo de relaciones
- Crear o modificar un recurso
- Crear o modificar atributos
- Crear o modificar grupos de acceso utilizando criterios complejos
- Crear o modificar grupos de recursos utilizando criterios complejos
- Crear una política basada en roles para vistas
- Cambiar el grupo de acciones en una política basada en roles para vistas
- Crear o modificar un grupo de políticas
- Asociar políticas a grupos de políticas

Acerca de los archivos XML para el control de acceso

En la tabla siguiente se muestran los nombres y las descripciones de archivos XML, archivos DTD de WebSphere Commerce y archivos XSL para XML Transformer:

Tabla 12. Archivos XML de WebSphere Commerce para el control de acceso

Nombre de archivo	Descripción
ACUserGroups_de_DE.xml ACUserGroups_en_US.xml ACUserGroups_es_ES.xml ACUserGroups_fr_FR.xml ACUserGroups_it_IT.xml ACUserGroups_ja_JP.xml ACUserGroups_ko_KR.xml ACUserGroups_pt_BR.xml ACUserGroups_zh_CN.xml ACUserGroups_zh_TW.xml	Definiciones de grupos de acceso y descripciones en cada uno de los idiomas soportados.
defaultAccessControlPolicies.xml	Archivo principal que contiene las definiciones de las políticas de control de acceso, grupos de acciones, grupos de recursos, relaciones, grupos de relaciones, acciones, categorías de recursos y atributos por omisión.
defaultAccessControlPolicies_de_DE.xml defaultAccessControlPolicies_en_US.xml defaultAccessControlPolicies_es_ES.xml defaultAccessControlPolicies_fr_FR.xml defaultAccessControlPolicies_it_IT.xml defaultAccessControlPolicies_ja_JP.xml defaultAccessControlPolicies_ko_KR.xml defaultAccessControlPolicies_pt_BR.xml defaultAccessControlPolicies_zh_CN.xml defaultAccessControlPolicies_zh_TW.xml	Archivos que contienen los nombres de visualización y las descripciones de las políticas de control de acceso, grupos de acciones, acciones, grupos de recursos, relaciones y atributos por omisión en cada idioma soportado.
ACPoliciesfilter.xml	Archivo de filtro que se utiliza para extraer de la base de datos toda la información de control de acceso.
OrganizationPoliciesFilter.xml	Archivo de filtro que se utiliza para extraer toda la información de control de acceso relacionada con las políticas propiedad de una organización específica.
ACUserGroupsFilter.xml	Archivo de filtro que se utiliza para extraer toda la información de grupo de acceso.

Tabla 12. Archivos XML de WebSphere Commerce para el control de acceso (continuación)

Nombre de archivo	Descripción
accesscontrolpolicies.dtd	El archivo XML de políticas de control de acceso se debe ajustar a esta DTD.
accesscontrolpoliciesnls.dtd	El archivo XML específico de idioma nacional (NLS) de las políticas de control de acceso, sólo para descripciones y nombres de visualización se debe ajustar a esta DTD.
ACUserGroups_es_ES.dtd	El archivo XML de grupos de usuarios de control de acceso se debe ajustar a esta DTD.
accesscontrol.xsl	El archivo XSL de normas de transformación para políticas de control de acceso se debe ajustar a este archivo XML.
accesscontrolnls.xsl	El archivo XSL de normas de transformación para el archivo XML de NLS de políticas de control de acceso (sólo para descripciones y nombres de visualización).
ACUserGroup.xsl	El archivo XSL de normas de transformación para archivos XML de grupos de acceso.
wcstoacpolicies.xsl	El archivo de normas de transformación XSL para el archivo ExtractedACPolicies.xml después de la extracción, para crear el archivo XML de políticas de control de acceso.
wcstoacpoliciesnls.xsl	El archivo de normas de transformación XSL para ExtractedACPolicies.xml después de la extracción, para crear el archivo XML de NLS de políticas de control de acceso.
wcstoacusergroup.xsl	El archivo de normas de transformación XSL para el archivo ExtractedACPolicies.xml después de la extracción, para crear el archivo XML de grupos de acceso.

Modificación de archivos XML

Puede manipular los archivos XML de modo que efectúen las siguientes tareas de autorización:

- Proteger vistas
- Proteger mandatos de controlador
- Implementar el control de acceso a nivel de recursos
- Proteger beans de datos
- Agrupar recursos por atributos

- Definir relaciones
- Definir grupos de relaciones

Protección de vistas

Cualquier vista que se llama directamente desde un URL o que se ha iniciado como una redirección desde otro mandato, necesita una política de control de acceso basada en roles para poder visualizarla. El ejemplo siguiente muestra una política basada en roles para las vistas:

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

El nombre de ResourceGroup, `ViewCommandResourceGroup`, indica que es una política basada en roles para vistas. La política indica que los usuarios del grupo de usuarios `ProductManagers` pueden visualizar las vistas del grupo de acciones `ProductMangersViews`. Del mismo modo, en la mayor parte de los roles existe un grupo de acciones correspondiente que agrupa las vistas a las que puede acceder dicho rol, por ejemplo, Rol de `Vendedor` -> `Vendedores` grupo de acceso -> grupo de acciones `Vistas de vendedores`.

A continuación se muestra un ejemplo del grupo de acciones `ProductMangersViews`:

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

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

 </ActionGoup>
```

El ejemplo anterior muestra tres acciones, `ProductImageView`, `ProductManufacturerView` y `ProductSalesTaxView` en el grupo de acciones `ProductManagerViews`.

A continuación se muestra un ejemplo de definición de la acción `ProductImageView`:

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

El atributo `Name`, `ProductImageView`, se utiliza como un código para hacer referencia a la acción en cualquier lugar del archivo XML como, por ejemplo, cuando se asocia la acción a un grupo de acciones.

Nota: El nombre de la vista, almacenado en la columna `VIEWNAME` de la tabla `VIEWREG`, debe coincidir con el nombre de `CommandName` en la definición de acción. El valor de `CommandName` se almacena en la columna ACTION de la tabla `ACACTION`. `Name` y `CommandName` no han de ser necesariamente iguales.

Añadir una vista nueva mediante las políticas existentes

Para añadir una vista nueva a la que se pueda acceder mediante roles con políticas de Vista basadas en roles, cree un archivo XML similar al que se muestra y, a continuación, efectúe lo siguiente:

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

<Policies>

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

  <ActionGroup Name="ProductManagersViews" OwnerID="RootOrganization">
              <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>

 </Policies>
```

1. Cree una nueva definición de acción en el archivo XML cuyo nombre de vista es *MyNewView*. Este nombre puede cambiarlo por uno de su elección.

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

2. Determine los roles que deben tener acceso a esta vista y asocie la nueva acción a los grupos de acciones correspondientes del archivo XML, como en el ejemplo siguiente:

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

     <ActionGroupAction Name="MyNewView"/>

    </ActionGroup>
   ```

   Ya existe una política basada en roles, `ProductManagersExecuteProductManagersViews`, que incluye este grupo de acciones, por lo tanto, no es necesario crear una política nueva. Asimismo, las políticas basadas en roles por omisión pertenecen al grupo de políticas `ManagementAndAdministrationPolicyGroup` que se aplica a la mayor parte, si no a todas, las organizaciones del sitio, por lo tanto, no es necesario realizar más suscripciones al grupo de políticas.

3. Cargue los cambios XML en la base de datos. Para obtener más información sobre cómo cargar los cambios XML, consulte el apartado “Cargar los cambios en la base de datos” en la página 177.

4. En la Consola de administración, actualice el registro de políticas de control de acceso, realizando lo siguiente:
   a. Inicie la consola de administración como administrador del sitio.
   b. Pulse **Configuración** > **Registro**.
   c. En la lista de registros, seleccione **Políticas de control de acceso**.
   d. Pulse **Actualizar**.

Añadir una vista nueva mediante una política nueva

Para añadir una vista nueva a la que se pueda acceder con un rol nuevo que no tenga una política basada en roles actualmente, cree un archivo XML similar al que se muestra y, a continuación, efectúe lo siguiente:

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

<Policies>

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

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

```
            <ActionGroupAction Name="MyNewView"/>
 </ActionGroup>

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

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

 </Policies>
```

1. Cree una nueva definición de acción en el archivo XML cuyo nombre de vista es *MyNewView*. Este nombre puede cambiarlo por uno de su elección.

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

2. Cree un nuevo grupo de acciones que se asociará al nuevo rol:

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

   Donde *XYZViews* es el nombre del grupo de acciones. El valor de OwnerID para grupos de acciones debe ser siempre RootOrganization.

3. Asocie la nueva acción al nuevo grupo de acciones:

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

    <ActionGroupAction Name="MyNewView"/>

   </ActionGroup>
   ```

   Donde *XYZViews* es el grupo de acciones y *MyNewView* es la acción que ha creado.

4. Cree una política que haga referencia al nuevo grupo de acciones:

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

   Donde *XYZExecuteXYZViews* es el nombre de política y *XYZViews* es el grupo de acciones. En WebSphere Commerce 5.5, debido al modelo de suscripción a políticas, no se utiliza el valor de OwnerID para las políticas de plantilla agrupables y estándar agrupables, para determinar a qué recursos se aplicará una política. El valor de OwnerID actualmente sólo lo utiliza la consola de administración cuando la organización (propietario) visualiza las políticas. Si una política se ha de aplicar a varias organizaciones, se le recomienda que se establezca el valor de OwnerID en la organización ancestro común como, por ejemplo, organización raíz. Si una política se ha de aplicar solamente a una organización específica, se le recomienda que establezca el valor de OwnerID en el `orgentity_id` de dicha organización.

5. Incluye la política nueva del grupo de políticas adecuada. Por omisión, la mayor parte de las políticas basadas en roles se colocan en ManagementAndAdministrationPolicyGroup, lo que debe aplicarse a todas las organizaciones.

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

   Donde el valor de `PolicyOwnerId` debe ser el mismo que el valor de `OwnerID` utilizado en la definición de políticas.
6. Cargue los cambios XML en la base de datos. Para obtener más información sobre cómo cargar los cambios XML, consulte el apartado "Cargar los cambios en la base de datos" en la página 177.
7. En la Consola de administración, actualice el registro de políticas de control de acceso, realizando lo siguiente:
   a. Inicie la consola de administración como administrador del sitio.
   b. Pulse **Configuración** > **Registro**.
   c. En la lista de registros, seleccione **Políticas de control de acceso**.
   d. Pulse **Actualizar**.

Ahora puede utilizar la vista.

Protección de los mandatos del controlador

Para poder ejecutar los mandatos de controlador es necesaria una política de control de acceso basada en roles. Un mandato de controlador o de tarea también requiere una política a nivel de recursos si el mandato está realizando la comprobación a nivel de recursos. Para obtener más información, consulte el apartado "Protección de recursos" en la página 156. El ejemplo siguiente muestra una política basada en roles para los mandatos de controlador:

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

El nombre de ActionGroupName, `ExecuteCommandActionGroup`, indica que se trata de una política basada en roles para mandatos de controlador. La política indica que los usuarios del grupo `Sellers` pueden ejecutar los mandatos del grupo de recursos `SellersCmdResourceGroup`.

A continuación se muestra un ejemplo de la definición de grupo `SellersCmdResourceGroup`:

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

El ejemplo anterior muestra los tres recursos siguientes del grupo de recursos que responden a los mandatos de controlador:

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

A continuación se muestra una definición de un recurso de ejemplo:

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

<ResourceAction Name="ExecuteCommand"/>

 </ResourceCategory>
```

El atributo de Name, com.ibm.commerce.contract.commands.ContractCloseCmdResourceCategory, se utiliza como un código para hacer referencia al recurso en el archivo XML. El nombre de ResourceActionName, ExecuteCommand, se utiliza para especificar las acciones que pueden realizarse en el recurso. Esta información se utiliza en la Consola de administración cuando se utilizan políticas de control de acceso para rellenar el recuadro de selección Acción correspondiente a un recurso determinado. En este caso, se especifica la acción Execute. La acción Execute se define del modo siguiente:

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

Nota: El nombre de interfaz del mandato de controlador debe coincidir con la clase ResourceBeanClass en la definición del recurso. El valor de ResourceBeanClass se almacena en la columna RESCLASSNAME de la tabla ACRESCGRY. Estos mandatos se utilizan como recursos porque amplían la interfaz ControllerCommand, la cual amplía la interfaz AccCommand y ésta, a su vez, amplía la interfaz Protectable. Para obtener más información, consulte la publicación *WebSphere Commerce, Guías de programación y aprendizaje*.

Añadir un mandato de controlador nuevo mediante las políticas existentes

Para añadir un mandato de controlador nuevo al que se pueda acceder mediante un nuevo rol, que tenga una política basada en roles existente, cree un archivo XML similar al siguiente. Después se describen los pasos específicos.

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

<Policies>

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

  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

<ResourceGroup Name="SellersCmdResourceGroup" OwnerID="RootOrganization">
    ResourceGroupResource Name="com.xyz.commands.MyNewControllerCmdResource
    Category"/>
 </ResourceGroup>

 </Policies>
```

1. Cree una nueva definición de recurso en el archivo XML que se corresponde con el nombre de la interfaz del mandato del controlador.

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

  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>
```

2. Determine los roles que deben tener acceso al mandato y asocie el nuevo recurso a los grupos de recursos correspondientes del archivo XML, como en el ejemplo siguiente:

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

 </ResourceGroup>
```

   Puede modificar el grupo de recursos dependiendo del rol que desea utilizar. Para obtener más información acerca de las políticas basadas en roles, consulte el apartado "Políticas basadas en roles" en la página 218.
3. Cargue los cambios XML en la base de datos. Para obtener más información sobre cómo cargar los cambios XML, consulte el apartado "Cargar los cambios en la base de datos" en la página 177.
4. En la Consola de administración, actualice el registro de políticas de control de acceso, realizando lo siguiente:
   a. Inicie la consola de administración como administrador del sitio.
   b. Pulse **Configuración** > **Registro**.
   c. En la lista de registros, seleccione **Políticas de control de acceso**.
   d. Pulse **Actualizar**.

Dado que ya existe una política basada en roles que incluye este grupo de recursos, ahora puede utilizarse el nuevo mandato de controlador, si no está realizando la comprobación a nivel de recursos. Para obtener información sobre la comprobación a nivel de recursos y los mandatos, consulte el apartado "Modificación del control de acceso a nivel de recursos de una política existente" en la página 154.

Añadir un mandato de controlador nuevo mediante una política nueva

Para añadir un mandato de controlador nuevo al que se pueda acceder mediante un nuevo rol, que no tenga una política basada en roles existente, cree un archivo XML similar al siguiente. Después se describen los pasos específicos.

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

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

  <ResourceAction Name="ExecuteCommand"/>
 </ResourceCategory>

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

    <Policy Name="XYZExecuteXYZsCmdResourceGroup"
   OwnerID="RootOrganization"
UserGroup="XYZ"
   ActionGroupName="ExecuteCommandActionGroup"
```

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

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

</Policies>
```

1. Cree una nueva definición de recurso en el archivo XML que se corresponda con el nombre de la interfaz del mandato de controlador. Puede consultar un ejemplo en el paso uno del apartado "Añadir un mandato de controlador nuevo mediante las políticas existentes" en la página 150.
2. Cree un nuevo grupo de recursos que se asociará al nuevo rol:
   ```
   <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
   </ResourceGroup>
   ```
3. Asocie el nuevo recurso al nuevo grupo de recursos:
   ```
   <ResourceGroup Name="XYZCmdResourceGroup" OwnerID="RootOrganization">
   <ResourceGroupResource Name="com.xyz.commands.MyNewControllerResourceCategory"/>
   </ResourceGroup>
   ```
4. Cree una política que haga referencia al nuevo grupo de recursos:
   ```
   <Policy Name="XYZExecute XYZsCmdResourceGroup"
      OwnerID="RootOrganization"
      UserGroup="XYZ"
      ActionGroupName="ExecuteCommandActionGroup"
      ResourceGroupName="XYZCmdResourceGroup">
      PolicyType="groupableStandard">
   </Policy>
   ```
5. Cargue los cambios XML en la base de datos. Para obtener más información sobre cómo cargar los cambios XML, consulte el apartado "Cargar los cambios en la base de datos" en la página 177.
6. En la Consola de administración, actualice el registro de políticas de control de acceso, realizando lo siguiente:
   a. Inicie la consola de administración como administrador del sitio.
   b. Pulse **Configuración** > **Registro**.
   c. En la lista de registros, seleccione **Políticas de control de acceso**.
   d. Pulse **Actualizar**.

Ahora puede utilizar el mandato de controlador si no está realizando la comprobación a nivel de recursos. Para obtener información sobre la comprobación a nivel de recursos y los mandatos, consulte el apartado "Modificación del control de acceso a nivel de recursos de una política existente" en la página 154.

Modificación del control de acceso a nivel de mandatos para una mandato de controlador

Dependiendo de las políticas de control de acceso, el mandato `UserRegistrationAdminAddCmd` no lo pueden ejecutar los usuarios cuyo rol sea únicamente el de Jefe de Marketing. El escenario siguiente describe los pasos necesarios para modificar las políticas existentes de modo que los usuarios puedan ejecutar este mandato. Puede utilizar los pasos de este escenario y personalizarlos según sus propios requisitos.

Todos los mandatos de controlador requieren una política de control de acceso a nivel de mandatos, con esta definición: `ActionGroupName =`

ExecuteCommandActionGroup. Asimismo debe tener un grupo de recursos que incluya el nombre de interfaz del mandato de controlador. Generalmente estas políticas hacen referencia a un rol específico, por ejemplo, MarketingManagersExecuteMarketingManagerCmdResourceGroup.

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

</Policy>
```

Nota: La política anterior es una de las políticas por omisión que se cargan en la base de datos durante la creación de instancias. Para obtener más información sobre las políticas por omisión, consulte "Políticas y grupos de control de acceso por omisión", en la página 217.

En este caso, si desea que los usuarios con el rol de Jefe de marketing puedan ejecutar UserRegistrationAdminAddCmd, tiene que añadir este mandato al grupo de recursos existente que se utiliza en la política creando su propio archivo XML y realizar las tareas siguientes:

1. Redefinir la acción ExecuteCommand
2. Redefinir com.ibm.commerce.usermanagement.commands.UserRegistrationAddCmd como registro de recursos.
3. Asociar la categoría de recursos al grupo de recursos correspondiente, en este caso, MarketingManagerCmdResourceGroup.
4. Copiar el archivo XML en el directorio *dir_instalación_WC*/xml/policies/xml. El XML resultante será similar al ejemplo siguiente:

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


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

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

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

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

 </Policies>
```

5. Cargue el archivo XML en la base de datos utilizando el script *dir_instalación_WC*/bin/acpload. Para obtener más información sobre cómo cargar archivos XML, consulte "Cargar los cambios en la base de datos" en la página 177.
6. En la consola de administración de WebSphere Commerce actualice el registro de políticas de control de acceso, realizando lo siguiente:
   a. Inicie la consola de administración como administrador del sitio.
   b. Pulse **Configuración** > **Registro**.
   c. En la lista de registros, seleccione **Políticas de control de acceso**.

d. Pulse **Actualizar**.

Ahora puede utilizar el mandato de controlador si no está realizando la comprobación a nivel de recursos. Si está realizando la comprobación a nivel de recursos, consulte el apartado "Modificación del control de acceso a nivel de recursos de una política existente".

Modificación del control de acceso a nivel de recursos de una política existente: Los mandatos que requieren control de acceso a nivel de recursos devuelven los recursos protegidos a los que van a acceder en el método `getResources()`. Esto hace que la infraestructura de control de acceso de WebSphere Commerce active una comprobación de control de acceso a nivel de recursos. WebSphere Commerce buscará en el sistema una política de control de acceso con un Grupo de acciones que contenga la acción igual al mandato actual. En este ejemplo `com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd`. El grupo de recursos de la política también debe incluir el recurso devuelto en el método `getResources()`. En este caso, el mandato `UserRegistrationAdminAddCmd` implementa el método `getResources()` y devuelve la organización en la que se va a registrar el usuario nuevo.

En `defaultAccessControlPolicies.xml` `com.ibm.commerce.usermanagement.commands.UserRegistrationAdminAddCmd` ya figura definida previamente como una acción:

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

También se incluye en un grupo de acciones definido en el archivo XML `defaultAccessControlPolicies.xml`:

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

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

Este grupo de acciones ya se ha utilizado en la política de rutina de carga existente:

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

</Policy>
```

Nota: Muchas políticas son políticas por omisión y se cargan en la base de datos durante la creación de instancias. Para obtener más información sobre las políticas por omisión, consulte "Políticas y grupos de control de acceso por omisión", en la página 217.

Para añadir el rol necesario a `UserRegistrationAdminAddCmd`, haga lo siguiente:

1. Añada el rol necesario al grupo de acceso que utiliza la política. En este ejemplo, `MembershipAdministratorsForOrg`.

   Este grupo de acceso se ha definido en el directorio *`dir_instalación_WC`*`/xml/policies/xml/ACUserGroup_en_US.xml` del modo siguiente:

```
<UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
   Description="Administradores de miembros de la organización" MemberGroupID="-97"

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

En el XML anterior, se incluyen usuarios que tienen como mínimo uno de los roles especificados, Administrador de compradores o Administrador de vendedores para una organización que es predecesora del propietario del recurso (organización) que ha devuelto `getResources()`. Si era su deseo añadir el rol de Director de marketing, debería haberlo ampliado de modo que incluyese el rol nuevo.

2. Copie el archivo XML en el directorio *dir_instalación_WC*/xml/policies/xml. El XML resultante será similar al ejemplo siguiente:

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

<UserGroups>

<UserGroup Name="MembershipAdministratorsForOrg" OwnerID="RootOrganization"
    Description="Administradores de miembros de la organización" MemberGroupID="-97">

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

</UserGroups>
```

3. Cargue el archivo XML en la base de datos utilizando el script *dir_instalación_WC*/bin/acpload. Para obtener más información sobre cómo cargar archivos XML, consulte “Cargar los cambios en la base de datos” en la página 177.
4. En la consola de administración de WebSphere Commerce actualice el registro de políticas de control de acceso, realizando lo siguiente:
   a. Inicie la consola de administración como administrador del sitio.

b. Pulse **Configuración** > **Registro**.
c. En la lista de registros, seleccione **Políticas de control de acceso**.
d. Pulse **Actualizar**.

Protección de recursos

Puede añadir control de acceso a nivel de recursos a los mandatos de controlador o de tareas. La comprobación a nivel de recursos se realiza durante la ejecución de WebSphere Commerce, basándose en los datos que devuelve el método `getResources()` de un mandato. La comprobación a nivel de recursos también se puede realizar durante la parte de ejecución del mandato correspondiente a `performExcecute()`, realizando llamadas directas al gestor de políticas de control de acceso mediante el método `checkIsAllowed(Object resource, String action) throws ECException`. Este método generará `ECApplicationException` si el usuario actual no tiene permiso para realizar la acción especificada en el recurso especificado.

Nota: Por omisión, el método `getResources()` devuelve un valor nulo y no se lleva a cabo ninguna comprobación a nivel recursos.

Debe crear una política a nivel de recursos para mandatos nuevos en los casos siguientes:

- El mandato nuevo es una extensión de un mandato WebSphere Commerce básico que realiza una comprobación a nivel de recursos pero el mandato nuevo implementa una interfaz diferente a la del mandato básico.
- El mandato nuevo propiamente dicho realiza la comprobación de control de acceso a nivel de recursos.

A continuación se muestra un ejemplo de una política a nivel de recursos:

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

Donde:

`Name`: el nombre de la política.

`PolicyType`: el tipo de política. Es una política de plantilla agrupable que se aplicará dinámicamente a la entidad de organización que es la propietaria del recurso y sus antecesores.

`OwnerID`. el miembro que posee la política.

`UserGroup`: la política se aplica a los usuarios de este grupo. El convenio de denominación para grupos de acceso en los que los roles adoptan dinámicamente el ámbito de la organización propietaria del recurso es añadir `ForOrg` al nombre del grupo.

`ActionGroupName`: el nombre del grupo de acciones que contiene las acciones que se han de realizar en el recurso.

ResourceGroupName: el nombre del grupo de acciones que contiene los recursos en los que se han de llevar a cabo acciones.

En el ejemplo anterior, el grupo de acciones ContractManage es el grupo de acciones que contiene el conjunto de mandatos que realizará las acciones en ContractDataResourceGroup. A continuación se muestra un ejemplo del grupo de acciones que se utiliza en la política a nivel de recursos anterior:

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

Los mandatos que anteriormente se habían definido como recursos para políticas basadas en roles se definen ahora como acciones. A continuación se muestra una definición de ejemplo de una acción que forma parte del grupo ContractManage anterior:

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

Nota: El valor de CommandName debe corresponderse con el nombre de la interfaz del mandato que está realizando la comprobación a nivel de recursos.

La mayor parte de los mandatos funcionan con beans enterprise. Estos beans suelen ser recursos que protegen las políticas a nivel de recursos. A continuación se muestra una definición de ejemplo del grupo de recursos que se utiliza en la política de recurso anterior:

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

En este ejemplo, se define ContractDataResourceGroup que consta de un recurso. El recurso se define del modo siguiente:

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

Donde:

Name: un código que se utiliza para hacer referencia a este recurso en otro lugar del archivo XML.

ResourceBeanClass: la clase que representa el recurso que se ha de proteger. Esta clase debe implementar la interfaz Protectable. Si el recurso es un bean enterprise, su interfaz remota debe ampliar la interfaz Protectable.

ResourceAction: especifica las acciones que se realizarán en este recurso. Esta información la utiliza la Consola de administración cuando determina las acciones que son válidas con un recurso específico.

Nota: Para obtener más información sobre la interfaz Protectable, consulte la publicación *WebSphere Commerce, Guías de programación y aprendizaje*.

Protección de los beans de datos

Los beans de datos contienen información acerca de los objetos de negocio y se utilizan para visualizar información acerca de los objetos de una página Web. Las páginas Web dinámicas suelen correlacionarse con vistas de WebSphere Commerce y estas vistas están protegidas mediante políticas basadas en roles. A veces, es necesario proteger adicionalmente el contenido de la página Web protegiendo sus beans de datos, si los hay.

Cuando se cumplimentan los beans de datos con el método `DataBeanManager.activate(..)`, los gestores de beans de datos aplican en los mismos el control de acceso. Los beans de datos se pueden proteger directa o indirectamente, mediante la interfaz Delegator. Los beans de datos protegidos directamente implementan también la interfaz Protectable. Si un bean de datos protegido directamente no implementa la interfaz Delegator, o devuelve un valor nulo para el método `getDelegate()`, significa que no está protegido y cualquiera puede visualizarlo.

Nota: Para obtener más información sobre la interfaz Protectable consulte la publicación *WebSphere Commerce, Guías de programación y aprendizaje*.

A continuación se muestra un ejemplo de una política a nivel de recursos para un bean de datos:

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

El valor de ActionGroupName, `DisplayDataBeanActionGroup`, indica que esta es una política para beans de datos. Este grupo de acciones incluye una acción `Display`.

Donde:

`Name`: el nombre de la política.

`UserGroup`: el grupo de acceso que contiene los usuarios a los que se aplica la política. En este caso, se incluyen todos los usuarios.

`ActionGroupName`: el valor de `DisplayDataBeanActionGroup` indica que se trata de una política a nivel de recursos para beans de datos.

`ResourceGroupName`: el nombre del grupo de recursos que contiene los beans de datos que se han de proteger.

`RelationName`: la relación que se debe cumplir entre un usuario y el recurso. En este caso, el usuario debe ser el creador del recurso de negocio `Order`.

`OrderDataBeanResourceGroup` se define del modo siguiente:

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

OrderDataBeanResourceGroup consta de dos recursos. A continuación se muestra una definición de un recurso de ejemplo para un bean de datos:

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

Donde:

Name: un código que se utiliza para hacer referencia a este recurso en el archivo XML.

ResourceBeanClass: el nombre de clase del bean de datos que se está protegiendo directamente. Esta clase debe implementar la interfaz Protectable.

ResourceAction: un elemento necesario para editar políticas en la Consola de administración. En este caso este elemento indica que Display es la acción válida que puede realizarse en este recurso.

Agrupación de recursos por atributos

Los grupos de recursos se pueden definir totalmente utilizando la columna CONDITIONS de la tabla ACRESGRP. La columna CONDITIONS almacena el documento XML que contiene las limitaciones y las parejas de atributo y valor que se utilizan para agrupar recursos. Este tipo de grupo de recursos se denomina grupo de recursos implícito y, generalmente, se utiliza cuando el nombre de clase del recurso resulta insuficiente. Por ejemplo, si una política de control de acceso se aplica a los recursos Order que tienen un estado igual a P (pendiente) o E (editado por un representante del servicio al cliente), se puede definir un grupo de recursos para la misma.

Nota: Para poder agrupar recursos por atributos que no sean el nombre de clase, el recurso debe implementar la interfaz Groupable. Para obtener más información sobre la interfaz Groupable, consulte la publicación *WebSphere Commerce, Guías de programación y aprendizaje*.

A continuación se muestra un ejemplo del grupo de recursos Order:

```
<ResourceGroup  Name="OrderResourceGroupwithPEStatus"
   OwnerID="RootOrganization">
  <ResourceCondition>
  <![CDATA[
  <profile>
     <andListCondition>
   <orListCondition>
  <simpleCondition>
         <variable name="Status"/>
         <operator name="="/>
         <value data="P"/>
  </simpleCondition>
  <simpleCondition>
         <variable name="Status"/>
         <operator name="="/>
         <value data="E"/>
  </simpleCondition>
```

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

</ResourceGroup>
```

Donde:

Name: el nombre del grupo de recursos que se almacena en la columna GRPNAME de la tabla ACRESGRP.

OwnerID: el propietario del grupo de recursos. Debe ser la organización raíz.

<ResourceCondition>: especifica los datos que se cargarán en la columna CONDITIONS de la tabla ACRESGRP, para definir el grupo de recursos.

<![CDATA[...]]>: indica una sección de los datos de caracteres que se utilizan tal y como se han escrito.

<profile>: un parámetro necesario para todas las condiciones de los recursos.

Un componente esencial de la definición del grupo de recursos es el elemento <simpleCondition> que tiene definido name="classname". Este elemento identifica la clase java del recurso al que se aplica el grupo. La clase java, com.ibm.commerce.order.objects.Order, puede verse en el ejemplo siguiente:

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

El ejemplo siguiente especifica la condición en el recurso com.ibm.commerce.objects.order.objects.Order, es decir, que el estado debe ser igual a P.

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

En el ejemplo anterior, <variable name="*valor*"/> representa los nombres de atributos que reconoce el método getGroupingAttributeValue (String attributeName, GroupContext context)() en el recurso. Este método forma parte de la interfaz Groupable. Para fines de gestión de grupos de recursos implícitos en la Consola de administración de WebSphere Commerce, el atributo también debe definirse en la tabla ACATTR y debe asociarse con el recurso de la tabla ACRESATREL. Cuando llegue el momento de buscar políticas aplicables para un recurso y una acción determinados, esta condición se comprobará llamando al método getGroupingAttributeValue(..), que en este caso pasa Status como el parámetro attributeName.

<orListCondition>, especifica que las condiciones de este bloque deben aplicarse utilizando un valor booleano OR. En este caso, el estado es P o E.
<andListConditon>, especifica que las condiciones de este bloque deben aplicarse utilizando un valor booleano AND. En este caso, (Classname = com.ibm.commerce.order.objects.Order) AND (Status = P OR Status=E).

A continuación, se muestra una definición de atributo de ejemplo para rellenar la tabla ACATTR.

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

El elemento Name es un término que identifica el atributo y el elemento Type identifica el tipo de datos del atributo. Los valores posibles del atributo son:

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

La asociación de un atributo con un recurso se especifica en la definición del recurso. Por ejemplo, en el siguiente ejemplo se asocia el atributo Status con OrderResourceCategory:

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

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

Donde:

<ResourceAttributes>: un bloque de código que asocia un atributo con un recurso.

AttributeTableName: el nombre de la tabla de base de datos del recurso.

AttributeColumnName: el nombre de la columna de la tabla de recursos que almacena el atributo.

ResourceKeyColumnName: el nombre de la columna de la tabla de recursos que almacena la clave primaria.

Definición de relaciones

Las políticas de control de acceso tienen un elemento de relación opcional. Esta relación solamente se puede crear cargando un archivo de políticas XML con la definición de relación que se muestra a continuación:

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

La entrada Name es el nombre de la relación utilizada en cualquier política y se añade a la tabla ACRELATION. Name corresponde al parámetro de relación del método fulfills() en el recurso protegible.

El ejemplo siguiente visualiza la definición de una relación denominada creator.

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

Definición de grupos de relaciones

Los grupos de relaciones contienen condiciones abiertas que son las condiciones pertenecientes al grupo de relaciones. Si tiene que definir los grupos de relaciones, deberá hacerlo definiendo la información de grupos de relaciones en el archivo XML o modificando el archivo defaultAccessControlPolicies.xml como se indica a continuación:

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

Cadenas de relaciones

Cada grupo de relaciones consta de una o varias condiciones de apertura RELATIONSHIP_CHAIN que se agrupan mediante los elementos andListCondition u orListCondition. Una cadena de relaciones es una serie de una o varias relaciones. La longitud de una cadena de relaciones la determina el número de relaciones del que consta. Esto puede determinarse analizando el número de entradas <parmeter name= "X" value="Y"> de la representación XML de la cadena de relaciones. A continuación se muestra un ejemplo de una cadena de relaciones con una longitud de uno.

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

Donde:

aValue: una serie que representa la relación entre el usuario y el recurso. Esta serie debe ser una de las relaciones comprobadas en el método fulfills del recurso.

Cuando una cadena de relaciones tiene una longitud de dos o más, se trata de una serie de dos relaciones. La primera entrada, <parmeter name= "X" value="Y">, es entre un usuario y una entidad de organización. La segunda entrada, <parameter name= "X" value="Y">, es entre una entidad de organización y el recurso. Las entradas intermedias de la cadena, <parmeter name= "X" value="Y">, son entradas entre organizaciones. A continuación se muestra un ejemplo de una cadena de relaciones con una longitud de dos:

```
<openCondition name=RELATIONSHIP_CHAIN">
<parameter name="valor1" value="valor2"/>
<parameter name="RELATIONSHIP" value="valor3"/>
</openCondition>
```

Donde:

valor1 : los valores posibles incluyen HIERARCHY y ROLE. HIERARCHY especifica que hay una relación jerárquica entre el usuario y la entidad de organización en la jerarquía de miembros. ROLE especifica que el usuario tiene un rol en la entidad de organización. Si el valor de valor1 es HIERARCHY, los valores posibles de valor1 son child, que devuelve una entidad de organización para la que el usuario es un hijo directo en la jerarquía de miembros. Si el valor de valor1 es ROLE, los valores posibles de valor1 son cualquier entrada de la columna NAME de la tabla ROLE, que devuelve todas las entidades de organización para las que el usuario actual tiene este rol.

valor3: una serie que representa la relación entre una o varias entidades de organización que se recuperan a partir de la evaluación del primer parámetro y el recurso. Este valor corresponde al parámetro de relación del método fulfills() del recurso protegible. Si el parámetro de evaluación, valor1 devuelve más de una entidad de organización, esta parte de RELATIONSHIP_CHAIN se satisface si como mínimo una de estas entidades de organización satisface la relación que especifica el parámetro valor2.

Nota: Para obtener más información acerca de cómo definir grupos de relaciones, consulte el apartado "Definición de grupos de relaciones" en la página 162

Definición de grupos de relaciones de una sola cadena

Si como parte de su política de control de acceso ha de imponer que un usuario debe pertenecer a la entidad de organización que es, por ejemplo, la entidad BuyingOrganizationalEntity del recurso, tendrá que crear un grupo de relaciones que conste de una cadena de relaciones con una longitud de dos. Esto se muestra en el ejemplo siguiente:

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

La cadena de relaciones tiene una longitud de dos porque consta de dos relaciones diferentes. La primera relación se produce entre el usuario y la entidad de organización padre. El usuario es el hijo en esta relación. En la segunda relación, el administrador de políticas de control de acceso comprueba si la entidad de organización satisface la relación BuyingOrganizationalEntity con el recurso. En otras palabras, devuelve true si se trata de la entidad de organización compradora del recurso.

Nota: Para obtener información sobre el código openCondition consulte la publicación *WebSphere Commerce Accelerator, Guía de personalización*.

Otro ejemplo sería si tuviera que imponer que el usuario debe tener el rol de representante de cuentas para la entidad de organización que es la entidad de organización compradora del recurso. Una vez más, este ejemplo utiliza el grupo de relaciones que consta de una cadena de relaciones con una longitud de dos. La primera parte de la cadena busca todas las entidades de organización para las que el usuario tiene el rol de representante de cuentas. A continuación, para el conjunto de entidades de organización, el administrador de políticas de control de acceso

comprueba si como mínimo una de ellas satisface la relación BuyingOrganizationalEntity con el recurso. Si es así, se devuelve el valor true.

El ejemplo siguiente muestra cómo se define este tipo de grupo de relaciones:

```
<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>
```

Definición de grupos de relaciones de varias cadenas

Si tiene que crear un grupo de relaciones que contenga una relación de varias cadenas, deberá especificar si el usuario debe satisfacer todas las cadenas de relaciones, lo que significa que se trata de un ejemplo de tipo AND, o si el usuario debe satisfacer como mínimo una de las relaciones de la cadena, lo que significa que se trata de un ejemplo de tipo OR.

En el ejemplo siguiente, el usuario debe ser el creador del recurso y debe pertenecer a la entidad BuyingOrganizationalEntity especificada en el recurso. La primera cadena, que especifica que el usuario debe ser el creador del recurso, tiene una longitud de uno. La segunda cadena, que especifica que el usuario debe pertenecer a la entidad BuyingOrganizationalEntity especificada en el recurso, tiene una longitud de dos.

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

Nota: Si el usuario debe satisfacer una de las dos cadenas de relaciones, debe modificar el código <andListConditon> por el código <orListConditon>.

Grupos de acceso

Los grupos de acceso por omisión que forman parte de WebSphere Commerce se encuentran en los archivos XML específicos del idioma como, por ejemplo, *dir_instalación_WC*/xml/policies/xml/ACUserGroups_entorno_nacional.xml. Este archivo sigue la DTD especificada por *dir_instalación_WC*/xml/policies/dtd/ACUserGroups_en_US.dtd.

A continuación se muestra el formato de un elemento de grupo de acceso:

```
<UserGroup Name="valor"
   OwnerID="valor"
   Description="valor"
```

```
   <UserCondition>
     <![CDATA[
       <profile>
        Condición XML
       </profile>
     ]]>
   </UserCondition>
</UserGroup>
```

Donde:

Name: el nombre del grupo de recursos que se almacena en la columna MBRGRPNAME de la tabla MBRGRP.

OwnerID: el Member ID que es el propietario de este grupo de acceso. La combinación de Name y OwnerID debe ser exclusiva. Los valores posibles que se pueden utilizar son: RootOrganization (-2001) o DefaultOrganization (-2000).

Description (opcional): es un atributo opcional que se utiliza para describir el grupo de acceso.

UserCondition (opcional): es un elemento opcional que especifica las condiciones implícitas de miembros de este grupo de acceso. Este criterio se almacena en la columna CONDITIONS de la tabla MBRGRPCOND.

Condición XML: utilizando la infraestructura de condiciones, cualquier combinación válida de los elementos orListCondition, andListCondition, simpleCondition y trueConditionCondition.

Se da soporte a los siguientes nombres de SimpleCondition para el elemento UserCondition:

Tabla 13. Nombres de condiciones simples (Simplecondition) a las que se da soporte

Nombre de variable	Descripción	Operadores soportados	Valores soportados	Calificadores	Valores de calificadores
role	Especifica que el usuario debe tener este rol en la tabla MBRROLE..	= !=	Cualquier valor de la columna NAME de la tabla ROLE.	org (si no se especifica, el usuario debe tener el rol para cualquier organización de la tabla MBRROLE).	• OrgEntityID: la entidad en la que el usuario debe tener el rol. • OrgAndAncestorOrgs: Cuando se utilizan en una política de plantilla agrupable. policy. De este modo, si comprueba si el usuario tiene el rol especificado en la organización propietaria del recurso o en cualquiera de sus organizaciones antecesoras.
registration status	Especifica que el usuario debe tener este estado de registro.	= !=	Cualquier valor de la columna REGISTER-TYPE en la tabla USERS como, por ejemplo, G para invitado y R para registrado.	ninguno	no disponible

Tabla 13. Nombres de condiciones simples (Simplecondition) a las que se da soporte (continuación)

Nombre de variable	Descripción	Operadores soportados	Valores soportados	Calificadores	Valores de calificadores
`status`	Especifica que el usuario debe tener este estado de miembro. Normalmente, se utiliza para el estado de aprobación de registro.	= !=	Cualquier valor de la columna STATE de la tabla MEMBER como, por ejemplo, `0` para aprobación de registro pendiente, `1` para registro aprobado y `2` para registro rechazado.	ninguno	no disponible
`org`	Especifica que el usuario es hijo de la organización especificada. Esta información está basada en los datos almacenados en la tabla MBRREL	= !=	• Cualquier valor de ORGENTITY_ID en la tabla ORGENTITY. • `?`: si se trata de una política de plantilla agrupable. Esto comprobará si el usuario es un hijo de la organización propietaria del recurso. También comprobará si el usuario es hijo de cualquier antecesor del propietario del recurso hasta, e incluido, el antecesor más cercano que se suscriba a un grupo de políticas.	ninguno	no disponible

Ejemplos de simpleConditions para grupos de acceso

rol:

Rol sin calificador: El ejemplo siguiente visualiza una simpleCondition de tipo `rol` sin calificador; normalmente se utiliza en políticas basadas en roles. En este ejemplo, el usuario debe tener el rol de administrador de vendedores para cualquier entidad de organización.

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

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

Rol con un calificador: El ejemplo siguiente visualiza una simpleCondition de tipo `rol` con un calificador; normalmente se utiliza en políticas a nivel de organización. En este ejemplo, el usuario debe tener el rol de vendedor para la entidad de organización con `ORGENTITY_ID = 100`.

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

Rol con un calificador y un parámetro: El ejemplo siguiente visualiza una simpleCondition de tipo rol con un calificador y un valor de datos especial OrgAndAncestorOrgs. Este valor de datos calificado, OrgAndAncestorOrgs, solamente funciona en las políticas de plantilla agrupables. En este ejemplo, el usuario debe tener el rol de Director de ventas, Administrador de cuentas o Vendedor, en la organización propietaria del recurso especificado o en cualquiera de los antecesores de la organización.

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

registrationStatus: El ejemplo siguiente visualiza una simpleCondition de tipo `registrationStatus`. En este ejemplo, el usuario debe estar registrado (`USERS.REGISTERTYPE = R`).

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

```
   <value data="R"/>
  </simpleCondition>
  </profile>
]]></UserCondition>
```

status: El ejemplo siguiente visualiza una simpleCondition de tipo `status`. En este ejemplo, el usuario debe tener aprobado el registro. (`MEMBER.STATUS = 1`)

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

org: El ejemplo siguiente visualiza una simpleCondition de tipo `org`. En este ejemplo, el usuario debe estar registrado en la entidad de organización `100`. En la tabla MBRREL, debe haber un registro en el que el usuario sea descendiente de una organización con `ANCESTOR_ID = 100` y `SEQUENCE = 1`.

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

Políticas

El archivo *dir_instalación_WC*`/xml/policies/xml/defaultAccessControlPolicies.xml` define las políticas de control de acceso por omisión que se incluyen con el producto. Sigue la DAD especificada por: *dir_instalación_WC*`/xml/policies/dtd/accesscontrolpolicies.dtd`.

A continuación se muestra la plantilla de un elemento de política:

```
<Policy Name="valor"
  OwnerId="valor"
  UserGroup="valor"
  UserGroupOwner="valor"
  ActionGroupName="valor"
  ResourceGroupName="valor"
  PolicyType="valor"
  RelationName="valor"
  RelationGroupName="valor"
  RelationGroupOwner="valor"
</Policy>
```

Donde:

`Name`: el nombre de la política. Se carga en la columna `POLICYNAME` de la tabla `ACPOLICY`. La combinación de `Name` y `OwnerID` debe ser exclusiva.

`OwnerID`: es el ID de miembro de la entidad de organización propietaria de la política. Se carga en la columna `member_id` de la tabla `ACPOLICY`. La combinación de

OwnerID y Name debe ser exclusiva. Hay dos valores especiales reconocidos por la herramienta de transformación, estos son: RootOrganization: -2001 y DefaultOrganization: -2000

UserGroup: el nombre del grupo de acceso especificado en la columna MBRGRPNAME de la tabla MBRGRP. Se carga en la columna mbrgrp_id de la tabla ACPOLICY. Los grupos de acceso por omisión se definen en el archivo *dir_instalación_WC*/xml/policies/xml/ACUserGroups_language.xml.

UserGroupOwner: es el ID del miembro propietario del grupo de acceso. Esto es necesario cuando el propietario del grupo de acceso es un miembro que no es el propietario de la política. Si no se especifica, se presupone que el grupo de acceso es propiedad del miembro que se especifica mediante el atributo OwnerID.

ActionGroupName: el nombre del grupo de acciones especificado en la columna GROUPNAME de la tabla ACACTGRP. Se utiliza para obtener el ID de grupo de acciones correspondiente (ACACTGRP_ID) que se almacenará en la tabla ACPOLICY. Las políticas basadas en roles para los mandatos de controlador tienen ActionGroupName establecido en ExecuteCommandActionGroup. Las políticas para beans de datos tienen ActionGroupName establecido en DisplayDatabeanActionGroup.

ResourceGroupName: el nombre del grupo de recurso, especificado en la columna GRPNAME de la tabla ACRESGRP. Se utiliza para obtener el ID de grupo de acciones correspondiente (ACRESGRP_ID) que se almacena en la tabla ACPOLICY. Las políticas basadas en roles para vistas tienen ResoureGroupName establecido en ViewCommandResourceGroup.

PolicyType: el tipo de política. Los valores válidos son groupableStandard y groupableTemplate. Por motivos de compatibilidad con versiones anteriores, se da soporte también a los valores standard y template. Si no se especifica este atributo cuando se carga una política nueva, se utilizará el valor nulo. Si no se especifica este atributo cuando se actualice una política existente, el valor no se modificará. La tabla siguiente muestra la correlación de valores de serie con valores de base de datos almacenados en la columna POLICYTYPE de la tabla ACPOLICY.

Tabla 14. Correlación de valores de serie con valores de base de datos

String	**ACPOLICY.POLICYTYPE**
groupableTemplate	3
groupableStandard	2
template	1
standard	0 o nulo

Para obtener más información sobre los tipos de políticas, consulte el Capítulo 3, “Conceptos relacionados con la autorización”, en la página 19.

RelationName (optional): El nombre de Relationship, como se especifica en la columna RELATIONNAME de la tabla ACRELATION. Si se especifica, se utiliza para obtener el ID de relación correspondiente (ACRELATION_ID) que está almacenado en la tabla ACPOLICY.

RelationGroupName (opcional): El nombre del grupo de relaciones como se especifica en la columna GRPNAME de la tabla ACRELGRP. Si se especifica este atributo, no debe especificarse RelationName ya que Relationship Group tiene prioridad.

RelationGroupOwner: el ID de miembro que es el propietario de Relationship Group. Este atributo solamente es necesario si se especifica el atributo RelationGroupName y si el valor del atributo OwnerID no es RootOrganization; en cuyo caso, RelationGroupOwner debe especificarse como RootOrganization (-2001).

Ejemplos de políticas

Políticas basadas en roles:

Para mandatos de controlador: En este ejemplo, los usuarios que pertenecen al grupo de acceso AllUsers pueden ejecutar los mandatos de controlador que forman parte del grupo de recursos AllUserCmdResourceGroup.

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

Para vistas: En este ejemplo, los usuarios que pertenecen al grupo de acceso MarketingManagers pueden ejecutar las vistas que pertenecen al grupo de acciones MarketingManagersViews.

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

Políticas a nivel de recursos:

Para mandatos: En este ejemplo, los usuarios que pertenecen al grupo de acceso AllUsers pueden realizar las acciones especificadas por el grupo de acceso CouponRedemption en los recursos especificados por CouponWalletResourceGroup, siempre que los usuarios satisfagan la relación de creator (creador) con respecto al recurso.

```
<Policy Name="AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource"
   OwnerID="RootOrganization"
   UserGroup="AllUsers"
   ActionGroupName="CouponRedemption"
   ResourceGroupName="CouponWalletResourceGroup"
   RelationName="creator"
   PolicyType="groupableStandard">
</Policy>
```

Para beans de datos: En este ejemplo, los usuarios pertenecientes al grupo de acceso AllUsers pueden visualizar beans de datos especificados por el grupo de recursos UserDatabeanResourceGroup, siempre que los usuarios satisfagan la relación owner (propietario) con respecto al recurso.

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

Políticas de plantilla agrupables: En este ejemplo, los usuarios que pertenecen al grupo de acceso

`OrgAdminConsoleMembershipAdministratorsForOrg`

puede realizar las acciones especificadas por el grupo de acciones `ApproveGroupUpdate` en los recursos que especifique `OrganizationDataResourceGroup`.

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

Al analizar la definición del grupo de acceso `OrgAdminConsoleMembershipAdministratorsForOrg` se revelará la condición siguiente para los miembros:

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

Nota: La `simpleCondition` de `role` se califica mediante `org` = **`OrgAndAncestorOrgs`**. `OrgAndAncestorOrgs` es una palabra clave que solamente está disponible en políticas de plantilla agrupables. Amplía dinámicamente el ámbito del rol al contexto del propietario del recurso actual. En este ejemplo, el usuario debe tener uno de los roles especificados en la organización propietaria del recurso o en cualquiera de los antecesores de la organización.

Definición de grupos de políticas

Los grupos de políticas se crean en políticas de grupo, basándose en los requisitos de la empresa y de control de acceso. Algunos grupos de políticas por omisión se crean durante la instalación, para obtener más información, consulte el apartado "Políticas y grupos de control de acceso por omisión", en la página 217. Otros grupos de políticas se crean a medida que se necesitan mientras se publica una tienda o un modelo de negocio. En la mayor parte de los casos simplemente puede añadir políticas nuevas que cree a los grupos de políticas existente. Si tiene que crear un grupo de políticas nuevo, debe definirlo en un archivo XML, similar a

defaultAccessControlPolicies.xml y después debe cargarlo en la base de datos. La siguiente es una definición de ejemplo:

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

donde:

Name: el nombre del grupo de políticas.

OwnerID: el ID de miembro de la entidad de organización propietaria del grupo de políticas. Se carga en la columna member_id de la tabla ACPOLGRP. La combinación de OwnerID y Name debe ser exclusiva. Hay dos valores especiales reconocidos por la herramienta de transformación, estos son: RootOrganization: -2001 y DefaultOrganization: -2000.

Asociación de políticas a grupos de políticas

Las políticas pueden pertenecer a varios grupos de políticas. No obstante, para facilitar la administración de políticas se recomienda que una política sólo pertenezca a un grupo de políticas. Esta asociación se debe definir en un archivo XML, similar a defaultAccessControlPolicies.xml y luego se ha de cargar en la base de datos. La siguiente es una definición de ejemplo:

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

donde:

PolicyGroupPolicy Name: el nombre de la política, definida previamente, que se ha de asociar con el grupo de políticas especificado. Esta política debe ser de uno de los tipos de políticas siguientes: groupableStandard o groupableTemplate.

PolicyGroupPolicy PolicyOwnerID (opcional): El ID de miembro de la entidad de organización propietaria de la política especificada. Si no se especifica este parámetro, el valor por omisión es el OwnerID del grupo de políticas. Hay dos valores especiales reconocidos por la herramienta de transformación, estos son: RootOrganization: -2001 y DefaultOrganization: -2000.

Suscripción a grupos de políticas

Los recursos de una organización se protegen mediante las políticas de los grupos de políticas a los que se ha suscrito la organización. Si dicha organización no se suscribe a ningún grupo de políticas, entonces se aplicarán los grupos de políticas a los que se suscribe el antecesor más próximo a dicha organización. Para obtener más información sobre los grupos de políticas a los que debe suscribirse una organización, consulte el apartado “Políticas y grupos de control de acceso por omisión”, en la página 217.

La suscripción a grupos de políticas se puede llevar a cabo en la Consola de administración de organizaciones, pero también se puede definir en un archivo XML, similar a defaultAccessControlPolicies.xml y luego se puede cargar en la base de datos. La siguiente es una definición de ejemplo:

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

donde:

OrganizationID: el ID de miembro de la entidad de organización que se suscribe a este grupo de políticas. Hay dos valores especiales reconocidos por la herramienta de transformación, estos son: `RootOrganization: -2001` y `DefaultOrganization: -2000`.

Datos de política que pueden traducirse

A continuación se muestra una plantilla de un archivo de políticas personalizado que puede utilizarse para definir datos de políticas traducibles:

```
 <?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
 <!--Los siguientes elementos de control de acceso que pueden TRADUCIRSE
deben estar definidos en este archivo:
 <Attribute_nls>
 <Action_nls>
 <Relation_nls>
 <ResourceCategory_nls>
 <ActionGroup_nls>
 <ResourceGroup_nls>
 <Policy_nls>
 <PolicyGroup_nls>-->
<!DOCTYPE PoliciesNLS SYSTEM "../dtd/accesscontrolpoliciesnls.dtd">

<PoliciesNLS LanguageID="valor">


 <!--Inserte aquí las definiciones de elementos de control de acceso -->
 </PoliciesNLS>
```

El atributo `LanguageID` es una serie correspondiente a los datos específicos del idioma del entorno nacional. Los valores válidos de `LanguageID` son:

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

Datos de política que no pueden traducirse

A continuación se muestra una plantilla de un archivo de políticas personalizado que contiene datos no traducibles:

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

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

 <!--Los siguientes elementos de control de acceso que NO PUEDEN TRADUCIRSE
deben estar definidos en este archivo:

 <Attribute>
 <Action>
 <ResourceCategory>
 <Relation>
 <RelationGroup>
 <ActionGroup>
 <ResourceGroup>
 <Policy>
```

```
 <PolicyGroup>-->
<Policies>

 <!--Inserte aquí las definiciones de elementos de control de acceso -->
 </Policies>
```

Datos específicos del entorno nacional

Los siguientes datos específicos del entorno nacional son opcionales y se pueden cargar para proporcionar una descripción adicional a los elementos de control de acceso definidos en el archivo XML no traducible. Los datos específicos del entorno nacional por omisión se pueden encontrar en la dirección siguiente:

dir_instalación_WC\xml\policies\xml\
defaultAccessControlPolicies_*entorno_nacional*.xml

por ejemplo, defaultAccessControlPolicies_es_ES.xml.

Atributo: El siguiente ejemplo define información de elementos de atributo adicional:

```
<Atrribute_nls AttributeName="Status"
DisplayName_nls="Atributo de estado"
Description_nls="Atributo de estado del recurso"
/>
```

Donde:

AttributeName: es el nombre del atributo. Este valor se almacena en la columna ATTRNAME de la tabla ACATTR.

DisplayName_nls: es el nombre de visualización del atributo. Este valor se almacena en la columna DISPLAYNAME de la tabla ACATTRDESC.

Description_nls: es una descripción opcional del atributo. Este valor se almacena en la columna DESCRIPTION de la tabla ACATTRDESC.

Acción: El siguiente ejemplo define información de elementos de acción adicional:

```
<Action_nls ActionName="OrderAdjustmentButton"
DisplayName_nls="Vista del botón ajuste de pedido"
Description_nls="Las vistas para cargar botones en la página de ajuste de pedido
cuando se formaliza un pedido desde Commerce Accelerator"
/>
```

Donde:

ActionName: es el nombre de la política. Este valor se almacena en la columna ACTION de la tabla ACACTION.

DisplayName_nls: es el nombre de visualización de la acción. Este valor se almacena en la columna DISPLAYNAME de la tabla ACACTDESC.

Description_nls: es una descripción opcional de la acción. Este valor se almacena en la columna DESCRIPTION de la tabla ACACTDESC.

Relación: El siguiente ejemplo define información de elementos de relación adicional:

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

Donde:

RelationName: es el nombre de la relación. Este valor se almacena en la columna RELATIONNAME de la tabla ACRELATION.

DisplayName_nls: es el nombre de visualización de la relación. Este valor se almacena en la columna DISPLAYNAME de la tabla ACRELDESC.

Description_nls: es una descripción opcional de la relación. Este valor se almacena en la columna DESCRIPTION de la tabla ACRELDESC.

Categoría de recursos: El siguiente ejemplo define información de categoría de recursos adicional:

```
<ResourceCategory_nls ResourceCategoryName="com.ibm.commerce.
catalog.objects."InterestItemList"
DisplayName_nls="Lista de artículos de interés"
Description_nls="Mandato de lista de artículos de interés"
/>
```

Donde:

ResourceCategoryName: es el nombre de la categoría de recursos. Este valor se almacena en la columna RESCLASSNAME de la tabla ACRESCGRY.

DisplayName_nls: es el nombre de visualización de la categoría de recursos. Este valor se almacena en la columna DISPLAYNAME de la tabla ACRSCGDES.

Description_nls: es una descripción opcional de la categoría de recursos. Este valor se almacena en la columna DESCRIPTION de la tabla ACRSCGDES.

Grupo de acciones: El siguiente ejemplo define información de grupo de acciones adicional:

```
<ActionGroup_nls ActionGroupName="DoEverything"
DisplayName_nls="Realizar todas las acciones"
Description_nls="Permite realizar todas las acciones"
/>
```

Donde:

ActionGroupName: es el nombre del grupo de acciones. Este valor se almacena en la columna GROUPNAME de la tabla ACACTGRP.

DisplayName_nls: es el nombre de visualización del grupo de acciones. Este valor se almacena en la columna DISPLAYNAME de la tabla ACACGPDESC.

Description_nls: es una descripción opcional del grupo de acciones. Este valor se almacena en la columna DESCRIPTION de la tabla ACACGPDESC.

Grupo de recursos: El siguiente ejemplo define información de grupo de recursos adicional:

```
<ResourceGroup_nls ResourceGroupName="AllResourceGroup"
DisplayName_nls="Todos los grupos de recursos"
Description_nls="Todos los recursos"
/>
```

Donde:

ResourceGroupName: el nombre del grupo de recursos. Este valor se almacena en la columna GRPNAME de la tabla ACRESGRP.

DisplayName_nls: es el nombre de visualización del grupo de recursos. Este valor se almacena en la columna DISPLAYNAME de la tabla ACRESGPDES.

Description_nls: es una descripción opcional del grupo de recursos. Este valor se almacena en la columna DESCRIPTION de la tabla ACRESGPDES.

Política: El siguiente ejemplo define información de políticas adicional:

```
<Policy_nls PolicyName="SiteAdministratorsCanDoEverything"
OwnerID="RootOrganization"
DisplayName_nls="Los administradores del sitio pueden realizar todas las acciones"
Description_nls="Política que permite que los administradores de sitio puedan
realizar todas las acciones "
/>
```

Donde:

PolicyName: es el nombre de la política de control de acceso. Este valor se almacena en la columna POLICYNAME de la tabla ACPOLICY.

OwnerID: es el ID de miembro de la entidad de organización propietaria de esta política.

DisplayName_nls: es el nombre de visualización de la política. Este valor se almacena en la columna DISPLAYNAME de la tabla ACPOLDESC.

Description_nls: es una descripción opcional de la política. Este valor se almacena en la columna DESCRIPTION de la tabla ACPOLDESC.

Grupo de políticas: El siguiente ejemplo define información adicional sobre el grupo de políticas:

```
<PolicyGroup_nls PolicyGroupName="B2CPolicyGroup" OwnerID="RootOrganization"
  DisplayName_nls="Grupo de políticas B2C"
  Description_nls="Este grupo de políticas contiene todas las políticas
específicas de B2C."
 />
```

donde:

PolicyGroupName: es el nombre del grupo de políticas de control de acceso al que se añadirá información adicional. Este valor se almacena en la columna NAME de la tabla ACPOLGRP.

OwnerID: es el ID de miembro de la entidad de organización propietaria de este grupo de políticas.

DisplayName_nls: es el nombre de visualización del grupo de políticas. Este valor se almacena en la columna DISPLAYNAME de la tabla ACPLGPDESC.

Description_nls: es una descripción opcional del grupo de políticas. Este valor se almacena en la columna DESCRIPTION de la tabla ACPLGPDESC.

Después de modificar los archivos XML

Comprobar los cambios

Para obtener información sobre cómo comprobar los cambios, consulte el apartado "Después de modificar la política" en la página 111.

Cargar los cambios en la base de datos

Si modifica la política directamente en los archivos XML, debe volver a cargar los archivos XML modificados en las bases de datos. Es importante mantener la coherencia entre los archivos XML y la información de control de acceso de las bases de datos por diferentes motivos:

- Cuando crea una instancia de WebSphere Commerce, las definiciones del grupo de políticas y del grupo de acceso se cargan desde los archivos XML.
- Si desea implementar las mismas políticas de control de acceso en una segunda instancia de WebSphere Commerce, puede hacerlo copiando los archivos XML en el directorio adecuado antes de crear la segunda instancia.
- Los archivos XML son un método práctico de ver y editar directamente las políticas y sus componentes, por lo que mantener actualizados estos archivos resulta esencial.

Cargar los cambios XML en la base de datos

El proceso de carga lee los archivos XML que contienen la información de políticas de control de acceso y las definiciones de los grupos de acceso y los carga en las bases de datos adecuadas. La información de políticas y grupos de acceso que contienen los archivos XML se cargan durante la instalación, sin embargo, deberá volver a cargar los archivos si los modifica.

Notas:

1. Si crea archivos XML personalizados, deberá copiarlos en el directorio *<dir_instalación_WC>*/xml/policies/xml para cargarlos en las bases de datos.
2. Hay un valor en los scripts de carga que especifica el siguiente valor de parámetro mientras se resuelve el ID y se cargan los datos en la base de datos: "-maxerror 100000". Esto significa que si se producen más de 100000 violaciones de claves externas durante la carga de datos, se ignorarán y el proceso no se cancelará con errores. Este valor se puede aumentar o disminuir según sea necesario. Por ejemplo, si desea que en caso de error se detenga el proceso, deberá cambiar el valor a 1.

Para 400 : si crea archivos XML personalizados, debe utilizar la vía de acceso completa a la DTD del archivo. Las DTD de políticas de control de acceso se encuentran en *dir_instalación_WC*/xml/policies/dtd.

Para cargar los grupos de acceso y las políticas de control de acceso, ejecute los mandatos siguientes:

Para 2000

1. Desde el directorio *<dir_instalación_WC>*\bin, ejecute los archivos de mandatos siguientes según sea necesario en el orden en que figuran aquí:
   - Para cargar las definiciones de grupos de usuarios (acceso), ejecute el archivo de mandatos **acugload**. **Sintaxis**: acugload.cmd *<nombre_base_datos>*

<usuario_base_datos> *<contraseña_usuario_base_datos>* *<archivo_xml_UserGroups>*[*nombre_esquema*] **Ejemplo**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml

- Para cargar el archivo de políticas de control de acceso principal, ejecute el archivo de mandatos **acpload**. **Sintaxis:**acpload.cmd *<nombre_base_datos>* *<usuario_base_datos>* *<contraseña_usuario_base_datos>* *<archivo_xml_políticas>*[*nombre_esquema*] **Ejemplo**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml
- Para cargar los nombres de visualización y los archivos de descripciones, ejecute el archivo de mandatos **acpnlsload**. **Sintaxis:**acpnlsload.cmd *<nombre_base_datos>* *<usuario_base_datos>* *<usuario_base_datos contraseña>* *<NLS archivo_xml_políticas>*[*nombre_esquema*] **Ejemplo**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_es_ES.xml

2. Compruebe si los archivos de anotaciones **acugload.log**, **acpload.log** y **acpnlsload.log** que se encuentran en *<dir_instalación_WC>*\logs contienen errores.

Para 400 AIX Solaris Linux

El ID de usuario de base de datos, debe tener el permiso siguiente para poder continuar con los pasos siguientes:

- Autorización de lectura/grabación/ejecución en los directorios, subdirectorios y archivos de *dir_instalación_WC*/xml/policies y *dir_instalación_WC*/logs.
- Autorización de lectura/ejecución en el directorio *dir_instalación_WC*/bin y sus archivos.

Si el ID de usuario de base de datos no tiene la autorización necesaria mencionada, deberá concederle esta autorización con el mandato chmod.

1. Inicie la sesión con el ID de usuario de base de datos.
2. Desde el directorio *<dir_instalación_WC>*/bin, ejecute los siguientes scripts del shell según sea necesario y en el orden en que se listan aquí:

1. Para cargar las definiciones de grupos de usuarios (acceso), ejecute el script del shell **acugload**. **Sintaxis:** acugload.sh *<nombre_base_datos>* *<usuario_base_datos>* *<usuario_base_datos contraseña>* *<archivo_xml_UserGroups>*[*nombre_esquema*] **Ejemplo**: acugload mall dbuser dbusrpwd ACUserGroups_en_US.xml
2. Para cargar el archivo de políticas de control de acceso principal, ejecute el script del shell **acpload**. **Sintaxis:**acpload.sh *<nombre_base_datos>* *<usuario_base_datos>* *<contraseña_usuario_base_datos>* *<archivo_xml_políticas>*[*nombre_esquema*] **Ejemplo**: acpload mall dbuser dbusrpwd defaultAccessControlPolicies.xml
3. Para cargar los nombres de visualización y los archivos de descripciones, ejecute el script del shell acpnlsload. **Sintaxis:** acpnlsload.sh *<nombre_base_datos>* *<usuario_base_datos>* *<usuario_base_datos contraseña >* *<NLS archivo_xml_políticas>*[*nombre_esquema*] **Ejemplo**: acpnlsload mall dbuser dbusrpwd defaultaccesscontrolpolicies_es_ES.xml

Compruebe si los archivos de anotaciones acugload.log, acpload.log y acpnlsload.log que están en *<dir_instalación_WC>*/logs contienen errores.

Nota: Después de ejecutar estos scripts debe consultar los archivos de anotaciones ya que los errores que puedan producirse mientras se ejecutan estos scripts no aparecerán en la línea de mandatos.

Para 400

Nota: Para 400 los archivos de anotaciones están en el directorio *dir_usuario_WC*/instances.

Extraer las definiciones de políticas y grupos de acceso de las bases de datos a archivos XML

El proceso de extracción lee la información de políticas y grupos de acceso de las bases de datos de control de acceso y genera archivos que capturan la información en formato XML. El programa de utilidad de extracción utiliza un archivo XML de filtro para especificar los datos que se han de extraer de la base de datos. Se proporcionan los siguientes archivos de filtro:

- `ACPoliciesfilter.xml`: se utiliza para extraer todos los datos de políticas y del grupo de acceso.
- `ACUserGroupsFilter.xml`: se utiliza para extraer todos los datos del grupo de acceso.
- `OrganizationPoliciesFilter.xml`: se utiliza para extraer todos los datos del grupo de acceso de una organización determinada. Antes de utilizar este archivo, se debe editar para especificar el ID de organización necesario. Se extraerán los datos de política propiedad de este ID de organización.

Para NT 2000

1. En el directorio <*dir_instalación_WC*>\bin ejecute el siguiente mandato acpextract:

   ```
   acpextract.cmd <nombre_base_datos> <usuario_base_datos>
   <contraseña_usuario_base_datos> <archivo_filtro_xml_entrada> [nombre_esquema]
   ```

   Por ejemplo,

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

   Se crearán los archivos siguientes:

   - `ExtractedACPolicies.xml`: este archivo contiene los datos que se han extraído mediante el mandato `Extract` para el criterio de filtro especificado.
   - `ExtractedACPolicies.dtd`: la DTD del archivo `ExtractedACPolicies.xml`.
   - `AccessControlUserGroups.xml`: el archivo que contiene las definiciones de grupos de acceso.
   - `AccessControlPolicies.xml`: el archivo que contiene la información de política de control de acceso que es independiente del idioma.
   - `AccessControlPolicies_entorno_nacional.xml`: el archivo de políticas de control de acceso que depende del idioma y que contiene los nombres de visualización y las descripciones.
2. Compruebe el archivo <*dir_instalación_WC*>\logs\acpextract.log por si se han producido errores de proceso.

Para 400 AIX Solaris Linux

1. Inicie la sesión con el ID de usuario de base de datos.
2. Desde el directorio <*dir_instalación_WC*>\bin, ejecute el siguiente script del shell acpextract:

   ```
   acpextract.sh <nombre_base_datos> <usuario_base_datos>
   <contraseña_usuario_base_datos> <archivo_filtro_xml_entrada> [nombre_esquema]
   ```

   Por ejemplo,

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

Se crearán los archivos siguientes:

- `ExtractedACPolicies.xml`: este archivo contiene los datos que se han extraído mediante el mandato `Extract` para el criterio de filtro especificado.
- `ExtractedACPolicies.dtd`: la DTD del archivo `ExtractedACPolicies.xml`.
- `AccessControlUserGroups.xml`: el archivo que contiene las definiciones de grupos de acceso.
- `AccessControlPolicies.xml`: el archivo que contiene la información de política de control de acceso que es independiente del idioma.
- `AccessControlPolicies_entorno_nacional.xml`: el archivo de políticas de control de acceso que depende del idioma y que contiene los nombres de visualización y las descripciones.

3. Compruebe el archivo *<dir_instalación_WC>*`\logs\acpextract.log` por si se han producido errores de proceso.

Para 400

1. Se crearán los archivos siguientes en el directorio *dir_instalación_WC*`/xml/policies/xml` utilizando el parámetro `OUTDIR`:
   - `ExtractedACPolicies.xml`: este archivo contiene los datos que se han extraído mediante el mandato `Extract` para el criterio de filtro especificado.
   - `ExtractedACPolicies.dtd`: la DTD del archivo `ExtractedACPolicies.xml`.
   - `AccessControlUserGroups.xml`: el archivo que contiene las definiciones de grupos de acceso.
   - `AccessControlPolicies.xml`: el archivo que contiene la información de política de control de acceso que es independiente del idioma.
   - `AccessControlPolicies_entorno_nacional.xml`: el archivo de políticas de control de acceso que depende del idioma y que contiene los nombres de visualización y las descripciones.

Parte 4. Seguridad de Payments

Esta parte describe las tareas de administración de seguridad de Payments.

Capítulo 14. Acceso a WebSphere Commerce Payments

WebSphere Commerce Payments autentica a los usuarios utilizando dominios. Un dominio es un registro de usuarios junto con un método de autenticación de dichos usuarios, por ejemplo, un nombre de usuario y una contraseña. Cada instalación de WebSphere Commerce Payments solamente puede utilizar un dominio cada vez. Ejemplos de tipos de dominio son los dominios LDAP y los dominios del sistema operativo. Un usuario debe estar definido en un dominio para poder concederle acceso a los recursos. Por lo tanto, un usuario es un usuario válido de WebSphere Commerce Payments única y exclusivamente si se cumplen estas dos condiciones:

- Está en el dominio
- Tiene asignado un rol en WebSphere Commerce Payments

WebSphere Commerce Payments emplea un esquema de control de acceso basado en roles que define cuatro roles de WebSphere Commerce Payments:

1. Administrador de Payments
2. Administrador de comerciantes
3. Supervisor
4. Asistente

El administrador de Payments puede utilizar la ventana Usuario de la interfaz de usuario de WebSphere Commerce Payments para asignar acceso (basado en un rol) a un usuario definido en un dominio. WCSRealm se proporciona con WebSphere Commerce Payments. La clase WCSRealm se configura automáticamente para el sistema. Este dominio permite que el servlet de WebSphere Commerce Payments utilice la información del administrador que está registrada en las tablas de usuario de WebSphere Commerce. Esta información de administrador la utilizan los administradores de Payments para que no pueda definir otro conjunto de ID de administradores para utilizar la interfaz de usuario de WebSphere Commerce Payments.

Capítulo 15. Mantenimiento de la seguridad de WebSphere Commerce Payments

La seguridad WebSphere Commerce Payments está basada en varios elementos clave para la seguridad. Estos elementos se combinan para crear un entorno en el que se pueden desplegar los servicios en la Web con seguridad.

Nota: Anteriormente IBM WebSphere Commerce Payments (al que a partir de este momento se hará referencia como WebSphere Commerce Payments) se conocía como Payment Manager. A partir de la versión 3.1.3, se ha cambiado el nombre de la aplicación por WebSphere Commerce Payments y en este documento se han modificado las referencias al producto.

Protección de WebSphere Commerce Payments

En el núcleo de WebSphere Commerce Payments se encuentra el servlet de pago. La composición de WebSphere Commerce Payments se completa con varios productos subordinados, el servidor Web configurado con WebSphere Application Server, la base de datos y la interfaz de usuario. En este capítulo se describen los métodos para proteger los diferentes componentes de WebSphere Commerce Payments.

Protección de datos confidenciales

Para cada mandato de consulta, la infraestructura verifica el rol del usuario en este rol mínimo y, por lo tanto, establece un indicador en el objeto QueryRequest que permite indicar si los datos confidenciales como, por ejemplo, los números de tarjeta de crédito o las direcciones de facturación deben devolverse totalmente visualizadas o si deben enmascararse. La infraestructura de WebSphere Commerce Payments no mantiene ningún dato confidencial que se pueda devolver mediante un mandato de consulta. No obstante, se proporcionan métodos nuevos para que los que escriban casetes puedan comprobar el valor de este indicador y también marcar los datos confidenciales de modo estándar. Cada casete debe diferenciar los datos confidenciales del resto de los datos almacenados. Generalmente, los datos confidenciales son el mismo conjunto de datos que un casete cifra antes de almacenarlo en la base de datos de WebSphere Commerce Payments.

El parámetro del sistema JVM `wpm.MinSensitiveAccessRole={clerk|supervisor|madmin|psadmin|none}` especifica el rol mínimo que debe tener asignado un usuario para poder acceder a los datos confidenciales. El valor es sensible a las mayúsculas y minúsculas. Si no se especifica esta propiedad, se presupone un valor de asistente, lo que permite que todos los usuarios puedan ver los datos confidenciales. Si se especifica un valor no válido, el servlet de Payment no se inicializa.

Tenga en cuenta que este parámetro se puede establecer durante la creación de la instancia de Payments y se puede actualizar con el Gestor de configuración de WebSphere Commerce. El nombre del parámetro del Gestor de configuración es Rol de acceso mínimo en el panel de la instancia de Payments. Para obtener más información sobre los paneles del Gestor de configuración, consulte la publicación *WebSphere Commerce, Guía de instalación* de su plataforma o la ayuda en línea del panel de la instancia de Payments desde el Gestor de configuración.

La tabla siguiente describe los valores soportados que se listan por orden ascendente de autorización:

Tabla 15. Autorización de rol de usuario de Payments

Usuario	Descripción
asistente	Los usuarios con un rol de asistente o superior pueden ver los datos confidenciales.
supervisor	Los usuarios con un rol de supervisor o superior pueden ver los datos confidenciales.
madmin	Los usuarios con un rol de Administrador de comerciantes o superior pueden ver los datos confidenciales.
psadmin	Sólo los administradores Payments pueden ver los datos confidenciales.
ninguno	Nadie puede ver los datos confidenciales.

Puede especificar el parámetro `wpm.MinSensitiveAccessRole` mediante el Gestor de configuración de WebSphere Commerce.

Protección de la base de datos

La base de datos WebSphere Commerce Payments almacena datos confidenciales y requiere protección contra lectura y grabación por parte de fuentes no autorizadas. WebSphere Commerce Paymentsproporciona soporte para el cifrado de datos confidenciales como, por ejemplo, la información de los titulares de tarjetas de crédito y las contraseñas que se almacena en la base de datos.

Datos de transacciones

Las siguientes son directrices para el manejo de datos de transacciones.

- La información confidencial sobre transacciones se almacena en una tabla de base de datos en la biblioteca de instancias. Esta biblioteca se especifica como el Nombre del esquema de instancia en el Asistente de creación de instancias de Payments.
- Cualquier copia de seguridad deberá mantenerse en un lugar seguro.
- Las tablas de base de datos de la biblioteca de la instancia contiene información crítica sobre configuración y transacciones y debe incluirse como parte de la estrategia de copia de seguridad del sistema. Asimismo, también debe realizar una copia de seguridad de lo siguiente:
  - Los archivos del directorio `/QIBM/UserData/CommercePayments/V55/`*`nombre_instancia`* es el nombre de la instancia de WebSphere Commerce Payments.
  - la instancia de HTTP Server que ha configurado para WebSphere Commerce Payments. Este HTTP Server se especifica como el servidor Web en el Asistente de creación de instancias de Payments.
  - Los objetos de la biblioteca de instancias de la máquina local al igual que la colección de bases de datos de la máquina remota cuando se utiliza el almacenamiento de base de datos remoto.

Parte 5. Diferentes temas sobre seguridad

Esta parte describe las diferentes tareas de seguridad que realiza el administrador del sistema WebSphere Commerce.

Capítulo 16. Habilitación de la seguridad de WebSphere Application Server

Este capítulo describe cómo habilitar la seguridad para WebSphere Application Server. Al habilitar la seguridad de WebSphere Application Server ningún usuario podrá invocar de forma remota los componentes JavaBeans.

Notas:

1. Windows Si se ha habilitado la seguridad global de WebSphere Application Server, como se describe en los pasos de este capítulo, no podrá detener correctamente el servidor WebSphere Application Server (por ejemplo, `server1`) desde el Servicios de Windows 2000. Para detener el servicio cuando se ha habilitado la seguridad, desde un indicador de mandatos emita el mandato `stopserver` desde el directorio *`dir_instalación_WAS`*`\bin` como se indica a continuación:

   ```
   stopserver servidor -username id_usuario -password contraseña
   ```

   donde *servidor* es el nombre del directorio de configuración WebSphere Application Server del servidor que desea detener (por ejemplo, `server1`), *id_usuario* es el nombre de usuario para fines de autenticación, si la seguridad está habilitada en el servidor y *contraseña* es la contraseña para autenticación si la seguridad está habilitada en el servidor.

   Cuando intenta detener el servidor desde el panel Servicios, no se incluyen las propiedades como, por ejemplo, el ID de usuario y la contraseña. Con la seguridad global habilitada, necesitará tanto el ID de usuario como la contraseña para fines de autenticación para detener el servidor. El servicio continúa ejecutándose a pesar de que el panel Servicios muestre que se ha detenido. Tenga en cuenta que el ID de usuario y la contraseña no son necesarios para iniciar el servicio desde el panel Servicios.
2. Para detener el servidor de aplicaciones cuando está habilitada la seguridad WebSphere Application Server, desde un indicador de mandatos utilice el mandato `stopserver` desde el directorio *`dir_instalación_WAS`*`/bin` como se indica a continuación:

   AIX Linux Solaris

   ```
   stopserver servidor -username id_usuario -password contraseña
   ```

   donde *servidor* es el nombre del servidor de aplicaciones WebSphere Application Server que desea detener (por ejemplo, `server1`), *id_usuario* es el nombre de usuario para fines de autenticación y *contraseña* es la contraseña para fines de autenticación.

   400

   ```
   stopserver -instance nombre_instancia_WAS servidor -username id_usuario
      -password contraseña
   ```

   donde *nombre_instancia_WAS* es el nombre de la instancia WebSphere Application Server, *servidor* es el nombre del servidor de aplicaciones WebSphere Application Server que desea detener (por ejemplo, `server1`), *id_usuario* es el nombre de usuario para fines de autenticación y *contraseña* es la contraseña para fines de autenticación.

3. AIX Linux Solaris Windows Cuando se habilita la seguridad de WebSphere Application Server, es necesario que la máquina posea los requisitos siguientes:
   - Un mínimo de memoria de 1 GB.
   - Un mínimo de tamaño de almacenamiento dinámico de 384 MB, para la aplicación de WebSphere Commerce.

Antes de empezar

Antes de empezar a habilitar la seguridad, necesitará conocer cómo valida los ID de usuario el sistema WebSphere Application Server en el que está habilitando la seguridad. WebSphere Application Server puede utilizar el registro de usuarios de LDAP o del sistema operativo como registro de usuarios de WebSphere Application Server.

Habilitación de la seguridad con un registro de usuarios de LDAP

AIX Solaris Linux Para habilitar la seguridad de WebSphere Application Server cuando utiliza LDAP como el registro de usuarios de WebSphere Application Server, conéctese al sistema con el ID `wasuser` y efectúe los pasos siguientes:

400 Para habilitar la seguridad de WebSphere Application Server cuando utiliza LDAP como registro de usuarios de WebSphere Application Server, conéctese al sistema y realice los pasos siguientes.

Windows Para habilitar la seguridad de WebSphere Application Server cuando se está utilizando LDAP como registro de usuarios de WebSphere Application Server, conéctese al sistema como usuario con autorización de administrador y realice los pasos siguientes.

1. Inicie WebSphere Application Server y abra la Consola de administración de WebSphere Application Server.
2. En la Consola de administración, modifique los valores de seguridad globales como se indica a continuación:
   a. En **Seguridad**, amplíe **Registros de usuarios** y pulse **LDAP**. Rellene los campos de la pestaña **Configuración** como se indica a continuación, dependiendo del tipo de servidor de directorios que esté utilizando:

Tabla 16. Usuarios de IBM Directory Server. AIX 400 Linux Solaris

Windows

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de usuario de servidor	ID de usuario	*ID_usuario*	• No debe ser el administrador de LDAP. • No utilice un usuario que se haya especificado como cn=xxx. • Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de usuario de servidor	Contraseña de usuario	*contraseña*	
Tipo	Tipo de servidor LDAP	SecureWay	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda	o=ibm,c=us	
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda		Este campo no es necesario
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace		Este campo no es necesario

Tabla 17. Usuarios de Netscape. Windows

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de usuario de servidor	ID de usuario	*ID_usuario*	• No debe ser el administrador de LDAP. • No utilice un usuario que se haya especificado como cn=xxx. • Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de usuario de servidor	Contraseña de usuario	*contraseña*	
Tipo	Tipo de servidor LDAP	Netscape	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda	o=ibm	
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda		Este campo no es necesario
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace		Este campo no es necesario

Tabla 18. Usuarios de Domino. Windows

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de usuario de servidor	Nombre abreviado/ID de usuario	*ID_usuario*	Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de usuario de servidor	Contraseña de usuario	*contraseña*	
Tipo	Tipo de servidor LDAP	Domino 5.0	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda		Este campo no es necesario
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda		Este campo no es necesario
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace		Este campo no es necesario

Tabla 19. Usuarios de Active Directory. Windows

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de usuario de servidor	Nombre de cuenta SAM	*ID_usuario*	• Nombre de conexión de usuario de cualquier usuario corriente. • No utilice un usuario que se haya especificado como cn=xxx. • Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de usuario de servidor	Contraseña de usuario	*contraseña*	
Tipo	Tipo de servidor LDAP	Active Directory	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda	CN=users, DC=domain1, DC=domain2, DC=com	
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda	CN=*ID_usuario*, CN=users, DC=domain1, DC=domain2, DC=com	El valor de *ID_usuario* es el Nombre de visualización. Este no es necesariamente igual al Nombre de conexión de usuario.
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace	*contraseña_enlace*	Debe ser la misma que la Contraseña de servidor de seguridad.

Pulse **Aplicar** y luego **Guardar**.

b. En la Consola de administración, expanda **Seguridad** y pulse **Seguridad global**.
   1) En la pestaña Configuración de la seguridad global, seleccione **Habilitado** y borre la marca de selección de **Forzar la seguridad de Java 2**.

      Nota: WebSphere Commerce 5.5 no da soporte a la seguridad de Java 2.
   2) En el campo J Mecanismo de autenticación activo, seleccione **LTPA (Lightweight Third Party Authentication)**.
   3) En el campo Registro de usuarios activo, seleccione **LDAP**.
   4) Pulse **Aplicar** y luego **Guardar**.

c. En la Consola de administración, expanda **Seguridad**, luego expanda **Mecanismos de autenticación** y pulse **LTPA**.
   1) En la pestaña Configuración LTPA, especifique los valores LTPA según sea necesario.
   2) En Propiedades adicionales, pulse **Inicio de sesión único (SSO)** y quite la marca de selección del cuadro de selección **Habilitado** si no desea utilizar esta función.
   3) Pulse **Aplicar** y luego **Guardar**.

d. En la Consola de administración, expanda **Aplicaciones**, luego pulse **Aplicaciones de empresa**.
   1) En la ventana Aplicaciones de empresa, pulse su aplicación de comercio, *nombre_instancia_WC* (por ejemplo, `WC_demo`).
   2) En Propiedades adicionales, pulse **Correlacionar roles de seguridad con usuarios y grupos**.
   3) Pulse **Buscar usuarios** y localice al usuario cuyo rol desea correlacionar.
   4) Para dicho usuario, seleccione **WCSecurityRole** y pulse **Aceptar**.

3. Cierre la Consola de administración y detenga y reinicie la Consola de administración de WebSphere Application Server. A partir de ahora, cuando abra la Consola de administración de WebSphere Application Server, se le solicitará el ID y la contraseña de servidor de seguridad.
4. Abra el Gestor de configuración de WebSphere Commerce y seleccione **Instancias** > *nombre_instancia* > **Propiedades de instancia** > **Seguridad** y pulse el recuadro de selección **Habilitar**. Se le solicitará que entre el nombre de usuario y la contraseña que ha entrado en el paso 2b. Pulse **Aplicar** y, a continuación, salga del Gestor de configuración.
5. Detenga y reinicie WebSphere Application Server Consola de administración.

Habilitación de la seguridad con un registro de usuarios del sistema operativo

AIX Linux Solaris Para utilizar el sistema operativo como un registro de usuarios, WebSphere Application Server se ha de ejecutar con el ID `root`. Ejecute WebSphere Application Server como `root` y efectúe los pasos siguientes:

400 Windows Para habilitar la seguridad de WebSphere Application Server cuando utiliza la validación de usuario del sistema operativo como el registro de usuarios de WebSphere Application Server, conéctese como usuario con autorización de administrador y efectúe los pasos siguientes:

1. AIX Linux Solaris Conéctese como root.

2. AIX Linux Solaris Inicie WebSphere Application Server e inicie la Consola de administración de WebSphere Application Server mientras esté conectado como `root`. Para arrancar el servidor:

   ```
   cd dir_instalación_WAS/bin
   ./startServer server
   ```

   donde *server* es el nombre del servidor de aplicaciones WebSphere Application Server, por ejemplo, `server1`.

3. En la Consola de administración de WebSphere Application Server, modifique los valores de seguridad globales como se indica a continuación:

   a. En la Consola de administración, expanda **Seguridad**, expanda **Registros de usuarios** y pulse **Sistema operativo local**. Rellene los campos de la pestaña **Configuración** para su servidor del registro de seguridad, como se indica a continuación:

Nombre de campo	Valores de ejemplo	Notas
ID de usuario de servidor	*wcsuser*	400 El ID de usuario de iSeries debe tener la autorización `*SECOFR`. AIX Solaris Linux Un ID de usuario root o que tenga autorización root. Windows El ID de usuario con privilegios administrativos para el sistema operativo con el que se ha conectado. Si la máquina pertenece a un dominio, utilice el ID de usuario totalmente calificado. Por ejemplo: *DomainXYZ\id_usuario*. Asegúrese de que esta cuenta exista en el servidor de dominios y de que sea miembro del grupo del Administrador.
Contraseña de servidor de seguridad	*contraseña*	Es la contraseña que pertenece al usuario con privilegios administrativos de sistema operativo con el que se ha conectado.

   Pulse **Aplicar** y luego **Guardar**.

   b. En la Consola de administración, expanda **Seguridad** y pulse **Seguridad global**.

      1) En la pestaña Configuración de la seguridad global, seleccione **Habilitado** y borre la marca de selección de **Forzar la seguridad de Java 2**.

      2) En el campo Mecanismo de autenticación activo, seleccione **SWAM (Simple WebSphere Authentication Mechanism**.

3) En el campo Registro de usuarios activo, seleccione **Sistema operativo local**.
4) Pulse **Aplicar** y luego **Guardar**.

4. En la Consola de administración, expanda **Aplicaciones**, luego pulse **Aplicaciones de empresa**.
   a. En la ventana Aplicaciones de empresa, pulse su aplicación de comercio, *nombre_instancia_WC* (por ejemplo, `WC_demo`).
   b. En Propiedades adicionales, pulse **Correlacionar roles de seguridad con usuarios y grupos**.
   c. Pulse **Buscar usuarios** y localice al usuario cuyo rol desea correlacionar.
   d. Para dicho usuario, seleccione **WCSecurityRole** y pulse **Aceptar**.
5. Abra el Gestor de configuración de WebSphere Commerce y seleccione **Lista de instancias → *nombre_instancia* → Propiedades de instancia→ Seguridad** y seleccione el recuadro de selección **Habilitar seguridad**. Seleccione **Registro de usuarios del sistema operativo** para la modalidad de autenticación y para entrar el nombre de usuario y la contraseña que ha entrado en el paso 3a en la página 196. Pulse **Aplicar** y, a continuación, salga del Gestor de configuración.
6. Detenga y reinicie el servidor de administración de WebSphere Application Server. A partir de ahora, cuando abra la Consola de administración de WebSphere Application Server, se le solicitará el ID y la contraseña del Servidor de seguridad .

Inhabilitación de la seguridad de EJB de WebSphere Commerce

WebSphere Commerce Business Edition le permite inhabilitar la seguridad de EJB. Para inhabilitar la seguridad EJB de WebSphere Commerce, efectúe lo siguiente:

1. Inicie la Consola de administración de WebSphere Application Server.
2. En la Consola de administración, expanda **Seguridad** y pulse **Seguridad global**. En la pestaña Configuración de la seguridad global, borre la marca de selección del recuadro **Habilitado**.
3. Abra el Gestor de configuración de WebSphere Commerce y seleccione **Lista de instancias → *nombre_instancia* → Propiedades de instancia→ Seguridad** y elimine la marca de selección de **Habilitar seguridad**.
4. Salga de la Consola de administración de WebSphere Application Server.
5. Detenga y reinicie el servidor de administración de WebSphere Application Server.

Opciones de despliegue de seguridad de WebSphere Commerce

WebSphere Commerce soporta diversas configuraciones de despliegue de seguridad. La tabla siguiente ilustra las opciones de despliegue de seguridad disponibles.

Tabla 20. Escenarios de seguridad de una sola máquina

La seguridad de WebSphere Application Server está habilitada.	• Utilice el sistema operativo como registro de WebSphere Application Server. • Utilice la base de datos como registro de WebSphere Commerce.
	• Utilice LDAP como registro de WebSphere Application Server. • Utilice LDAP como registro de WebSphere Commerce.
	• Utilice LDAP como registro de WebSphere Application Server.
La seguridad de WebSphere Application Server está inhabilitada y el sitio de WebSphere Commerce está ubicado detrás de un cortafuegos.	• No se necesita un registro de WebSphere Application Server. • Utilice la base de datos como registro de WebSphere Commerce.
	• No se necesita un registro de WebSphere Application Server. • Utilice LDAP como registro de WebSphere Commerce.

Tabla 21. Escenarios de seguridad de varias máquinas

La seguridad de WebSphere Application Server está habilitada. LDAP se despliega siempre.	• Utilice LDAP como registro de WebSphere Application Server. • Utilice LDAP como registro de WebSphere Commerce.
	• Utilice LDAP como registro de WebSphere Application Server. • Utilice una base de datos como registro de WebSphere Commerce. • Necesitará configurar LDAP y poner una entrada administrativa en el registro de LDAP.
La seguridad de WebSphere Application Server está inhabilitada y el sitio de WebSphere Commerce está ubicado detrás de un cortafuegos.	• Utilice una base de datos como registro de WebSphere Commerce. • No se necesita un registro de WebSphere Application Server. • No se soporta el inicio de sesión único.
	• Utilice LDAP como registro de WebSphere Application Server. • No se necesita un registro de WebSphere Application Server.

Nota: Si el sitio de WebSphere Commerce funciona detrás de un cortafuegos, puede inhabilitar la seguridad de WebSphere Application Server. Sólo

deberá inhabilitar la seguridad de WebSphere Application Server si está seguro de que no se están ejecutando aplicaciones delictivas detrás del cortafuegos.

Configuración de la seguridad del Supervisor de antememoria dinámica

Si está utilizando el Supervisor de antememoria dinámica de WebSphere Application Server para supervisar y si la aplicación que está supervisando tiene definidos roles de seguridad en su descriptor de despliegue, debe realizar lo siguiente:

Vaya al panel ″Correlacionar roles de seguridad con usuarios y grupos) de la Consola de administración de WebSphere Application Server, pulse **Aplicaciones —> Instalar nueva aplicación** y realice los pasos necesarios (que no están relacionados con la seguridad). Para obtener más información, consulte el tema ″Despliegue de aplicaciones seguras″ y ″Asignación de usuarios y grupos a roles″ del InfoCenter de WebSphere Application Server (`http://www.ibm.com/software/webservers/appserv/infocenter.html`.) En el panel ″Correlacionar roles de seguridad con usuarios y grupos″:

1. Especifique los usuarios y grupos que están correlacionados con cada uno de los roles de seguridad.
2. Seleccione el recuadro de selección que hay junto a **Rol**, según sea necesario, para seleccionar todos los roles o para seleccionar roles individuales. Para cada rol, puede especificar si se correlacionan con el rol los usuarios definidos previamente como, por ejemplo, Todos o Todos autenticados. Para seleccionar usuarios o grupos específicos del registro de usuarios:
   a. Seleccione un rol y pulse **Buscar usuarios** o **Buscar grupos**.
   b. En el panel **Buscar usuarios** o **Buscar grupos** que se visualizará, escriba el criterio de búsqueda para obtener una lista de los usuarios o grupos del registro de usuarios.
   c. Seleccione grupos o usuarios individuales de la lista resultante.
   d. Pulse **Aceptar** para correlacionar los usuarios o grupos seleccionados con el rol que ha seleccionado en el panel ″Correlacionar roles de seguridad con usuarios o grupos″.

Actualmente, hay un rol definido que proporciona acceso a todas las funciones del supervisor de antememoria. Esto significa que se puede utilizar esta página para especificar los usuarios que pueden acceder al Supervisor de antememoria dinámica.

Administración de instancias de WebSphere Commerce mediante el Gestor de configuración

Si ha habilitado la seguridad global de WebSphere Application Server, debe realizar los pasos siguientes para detener, iniciar, crear o suprimir instancias de WebSphere Commerce o WebSphere Commerce Payments desde el Gestor de configuración:

1. En el directorio *dir_instalación_WAS*/properties, actualice los archivos y propiedades siguientes en los valores siguientes:
   - sas.client.props

     com.ibm.CORBA.securityEnabled=true

     com.ibm.CORBA.loginSource=properties

     com.ibm.CORBA.LoginUserid=validUser

com.ibm.CORBA.LoginPassword=validPassword

- soap.client.props

  com.ibm.SOAP.loginUserid=validUser

  com.ibm.SOAP.loginPassword=validPassword

  com.ibm.SOAP.secrityEnabled=true

2. En el directorio *dir_instalación_WAS*/bin ejecute el mandato PropFilePasswordEncoder (en una línea) para codificar la contraseña en los archivos sas.client.props y soap.client.props.

   AIX Linux Solaris

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

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

   400

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

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

   Windows

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

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

3. Actualice el script config_client:

   AIX 400 Linux Solaris Añada $CLIENTSOAP $CLIENTSAS a la lista de argumentos Java. Por ejemplo:

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

   Windows Añada %CLIENTSOAP% %CLIENTSAS% a la lista de argumentos Java. Por ejemplo:

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

4. Actualice el script config_server:

   AIX 400 Linux Solaris Añada $CLIENTSOAP $CLIENTSAS a la lista de argumentos Java. Por ejemplo:

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

   Windows Añada %CLIENTSOAP% %CLIENTSAS% a la lista de argumentos Java. Por ejemplo:

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

Capítulo 17. Habilitación de SSL para producción con IBM HTTP Server

400 Esta sección no se aplica a la plataforma iSeries. Para obtener información sobre iSeries, consulte el apartado "Habilitación de SSL en IBM HTTP Server (iSeries)" en la página 208.

Después de crear la instancia de WebSphere Commerce con IBM HTTP Server, SSL está habilitado para realizar pruebas. Antes de abrir el sitio a los compradores, deberá habilitar SSL para producción siguiendo los pasos de este capítulo.

Acerca de la seguridad

IBM HTTP Server proporciona un entorno seguro para las transacciones comerciales utilizando la tecnología de cifrado. El cifrado es la codificación de las transacciones de información en Internet para que éstas no se puedan leer hasta que el receptor las descodifique. El remitente utiliza un patrón algorítmico o clave para codificar (cifrar) una transacción y el receptor utiliza una clave de descifrado. Estas claves las utiliza el protocolo SSL (Secure Sockets Layer).

El servidor Web utiliza un proceso de autenticación para verificar la identidad de la persona con la que se están realizando negocios (es decir, para asegurarse de que dicha persona es quien afirma ser). Esto implica la obtención de un certificado firmado por un tercero fiable denominado autoridad de certificación (CA). Para los usuarios de IBM HTTP Server, la CA puede ser Equifax® o VeriSign® Inc. También se dispone de otras CA.

Para crear un archivo de claves de producción, realice los pasos siguientes:

1. Configure un archivo de claves de seguridad para producción.
2. Solicite un certificado seguro a una autoridad de certificación.
3. Establezca el archivo de claves de producción como archivo de claves actual.
4. Reciba el certificado y pruebe el archivo de claves de producción.

Estos pasos se describen detalladamente a continuación.

Notas:

1. Si ya está utilizando un archivo de claves de producción firmado por una autoridad de certificación, es posible que pueda saltarse estos pasos. Para determinarlo, lea este capítulo.
2. Mientras realice estos pasos, puede que el navegador muestre mensajes de seguridad. Examine cuidadosamente la información de cada mensaje y decida cómo debe continuar.

Configuración de un archivo de claves de seguridad para producción

Para configurar un archivo de claves de seguridad para producción, realice lo siguiente en la máquina servidor Web:

1. Detenga IBM HTTP Server.
2. Vaya al subdirectorio `conf` bajo el subdirectorio de instalación de IBM HTTP Server de la máquina.

3. Cree una copia de seguridad del archivo `httpd.conf` y asígnele el nombre `httpd.conf.backup` al archivo de copia de seguridad.
4. Abra `httpd.conf` en un editor de texto.
5. Descomente las líneas siguientes (suprimiendo el signo de almohadilla, "#", al comienzo de la línea) para el puerto 443:
   - Windows
     a. `LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll`
     b. `Listen 443`
     c. `<VirtualHost sistpral.algún_dominio.com:443>` (En esta línea también debe sustituir el nombre de sistema principal totalmente calificado.)
     d. `SSLEnable`
     e. `</VirtualHost>`
     f. `Keyfile "dir_instalación_HTTPServer/ssl/keyfile.kdb"`
   - AIX Linux Solaris
     a. `LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so`
     b. `AddModule mod_ibm_ssl.c`
     c. `Listen 443`
     d. `<VirtualHost sistpral.algún_dominio.com:443>` (En esta línea también debe sustituir el nombre de sistema principal totalmente calificado.)
     e. `SSLEnable`
     f. `</VirtualHost>`
     g. `SSLDisable`
     h. `Keyfile "dir_instalación_HTTPServer/ssl/keyfile.kdb"`
     i. `SSLV2Timeout 100`
     j. `SSLV3Timeout 1000`
6. Descomente las líneas siguientes (suprimiendo el signo de almohadilla, "#", al comienzo de la línea):
   a. Para las herramientas administrativas de WebSphere Commerce necesita los puertos 8000, 8002 y 8004:

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

      Si está utilizando WebSphere Commerce Payments, necesitará también los puertos 5432 y 5433:

      ```
      Listen 5432
      Listen 5433
      ```

   b. Asegúrese de que las secciones de sistema principal virtual de los puertos anteriores también estén descomentadas (suprimiendo los signos de almohadilla, "#", al comienzo de las líneas si los hubiera). En estas secciones también debe sustituir el nombre de sistema principal totalmente calificado. Para obtener una lista de las variables de nombre de vía de acceso por omisión en los ejemplos siguientes, consulte el apartado "Variables de vía de acceso" en la página ix.

Los ejemplos siguientes se han sacado de las secciones de sistema principal virtual no comentadas de un archivo `httpd.conf` del sistema Windows. Estas secciones son similares en otros sistemas operativos.

```
########## IBM WebSphere Payments (No edite esta sección) #################
Listen 5432
Listen 5433
########## Fin de IBM WebSphere Payments (No edite esta sección) ##########

...

########## IBM WebSphere Commerce (No edite esta sección) #################
Listen 8000
Listen 8002
Listen 8004
########## Fin de IBM WebSphere Commerce (No edite esta sección) ##########
```

Figura 7. Ejemplo de secciones "Listen" de un archivo httpd.conf

```
########## Fin de IBM WebSphere Commerce (No edite esta sección) ##########
## VirtualHost: Permite que el daemon responda a las peticiones de más de
## una dirección de servidor, si se ha configurado la máquina de servidor para que acepte paquetes IP
## para varias direcciones. Puede realizarse con el distintivo de alias ifconfig
## o mediante parches de kernel como, por ejemplo, VIF.
#
## En un mandato VirtualHost puede incluirse cualquier directiva
httpd.conf o srm.conf.
## Consulte también la entrada BindAddress.
#
#<VirtualHost sistpral.algún_dominio.com:443>
```

Figura 8. Ejemplo de secciones de cabeceras "virtual host" de un archivo httpd.conf

```
########## IBM WebSphere Payments (No edite esta sección) #################
<VirtualHost sistpral.algún_dominio.com:5433>
SSLEnable
SSLClientAuth 0
ServerName wordsworth.torolab.ibm.com
DocumentRoot
"dir_instalación_HTTPServer\htdocs\en_US"
</VirtualHost>
########## Fin de IBM WebSphere Payments (No edite esta sección) ##########
```

Figura 9. Ejemplo de sección "virtual host" del archivo httpd.conf para Payments

```
########## IBM WebSphere Commerce (No edite esta sección) #################
#Instance name : nombre_instancia
<VirtualHost sistpral.algún_dominio.com:80>
ServerName sistpral.algún_dominio.com
DocumentRoot
"dir_instalación_HTTPServer/htdocs/en_US"
Alias /wcsdoc   "dir_instalación_WC/web/doc"
Alias /wcsstore  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/Stores.war"
Alias /wcs   "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war"
</VirtualHost>
```

Figura 10. Ejemplo de sección "virtual host" del archivo httpd.conf para el puerto 80 de WebSphere Commerce. (Puerto no protegido)

```
<VirtualHost sistpral.algún_dominio.com:443>
SSLEnable
SSLClientAuth 0
ServerName sistpral.algún_dominio.com
DocumentRoot
"dir_instalación_HTTPServer/htdocs/en_US"
Alias /wcsdoc   "dir_instalación_WC/web/doc"
Alias /wcsstore  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/Stores.war"
Alias /wcs   "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war"
</VirtualHost>
```

Figura 11. Ejemplo de sección "virtual host" del archivo httpd.conf para el puerto 44 de WebSphere Commerce. (Puerto protegido)

```
<VirtualHost sistpral.algún_dominio.com:8000>
SSLEnable
SSLClientAuth 0
ServerName sistpral.algún_dominio.com
DocumentRoot
"dir_instalación_HTTPServer/htdocs/en_US"
Alias /wcsdoc   "dir_instalación_WC/web/doc"
Alias /wchelp   "dir_instalación_WC/web/doc/en_US"
Alias /adminconsole  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/Stores.war"
Alias /accelerator  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war"
Alias /wcadmin  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/SiteAdministration.war"
Alias /wcorgadmin  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/OrganizationAdministration.war"
Alias /orgadminconsole "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

Figura 12. Ejemplo de sección "virtual host" del archivo httpd.conf para el puerto 800 de WebSphere Commerce. (WebSphere Commerce Accelerator)

```
<VirtualHost sistpral.algún_dominio.com:8002>
SSLEnable
SSLClientAuth 0
ServerName sistpral.algún_dominio.com
DocumentRoot
"dir_instalación_HTTPServer/htdocs/en_US"
Alias /wcsdoc   "dir_instalación_WC/web/doc"
Alias /wchelp   "dir_instalación_WC/web/doc/en_US"
Alias /adminconsole  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/Stores.war"
Alias /accelerator  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war"
Alias /wcadmin  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/SiteAdministration.war"
Alias /wcorgadmin  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/OrganizationAdministration.war"
Alias /orgadminconsole "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
```

Figura 13. Ejemplo de sección "virtual host" del archivo httpd.conf para el puerto 8002 de WebSphere Commerce. Consola de administración de WebSphere Commerce

```
<VirtualHost sistpral.algún_dominio.com:8004>
SSLEnable
SSLClientAuth 0
ServerName sistpral.algún_dominio.com
DocumentRoot
"dir_instalación_HTTPServer/htdocs/en_US"
Alias /wcsdoc   "dir_instalación_WC/web/doc"
Alias /wchelp   "dir_instalación_WC/web/doc/en_US"
Alias /adminconsole  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/SiteAdministration.war/tools/adminconsole/wcsadmincon.html"
Alias /wcsstore  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/Stores.war"
Alias /accelerator  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war/tools/common/accelerator.html"
Alias /wcs   "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/CommerceAccelerator.war"
Alias /wcadmin  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/SiteAdministration.war"
Alias /wcorgadmin  "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/OrganizationAdministration.war"
Alias /orgadminconsole "dir_instalación_WAS\installedApps\spral\WC_nombre_instancia.ear/OrganizationAdministration.war/tools/buyerconsole/wcsbuyercon.html"
</VirtualHost>
########## Fin de IBM WebSphere Commerce (No edite esta sección) ##########
```

Figura 14. Ejemplo de sección "virtual host" del archivo httpd.conf para el puerto 8004 de WebSphere Commerce. Consola de administración de WebSphere Commerce

Nota: Se recomienda que el software de cortafuegos bloquee el acceso externo al puerto que ha configurado para las Herramientas de WebSphere Commerce (puertos 8000, 8002 y 8004 por omisión). Consulte la documentación para el software de cortafuegos que esté utilizando en el sitio para obtener información sobre cómo realizar dicha tarea.

7. Guarde los cambios.
8. Para asegurarse de que el archivo `httpd.conf` no contiene errores de sintaxis:

   AIX Linux Solaris Vaya al subdirectorio `bin` del directorio de instalación de IBM HTTP Server de la máquina y ejecute el mandato siguiente:
   ```
   ./httpd -t
   ```

   Windows Vaya al directorio de instalación de IBM HTTP Server de la máquina y ejecute el mandato siguiente:
   ```
   apache -t
   ```
9. Inicie IBM HTTP Server.

Solicitud de un certificado seguro a una autoridad de certificación

Para validar el archivo de claves de seguridad que acaba de crear en el paso anterior, necesita un certificado de una autoridad de certificación (CA), por ejemplo Equifax o VeriSign. El certificado contiene la clave pública del servidor, el Nombre distinguido asociado al certificado del servidor y el número de serie y la fecha de caducidad del certificado.

Si desea utilizar una CA diferente, póngase en contacto con ella directamente para obtener información sobre el procedimiento que debe seguir.

Usuarios de Equifax

Para solicitar un certificado de servidor seguro a Equifax, consulte la dirección Web siguiente y siga las instrucciones que se proporcionan:

`http://www.equifax.com`

Deberá recibir de Equifax el certificado de servidor de seguridad por correo electrónico en un periodo de 2 a 4 días laborables.

Usuarios de VeriSign

Para solicitar un certificado de servidor seguro a VeriSign, consulte el URL siguiente y siga las instrucciones que se proporcionan:

`http://www.verisign.com`

AIX Aunque esté utilizando los procedimientos para IBM HTTP Server, siga el enlace para ICCS (**Internet Connection Secure Server**). Siga las instrucciones que se proporcionan. Cuando reciba el certificado, cree el archivo de claves de producción tal como se describe en el apartado anterior, si aún no lo ha creado.

Solaris ç Aunque esté utilizando los procedimientos para IBM HTTP Server, siga el enlace para ICCS (**Internet Connection Secure Server**). La página que aparece a continuación indica que los procedimientos se aplican a las plataformas OS/2 y AIX. Estas instrucciones también se aplican para el software Solaris.

Siga las instrucciones que se proporcionan. Una vez que haya sometido la petición, el certificado deberá llegar en un periodo de tiempo de tres a cinco días laborables. Cuando lo reciba, cree el archivo de claves de producción tal como se describe en el apartado anterior, si aún no lo ha creado.

Cómo recibir el archivo de claves de producción y configurarlo como el archivo de claves actual

Cuando llegue el certificado de la CA, tendrá que hacer que el servidor Web utilice el archivo de claves de producción. Realice los pasos siguientes:

1. Copie los archivos *nombrecertificado*`.kdb`, *nombrecertificado*`.rdb` y *nombrecertificado*`.sth` que ha recibido de la autoridad de certificación en el subdirectorio `ssl` bajo la vía de acceso de instalación de IBM HTTP Server de la máquina, donde *nombrecertificado* es el nombre de certificado que ha proporcionado con la petición de certificado.
2. Detenga IBM HTTP Server.
3. AIX Solaris Exporte `JAVA_HOME` ejecutando los mandatos siguientes:

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

   donde *nombre_sistema_principal* es el nombre de sistema principal totalmente calificado de la máquina que está utilizando actualmente y *java_home* es:

   - AIX `/usr/java130`
   - Solaris `/opt/WebSphere/AppServer/java131`
4. Abra el programa de utilidad de gestión de claves IKeyman.
5. Abra el archivo *nombrecertificado*`.kdb` y entre la contraseña cuando se le solicite.
6. Seleccione **Certificados personales** y pulse **Recibir**.
7. Pulse **Examinar**.
8. Seleccione la carpeta donde ha almacenado los archivos que ha recibido de la autoridad de certificación. Seleccione el archivo *nombrecertificado*`.txt` y pulse **Aceptar**.
9. El recuadro de lista **Certificados personales** debe listar ahora el certificado *nombrecertificado* de Verisign o el certificado *nombrecertificado* de Equifax.
10. Salga del Programa de utilidad de gestión de claves.

11. Cambie de directorio y vaya al subdirectorio `conf` bajo la vía de acceso de instalación de IBM HTTP Server de la máquina.
12. Cree una copia de seguridad de `httpd.conf`.
13. Abra `httpd.conf` en un editor de texto.
14. Asegúrese de que las líneas listadas en el paso 5 en la página 202 no estén comentadas.
15. Busque la directiva `Keyfile "`*`vía_acceso_archivo_claves`*`/keyfile.kdb"` y cambie el nombre de vía de acceso para que apunte al archivo que ha creado en los pasos anteriores.
16. Reinicie IBM HTTP Server.

Prueba del archivo de claves de producción

Para probar la clave de producción, realice lo siguiente:

1. Vaya al URL siguiente con el navegador:

   `https://`*`nombre_sistema_principal`*

   Notas:

   a. Si ha personalizado el servidor Web, puede que necesite escribir el nombre de la página frontal del servidor Web después del nombre de sistema principal.
   b. Asegúrese de escribir `https`, *no* `http`.

   Si la clave está definida correctamente, verá varios mensajes acerca del nuevo certificado.
2. Si desea aceptar este certificado, en el panel **Nuevo certificado de sitio** seleccione el botón de selección **Aceptar este certificado para siempre (hasta que caduque)**.
3. Desde el navegador Web, restaure los valores de servidor de antememoria y proxy (o socks) a sus estados originales.

SSL ya está habilitado en el servidor.

Consideraciones sobre SSL para WebSphere Commerce Payments

Por omisión, la comunicación entre WebSphere Commerce y WebSphere Commerce Payments se efectúa a través de SSL. No obstante, si inicia directamente la interfaz de usuario de WebSphere Commerce Payments del modo siguiente estará invocando WebSphere Commerce Payments utilizando comunicaciones que no son de SSL:

`http:``//`*`nombre_sistema_principal`*`:`*`número_puerto`*`/webapp/PaymentManager`

donde *nombre_sistema_principal* es el nombre de la máquina servidor de Payments y *número_puerto* es 5432 (por omisión).

Para asegurarse de que la comunicación es a través de SSL, utilice el URL siguiente:

`https:``//`*`nombre_sistema_principal`*`:`*`número_puerto`*`/webapp/PaymentManager`

donde *nombre_sistema_principal* es el nombre de la máquina servidor de Payments y *número_puerto* es 5433 (por omisión).

Aumento de la confidencialidad

Cuando WebSphere Commerce recibe una petición URL, el controlador Web recupera el nombre de la interfaz para el mandato de controlador solicitado y lo utiliza para buscar el nombre de clase de implementación en la tabla CMDREG. Asimismo determina si es necesario el protocolo HTTPS (protegido) para las peticiones URL comprobando la columna HTTPS de la tabla URLREG.

Cualquier mandato que visualice información confidencial deberá tener el valor HTTPS igual a "1" (uno) en la tabla URLREG. Por ejemplo, un mandato de vista OrderProcessView que contenga información detallada sobre un pedido de un cliente solamente se puede transmitir a través del protocolo HTTPS y, por lo tanto, el valor de la entrada OrderProcessView de la tabla URLREG será "1" (uno) en la columna HTTPS.

Habilitación de SSL en IBM HTTP Server (iSeries)

400 Este apartado se aplica a la plataforma iSeries.

SSL es un protocolo de seguridad. SSL asegura que los datos transferidos entre un cliente y un servidor permanezcan privados. Permite que el cliente autentique la identidad del servidor y que el servidor autentique la identidad del cliente.

Los certificados digitales son documentos electrónicos que autentican los servidores y clientes involucrados en las transacciones seguras por Internet. El emisor de certificados digitales se denomina Autoridad de certificación (CA). El sistema iSeries puede efectuar el rol de una CA en un entorno de Intranet emitiendo certificados de servidor y de cliente y funcionar como un servidor autenticado con certificados de servidor emitidos por una CA de iSeries o una CA de Internet como VeriSign. Como servidor Web, también se puede configurar IBM HTTP Server para iSeries para que solicite certificados de cliente para autenticar los clientes habilitados SSL.

Para obtener información detallada sobre cómo habilitar SSL en IBM HTTP Server para iSeries, consulte el Centro de información de iSeries (http://publib.boulder.ibm.com/html/as400/infocenter.html). Cuando esté en este sitio, seleccione la versión del sistema operativo y el idioma y luego pulse **Ir**. Busque el tema "Protección de aplicaciones con SSL" para obtener información sobre cómo habilitar SSL.

Utilización de SSL con WebSphere Commerce Payments

Si crea la tienda de certificados del sistema después de crear la instancia de WebSphere Commerce debe conceder acceso a la misma a la instancia de WebSphere Commerce Payments y a la instancia de WebSphere Commerce. Por ejemplo, los mandatos siguientes concederán el acceso necesario a la instancia de WebSphere Commerce Payments en un sistema V5R1:

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

y los mandatos siguientes otorgan, a WebSphere Commerce, el acceso necesario en un sistema V5R1:

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

Si opta por utilizar una instancia de WebSphere Commerce Payments remota, deberá configurar tanto la instancia de WebSphere Commerce como la instancia de WebSphere Commerce Payments para que acepten la autoridad de certificación remota que ha emitido el certificado digital. Para establecer una relación de confianza entre dos aplicaciones remotas, consulte el siguiente procedimiento general:

1. En la máquina de WebSphere Commerce, utilice el gestor de certificados digitales para exportar la autoridad de certificación del servidor.
2. Transfiera el archivo de certificados a la máquina de WebSphere Commerce Payments.
3. En la máquina de WebSphere Commerce Payments, utilice el gestor de certificados digitales para importar la autoridad de certificación del servidor WebSphere Commerce.
4. Configure el servidor de aplicaciones de WebSphere Commerce Payments para que acepte la autoridad de certificación del servidor WebSphere Commerce importado.
5. En la máquina de WebSphere Commerce Payments, utilice el gestor de certificados digitales para exportar la autoridad de certificación del servidor.
6. Transfiera el archivo de certificados a la máquina de WebSphere Commerce.
7. En la máquina de WebSphere Commerce, utilice el gestor de certificados digitales para importar la autoridad de certificación del servidor de WebSphere Commerce Payments.
8. Configure el servidor de aplicaciones de WebSphere Commerce para que acepte la autoridad de certificación del servidor WebSphere Commerce Payments importado.

Para obtener información detallada, consulte la página Web de la biblioteca técnica de WebSphere Commerce (`http://www.software.ibm.com/software/commerce/wscom/library/lit-tech.html`) y busque **Hints and Tips**.

Capítulo 18. Habilitación de SSL para IBM Directory Server (LDAP)

Los siguientes son los pasos para configurar la seguridad SSL para IBM Directory Server y WebSphere Commerce.

Configuración de IBM Directory Server

400 Este apartado no se aplica a la plataforma iSeries. Para obtener información sobre iSeries, consulte el apartado "Configuración de IBM OS/400 Directory Services en la plataforma iSeries".

Para configurar IBM Directory Server:

1. Instale IBM Directory Server siguiendo las instrucciones del producto IBM Directory Server. Asegúrese de instalar el componente GSKit.
2. Una vez completada la instalación, inicie el Gestor de claves de IBM ejecutando el ejecutable gsk5ikm.
3. Cree un archivo de base de datos de claves CMS nuevo. Asegúrese de que **ocultar la contraseña para un archivo** esté seleccionado (por ejemplo `ldap_key.kdb`)
4. Cree un certificado autofirmado utilizando X509 Versión 3 y el tamaño de clave 1024. Puede asignar al certificado una etiqueta con algún significado como, por ejemplo, su nombre.
5. Extraiga el certificado como un archivo de certificado, por ejemplo `cert.arm`, utilizando el tipo de datos `Datos ASCII codificados de base 64`.
6. En un navegador vaya a la siguiente dirección: `http://`*`nombre_sistema_principal`*`/ldap`, donde *nombre_sistema_principal* es el nombre de la máquina del servidor LDAP.
7. Pulse **Seguridad —> SSL —> Valores** y realice los cambios siguientes:
   - Estado de SSL: SSL activo o SSL sólo
   - Método de autenticación: Autenticación de servidor
   - Puerto seguro: 636
   - Vía de acceso y nombre de archivo de base de datos de claves:

     AIX Linux Solaris `/Keys/ldap_key.kdb`

     Windows *`unidad`*`:\Keys\ldap_key.kdb`
   - Etiqueta de clave: *su_etiqueta*. La etiqueta del certificado.
   - Contraseña de clave: *xxxxx*. La contraseña del archivo de base de datos de claves CMS. Si selecciona **Ocultar la contraseña para un archivo**, no necesitará entrar la contraseña.
8. Pulse **Actualizar** y reinicie SecureWay.

Configuración de IBM OS/400 Directory Services en la plataforma iSeries

400 Para configurar IBM OS/400 Directory Services en iSeries:

1. Instale IBM iSeries Access para Windows.

2. Inicie iSeries Navigator en una máquina Windows seleccionando **Inicio** —> **Programas** —> **IBM iSeries Access para Windows** —> **iSeries Navigator**.
3. Cree una conexión con la máquina iSeries de destino si no hay ninguna conexión con la máquina.
4. Expanda la máquina de destino en el panel de la izquierda y luego expanda **Red** —> **Servidores** en el panel de la izquierda.
5. Pulse **TCP/IP** en el panel de la izquierda.
6. Pulse con el botón derecho en **Directorio** en el panel derecho y seleccione **Propiedades** en el menú emergente.
7. En la ventana Propiedades del directorio, pulse la pestaña **Red**.
8. Pulse **Gestor de certificados digitales** para iniciar el Gestor de certificados digitales y asignar un certificado a la aplicación `Directory Services Server`".
9. Después de asignar el certificado a Directory Services Server, pulse **Aceptar** para cerrar la ventana Propiedades del directorio.
10. Vuelva a abrir la ventana de propiedades del directorio y verá que SSL (Secure Socket Layer) está habilitado. Puede aceptar los valores por omisión:
    - Estado de SSL:
    - Método de autenticación: Autenticación de servidor
    - Puerto seguro: 636
11. Reinicie Directory Services Server.

Asignación e importación de un certificado autofirmado a WebSphere Application Server

400 Si su certificado SSL no lo ha emitido una autoridad de certificación (CA) como, por ejemplo, VeriSign o Thwate, debe exportar la CA local desde una máquina iSeries e importarla al almacén de claves de confianza por omisión de la máquina WebSphere Commerce. Para habilitar SSL con el certificado local iSeries y exportar la CA local desde una máquina iSeries, haga lo siguiente:

1. Asegúrese de que el servidor `HTTP *Admin` esté ejecutándose. Si no lo está, ejecute:
   ```
   STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)
   ```
2. Abra la página Tareas de iSeries yendo con el navegador a la dirección siguiente: `http://nombre_sistema_principal:2001`.
3. Seleccione **Gestor de certificados digitales**.
4. Pulse en **Seleccionar un almacén de certificados**.
5. En el Almacén de certificados, seleccione ***System**.
6. Si no ve el enlace **Instalar certificado de CA local en el PC**, debe crear una CA local:
   a. Pulse Crear una autoridad de certificación (CA).
   b. Reinicie `*Admin` HTTP Server en iSeries.
   c. Cree el certificado nuevo con un tipo de Cliente o de Servidor.
   d. Seleccione la Autoridad de certificación local que acaba de crear.
   e. Asigne este certificado a Directory Services Server.
7. Pulse **Instalar certificado de CA local en el PC**.
8. Pulse Instalar certificado. A continuación, guarde el certificado (archivo `.cer`) en una carpeta temporal.

9. Importe la autoridad de certificación (archivo .cer) a Microsoft Internet Explorer y, a continuación, vuelva a exportar la autoridad de certificación como un archivo .cer (codificación binaria 64) en un directorio temporal.
10. Importe el certificado (codificación binaria 64) al almacén de claves de confianza de WebSphere Application Server. Por ejemplo:

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

WebSphere Application Server

En WebSphere Application Server:

1. Inicie el programa IKeyMan (IBM Key Manager) que se proporciona con WebSphere Application Server. Puede encontrarlo en el menú de WebSphere Application Server o puede escribir directamente ikeyman en una ventana de mandatos.

   Nota: Este programa IBM Key Manager es diferente del que proporciona SecureWay

   La contraseña por omisión es 'changeit'.
2. Abra el almacén de claves carcerts WebSphere Application Server (por ejemplo, *dir_instalación_WAS*\AppServer\java\jre\lib\security\cacerts en Windows)
3. Marque **Certificados de firmante**, a continuación pulse **Añadir**. Utilice el tipo de datos **Datos ASCII codificados de base 64** y seleccione el archivo de certificados que ha creado en el paso 5 en la página 211.
4. Escriba un nombre para el certificado.
5. Cierre IKeyMan.

WebSphere Commerce

Si desea configurar WebSphere Commerce para que funcione con SecureWay Directory Server, deberá modificar el archivo *instancia*.xml:

1. Añada una variable de entorno JNDI nueva:

   ```
   java.naming.security.protocol = ssl
   ```
2. Cambie LdapPort a 636:

   ```
   LdapPort = 636
   ```
3. Reinicie WebSphere Commerce.

El siguiente es un ejemplo:

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

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

```
    . . . .
   />

</MemberSubSystem>
```

Parte 6. Apéndices

Apéndice. Políticas y grupos de control de acceso por omisión

El apéndice lista las políticas y grupos por omisión que se proporcionan con WebSphere Commerce.

Políticas de control de acceso por omisión

Las políticas de control de acceso por omisión están organizadas en las categorías siguientes:

- **Políticas basadas en roles:** las políticas basadas en roles para cada rol por omisión. También se hace referencia a estas políticas como políticas a nivel de mandatos ya que definen quién puede ejecutar los mandatos.
- **Políticas a nivel de recursos:** las políticas a nivel de recursos están agrupadas por área de negocio. Estas políticas definen las acciones que puede realizar un grupo de usuarios en recursos específicos. Bajo cada área de negocio, las políticas se organizan según el tipo de recurso que regulan:
  - **Recursos de datos** - los objetos de negocio que se pueden manipular como, por ejemplo, un pedido o una oferta de compra.
  - **Recursos de beans de datos** - contienen información acerca de los objetos de negocio. Los beans de datos se utilizan para visualizar información acerca de los objetos de una página Web.

Tabla 22. Dónde puede encontrar información sobre políticas

Políticas	**Comienza en**
Políticas basadas en roles	“Políticas basadas en roles” en la página 218
Políticas a nivel de recursos por área de negocio	“Políticas a nivel de recursos por área de negocio” en la página 221
Pedidos	“Pedidos” en la página 221
Intercambio (contratos)	“Intercambio (Contratos)” en la página 222
Aprobaciones	“Aprobaciones” en la página 223
Subastas	“Subastas” en la página 223
Business Intelligence	“Business Intelligence” en la página 223
Miembros	“Miembros” en la página 223
Marketing	“Marketing” en la página 224
Catálogo	“Catálogo” en la página 225
Conectividad y notificación	“Conectividad y notificación” en la página 225
Compras	“Compras” en la página 226
Cupones	“Cupones” en la página 226
Perfiles de clientes	“Perfiles de clientes” en la página 226
Descuentos	“Descuentos” en la página 226
Inventario planificado	
Gestión de inventario	
Gestión de pedidos	“Gestión de pedidos” en la página 227
Pagos	“Pagos” en la página 227
Editor de políticas	“Editor de políticas” en la página 228
Asesor de productos	“Asesor de productos” en la página 228
RFQ	“RFQ” en la página 228

Tabla 22. Dónde puede encontrar información sobre políticas (continuación)

Políticas	Comienza en
Normas	"Normas" en la página 228
Planificador	"Planificador" en la página 229
Commerce Accelerator	"Commerce Accelerator" en la página 229
Envío	"Envío" en la página 229
Impuestos	"Impuestos" en la página 229
Ayuda en directo/Espacio de trabajo colaborativo/Atención al cliente	"Ayuda en directo/Espacios de trabajo colaborativos/Atención al cliente" en la página 229
Estado de la tienda	"Estado de la tienda" en la página 230
Gestión de tiendas	

Políticas basadas en roles

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

- CategoryManagersExecuteCategoryManagersViews
- CustomersExecuteCustomersViews
- ProductManagersExecuteProductManagersViews
- PickPackersExecutePickPackersViews
- ReceiversExecuteReceiversViews
- ReturnsAdministratorsExecuteReturnsAdministratorsViews
- OperationsManagersExecuteOperationsManagersViews
- LogisticsManagersExecuteLogisticsManagersViews
- SellerAdministratorsExecuteSellerAdministratorsViews
- SellersExecuteSellersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersViews
- NonRejectedUsersExecuteNonRejectedUsersViews
- GuestUsersExecuteGuestUsersViews
- RegisteredApprovedUsersExecuteRegisteredApprovedUsersCommandsResourceGroup
- ChannelManagersExecuteChannelManagersCommands
- AllUsersExecuteAllSiteUserCmdResourceGroup
- AllUsersExecuteAllSiteUsersViews
- RegisteredCustomersForOrgExecuteRegisteredUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredUserViews
- ChannelManagersExecuteChannelManagersViews
- AllUsersExecuteResellerUserCmdResourceGroup
- AllUsersExecuteResellerUserViews
- RegisteredCustomersForOrgExecuteRegisteredResellerUserCmdResourceGroup
- RegisteredCustomersForOrgExecuteRegisteredResellerUserViews

La tabla siguiente muestra las políticas basadas en roles por rol, grupo de acceso, grupo de recursos y vista.

Notas:

1. La mayor parte de los elementos de la tabla, excepto la columna **Rol**, se han dividido en cada casilla para visualizarlos mejor ya que son muy largos.
2. No todos los roles siguientes son roles definidos en WebSphere Commerce. Para obtener más información sobre los roles de WebSphere Commerce definidos, consulte el apartado "Roles" en la página 32.

Tabla 23. Políticas basadas en roles por rol, grupo de acceso, grupo de recursos y vista.

Rol	Grupo de acceso utilizado en políticas basadas en roles	Grupo de recursos utilizado en las políticas basadas en roles para mandatos de controlador	Grupo de acciones utilizado en las políticas basadas en roles para Vistas
Administrador de sitio	SiteAdministrators	no disponible	no disponible
Administrador de compradores	BuyerAdministrators	BuyerAdministrators CommandsResourceGroup	BuyerAdministratorsViews
Aprobador de compradores	BuyerApprovers	BuyerApproversCmd ResourceGroup	BuyerApproversViews
Invitado[1]	Guests	GuestUsersCmd ResourceGroup	GuestUsersViews

Tabla 23. Políticas basadas en roles por rol, grupo de acceso, grupo de recursos y vista. (continuación)

Rol	Grupo de acceso utilizado en políticas basadas en roles	Grupo de recursos utilizado en las políticas basadas en roles para mandatos de controlador	Grupo de acciones utilizado en las políticas basadas en roles para Vistas
Representante de servicio al cliente	CustomerService Representatives	CustomerService RepCmdResourceGroup	CustomerService Representative Views
Director de marketing	MarketingManagers	MarketingManager CmdResourceGroup	MarketingManagersViews
Supervisor de servicio al cliente	CustomerService Supervisors	CustomerService Supervisor CmdResourceGroup	CustomerService SupervisorViews
Representante de cuentas	Account Representatives	AccountRepresentativesCmd ResourceGroup	AccountRepresentatives Views
Director de ventas	SalesManagers	SalesManagersCmd ResourceGroup	SalesManagersViews
Jefe de producto	ProductManagers	ProductManagers CmdResourceGroup	ProductManagersViews
Administrador de vendedores	Vendedor Administrators	SellerAdministrators CommandsResourceGroup	SellerAdministrators Views
Vendedor	Sellers	SellersCmdResourceGroup	SellersViews
Gestor de categorías	CategoryManagers	CategoryManagers CmdResourceGroup	CategoryManagersViews
Comprador (parte compradora)	Buyers(buy-side)	Buyers(buy-side) CommandsResourceGroup	Buyers(buy-side)Views
Comprador (parte vendedora)	Buyers(sell-side)	Buyers(sell-side) CommandsResourceGroup	Buyers (sell-side)Views
Empaquetador	PickPackers	PickPackersCmd ResourceGroup	PickPackersViews
Receptor	Receivers	ReceiversCmdResourceGroup	ReceiversViews
Administrador de devoluciones	ReturnsAdministrators	ReturnsAdministratorsCmd ResourceGroup	ReturnsAdministrators Views
Director de operaciones	OperationsManagers	OperationsManagersCmd ResourceGroup	OperationsManagersViews
Director de logística	LogisticsManagers	LogisticsManagersCmd ResourceGroup	LogisticsManagersViews
Responsable de compras	ProcurementBuyers	ProcurementBuyersCmd ResourceGroup	no disponible
Usuario registrado y aprobado[2]	RegisteredApproved Users	RegisteredApprovedUsers CommandsResourceGroup	RegisteredApproved UsersViews
Usuario no rechazado[3]	NonRejectedUsers	NonRejectedUserCommands ResourceGroup	NonRejectedUsersViews
Gestor de canales	ChannelManagers	ChannelManagersCmd ResourceGroup	ChannelManagersViews

Tabla 23. Políticas basadas en roles por rol, grupo de acceso, grupo de recursos y vista. (continuación)

Rol	Grupo de acceso utilizado en políticas basadas en roles	Grupo de recursos utilizado en las políticas basadas en roles para mandatos de controlador	Grupo de acciones utilizado en las políticas basadas en roles para Vistas
Todos los usuarios[4]	AllUsers	ResellerUserCmd ResourceGroup[5]	ResellerUserViews[5]
		AllSiteUserCmd ResourceGroup[6]	AllSiteUsersViews[6]
Cliente registrado (con el calificador de rol OrgandAncestorOrgs)	Registered CustomersForOrg	RegisteredUserCmd ResourceGroup	RegisteredUserViews
		RegisteredResellerUser CmdResourceGroup	RegisteredReseller UserViews

Notas:

1. "Invitado" no es un rol verdadero. Los usuarios cuyo estado de registro se ha establecido en "G" (la columna USER.REGISTERTYPE se ha establecido explícitamente en "G") pertenecen de forma implícita al grupo de acceso Guests.
2. "Usuario registrado y aprobado" no es un rol verdadero. Los usuarios cuyo estado de registro se ha establecido en "R" (la columna USER.REGISTERTYPE se ha establecido en "R") y cuyo estado es aprobado (la columna MEMBER.STATE se ha establecido en 1) pertenecen de forma implícita al grupo de acceso RegisteredApprovedUsers.
3. "Usuario no rechazado" no es un rol verdadero. Los usuarios cuyo estado de registro es no rechazado (la columna MEMBER.STATE no se ha establecido en 2) pertenecen de forma implícita al grupo de acceso NonRejectedUsers.
4. "Todos los usuarios" no es un rol verdadero. Todos los usuarios del sistema pertenecen implícitamente al grupo de acceso AllUsers.
5. Estos grupos de acciones y grupos de recursos pertenecen a políticas que forman parte de B2CPolicyGroup. Este grupo de políticas se aplica probablemente a las organizaciones que siguen el modelo de negocio B2C.
6. Estos grupos de acciones y grupos de recursos pertenecen a políticas que forman parte de ManagementAndAdministrationPolicyGroup. Este grupo de políticas probablemente se aplica a todas las organizaciones.

Políticas a nivel de recursos por área de negocio

Pedidos

Recursos de datos: pedido:

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

- ResellerAdministratorsForOrgExecuteOrderProcessOnOrderDataResourceGroup
- EmailOrderNotificationManagersForOrgExecuteCustomerServiceEmailOrderOnOrderResource

Recursos de datos: lista de solicitudes:
- AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
- AllUsersExecuteRequisitionListSharedReadCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveReadCommandsOnPrivateRequisitionListResource
- AllUsersExecuteRequisitionListWriteCommandsOnRequisitionListResource
- AllUsersExecuteRequisitionListSharedProcessCommandsOnSharedRequisitionListResource
- AllUsersExecuteRequisitionListExclusiveProcessCommandsOnPrivateRequisitionListResource

Recursos de datos: artículo de interés:
- AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
- AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource

Recursos de datos: RMA:
- AllUsersExecuteRMACreateCommandsOnStoreResource
- AllUsersExecuteRMAReadCommandsOnRMAResource
- AllUsersExecuteRMAPrepareOnRMAResource
- AllUsersExecuteRMAWriteCommandsOnRMAResource
- AllUsersExecuteRMAProcessCommandsOnRMAResource
- RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
- RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
- RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
- RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
- StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource

Beans de datos: pedido:
- AllUsersDisplayOrderDatabeanResourceGroup
- AllUsersDisplayApprovalsOrderDataBeansResourceGroup
- AccountRepresentativesForOrgDisplayOrderDatabeanOnlyResourceGroup

Beans de datos: lista de solicitudes:
AllUsersDisplaySharedRequisitionListDataBeansIfSameOrganizationalEntityAsCreator

Beans de datos: artículo de interés: AllUsersDisplayInterestItemDatabeanResourceGroup

Beans de datos: RMA: AllUsersDisplayRMADatabeanResourceGroup

Intercambio (Contratos)

Recursos de datos: contrato:
- ContractCreatorsForOrgExecuteContractCreateCommandsOnMemberResource
- ContractManagersForOrgExecuteContractManageCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractDeployCommandsOnContractResource
- ContractViewersExecuteContractDisplayCommandsOnContractResource
- ContractOperatorsForOrgExecuteContractSubmitCommandsOnContractResource
- ContractManagersForOrgExecuteContractAccountManageCommandsOnAccountResource

Recursos de datos: política de negocio:

- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyCreateCommandsOnStoreResource
- BusinessPolicyAdministratorsForOrgExecuteBusinessPolicyManageCommandsOnBusinessPolicyResource

Recursos de datos: creación de tiendas:
StoreCreatorsForOrgExecuteStoreCreationCommandsOnOrganizationResource

Beans de datos: AccountHandlersForOrgDisplayTradingDatabeanResourceGroup

Aprobaciones

Recursos de datos:
- AllUsersExecuteApproveCommandsOnApprovalResource
- FlowAdministratorExecutesFlowAdminCreateCommandsOnStoreEntityResource
- FlowAdministratorExecutesFlowadminDeleteCommandsOnFlowadminResource

Beans de datos: FlowAdministratorsForOrgDisplayFlowadminDatabean

Subastas

Recursos de datos:
- AuctionAdministratorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
- AuctionManagersForOrgExecuteAdminRetractBidCommandsOnAuctionResource
- AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteAuctionStyleManageCommandsOnAuctionStyleResource
- AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommandsOnStoreEntityResource
- AuctionAdministratorsForOrgExecuteBidControlRuleManageCommandsOnBidControlRuleResource
- RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteBidManageCommandsOnBidResources
- RegisteredApprovedUsersExecuteAutoBidCreateCommandsOnAuctionResource
- RegisteredApprovedUsersExecuteAutoBidManageCommandsOnAutoBidResources

Beans de datos: AuctionDatabeanOwnersDisplayAuctionDatabeans

Business Intelligence

Recursos de datos:
- BusinessAnalystsForOrgExecuteViewContextListCommandsOnStoreEntityResource
- IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReportCommands OnStoreEntityResource

Miembros

Recursos de datos: usuario:
- MembershipAdministratorsForOrgExecuteUserAdminUpdateCommandsOnUserResource
- GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
- NonRejectedUsersExecuteUserSelfRegistrationContinuationCommandsOnUserResource
- NonRejectedUsersExecuteNonRejectedUserCommands
- AllUsersDisplayUserDatabeanResourceGroup
- NonRejectedDisplayUserDatabeanResourceGroup

Recursos de datos: organización:

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

Recursos de datos: grupo de miembros:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnUserResource
- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberGroupMemberUpdate CommandsOnMemberGroupResource
- MemberGroupAdministratorsForOrgExecuteMemberGroupCreateCommandsOnMemberResource
- MemberGroupManagersForOrgExecuteMemberGroupManageCommandsOnMemberGroupResource

Recursos de datos: dirección:

- NonRejectedUsersExecuteAddressManageCommandsOnUserResource
- MembershipAdministratorsForOrgExecuteAddressManageCommandsOnMemberResource

Recursos de datos: rol:

- MembershipAdministratorsForOrgExecuteRoleUnassignCommandsOnUserResource
- OrganizationRoleAdministratorsExecuteRoleManageCommandsOnOrganizationResource
- MembershipAdministratorsForOrgExecuteUserRoleAssignCommandsOnOrganizationResource

Recursos de datos: atributo de miembros:

- OrgAdminConsoleMembershipAdministratorsForOrgExecuteMemberAttributeCommands OnOrgResource
- AllUsersExecuteMemberAttributeCommandsOnUserResource

Beans de datos:

- MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayOrganizationDatabeanResourceGroup
- MembershipAdministratorsForOrgDisplayUserDatabeanResourceGroup
- EmployeesDisplayOrganizationSpecificDatabeanResourceGroup

Marketing

Recursos de datos: campañas:

- CampaignManagersForOrgExecuteCampaignRelatedCreateCommandsOnStoreEntityResource
- CampaignManagersForOrgExecuteCampaignUpdateCommandsOnCampaignResource
- CampaignManagersForOrgExecuteInitiativeUpdateCommandsOnInitiativeResource

- CampaignManagersForOrgExecuteEMarketingSpotUpdateCommandsOnEMarketingSpotResource
- CampaignManagersForOrgExecuteCollateralUpdateCommandsOnCollateralResource

Recursos de datos: actividades de correo electrónico:
- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnEmailActivity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroup
- EmailActivityEditorsForOrgExecuteEmailActivityDeleteCommandsOnEmailActivity DataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivityConfigurationSaveCommands OnEmailActivityDataResourceGroup
- EmailActivityConfigurationEditorsForOrgExecuteEmailActivitySaveCommandsOnStoreEntity DataResourceGroupAllUsersExecuteEmailOptOutDataResourceGroup

Beans de datos: campañas: CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

Beans de datos: actividades de correo electrónico:
- EmailUserReceiveDataBeanPolicy
- EmailActivityDataBeanPolicy
- EmailConfigurationDataBeanPolicy

Beans de datos: promociones electrónicas: EpromotionDisplayDataBeanPolicy

Catálogo

Recursos de datos:
- CatalogManagersForOrgExecuteStoreCategoryManageCommandsOnCatalogResource
- CatalogManagersForOrgExecuteCatalogManageCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteCatalogGroupManageCommandsOnCatalogGroupResource
- CatalogEntryManagersForOrgExecuteStoreCatalogEntryManageCommandsOnStoreEntityResource
- CatalogGroupManagersForOrgExecuteProductSetAddCommandsOnCatalogResource
- CatalogGroupManagersForOrgExecuteProductSetManageCommandsOnProductSetResource
- CatalogEntryManagersForOrgExecuteCatalogEntryManageCommandsOnCatalogEntryResource
- CatalogEntryManagersForOrgExecuteCatalogEntryRelationManageCommandsOnCatalogResource
- CatalogEntryManagersForOrgExecuteCatalogStoreManageCommandsOnStoreEntityResource

Beans de datos:
- ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup
- CatalogGroupViewersForOrgDisplayCatalogGroupDataBeansResourceGroup
- CatalogListViewersForOrgDisplayCatalogListDataBeansResourceGroup

Conectividad y notificación

Recursos de datos:

- BackendOrderAdministratorsForOrgExecuteBackendOrderStatusCreateCommandsOnOrderDataResource
- BackendPickPackersForOrgExecuteBackendPickPackListCommandsOnFulfillmentCenterDataResource
- MessagingUpdateAdministratorsForOrgExecuteMessagingUpdateCommandsOnStoreEntityResource

Compras

Recursos de datos:

- ProcurementAdministratorsForOrgExecuteProcurementAuthenticationAndRegistration OnOrganizationResource
- ProcurementShoppingCartManagersExecuteProcurementShoppingCartManageOnOrderResource

Cupones

Recursos de datos:

- CouponAdministratorsForOrgExecuteCouponPromotionCreateCommandsOnStoreEntityResource
- CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommandsOnCouponPromotion Resource
- AllUsersExecuteCouponRedemptionCommandsOnCouponWalletResource
- AllUsersExecuteCouponDeleteCommandsOnCouponWalletResource
- CouponAdministratorsForOrgExecuteCouponPromotionUpdateCommandsOnStoreEntityResource
- AllUsersExecuteCouponSaveCommandsOnCouponWalletResource

Beans de datos: CouponAdministratorsForOrgDisplayECouponPromotionBeans

Perfiles de clientes

Recursos de datos:
CustomerProfileEditorsForOrgExecuteSegmentManageCommandsOnStoreEntityResource

Beans de datos: CustomerProfileEditorsForOrgDisplaySegmentationDatabeansResourceGroup

Descuentos

Recursos de datos:

- DiscountAdministratorsForOrgExecuteDiscountCreateCommandsOnStoreEntityResource
- DiscountAdministratorsForOrgExecuteDiscountDeployCommandsOnCalculationCodeResource
- DiscountAdministratorsForOrgExecuteDiscountAssociateCommandsOnCalculationCodeResource

Beans de datos: DiscountViewersForOrgDisplayDiscountDatabeans

Gestión de inventario

Recursos de datos:

- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterCreateCommandsOn OrganizationResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManageCommandsOn FulfillmentCenterResource
- PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommandsOn FulfillmentCenterResource
- VendorInventoryManagersForOrgExecuteVendorManageCommandsOnVendorResource
- VendorInventoryManagersForOrgExecuteVendorCreateCommandsOnStoreEntityResource
- ExpectedInventoryManagersForOrgExecuteInventoryManageCommandsOnStoreEntityResource
- PickPackGeneratorsForOrgExecutePickPackGenerateCommandsOnFulfillmentCenterResource
- InventoryAdjustersForOrgExecuteInventoryAdjustCommandsOnStoreEntityResource
- ReturnReasonsManagersForOrgExecuteReturnReasonsCommandsOnStoreEntityResource
- FulfillmentCenterManagersForOrgExecuteFulfillmentCenterReleaseOnFulfillmentCenter ReleaseDataResourceGroup
- SharedFulfillmentCenterPickBatchInventoryManagersExecuteReleaseReadyShipCommands OnFulfillmentCenterDataResource

- SharedFulfillmentCenterPickPackGeneratorsExecutePickPackGenerateCommands OnFulfillmentCenterResource
- SharedFulfillmentCenterManagersExecuteFulfillmentCenterReleaseCommandsOnFulfillment CenterReleaseDataResourceGroup

Beans de datos:
- ReturnReasonsManagersForOrgDisplayReturnReasonsOrderManagementDataBeansResourceGroup
- ExpectedInventoryManagersForOrgDisplayExpectedInventoryDataBeansResourceGroup
- VendorInventoryManagersForOrgDisplayVendorInventoryDataBeansResourceGroup
- ProductFindInventoryManagersForOrgDisplayProductFindInventoryDataBeansResourceGroup
- FulfillmentCenterManagersForOrgDisplayFulfillmentCenterDataBeansResourceGroup
- PickBatchInventoryManagersForOrgDisplayPickBatchInventoryDataBeansResourceGroup
- ReceiverOrderManagersForOrgDisplayReceiverOrderManagementDataBeansResourceGroup
- ReturnsAdminOrderManagersForOrgDisplayReturnsAdminOrderManagementDataBeans ResourceGroup
- SuperUserOrderManagersForOrgDisplaySuperUserOrderManagementDataBeans ResourceGroupFulfillmentManagersForOrgDisplayReleaseOrderItemsDatabeanResourceGroup

Gestión de pedidos

Recursos de datos:
- CustomerOrderManagersForOrgExecuteCustomerServiceOrderWriteCommands OnOrderResource
- CustomerOrderManagersForOrgExecuteCustomerServiceOrderCreateCommands OnStoreEntityResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnWriteCommands OnRMAResource
- CustomerOrderManagersForOrgExecuteCustomerServiceReturnCreateCommands OnStoreEntityResource
- CustomerOrderManagersExecuteCustomerWriteCommandsOnUserResource
- CustomerOrderManagersForDefaultOrgExecuteCustomerServiceCustomerWriteCommandsOn UserDataResourceGroupwithGuestRegisterType

Beans de datos:
- CustomerOrderManagersForOrgDisplayCustomerOrderManagementDatabeans
- MemberOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- MemberOrderManagersDisplayOrganizationSpecificDatabeans
- MemberOrderManagersDisplayUserDatabeanResourceGroup
- UserOrderManagersForDefaultOrgDisplayGuestMemberDatabeans
- UserOrderManagersDisplayOrganizationSpecificDatabeans
- UserOrderManagersDisplayUserDatabeanResourceGroup
- LogisticsManagersForOrgDisplayOrdersAndReturnsListsDatabeans
- ReturnsManagersForOrgDisplayReturnsListsDatabeans

Pagos

Recursos de datos:
- AccountManagersForOrgExecuteAccountCreateCommandsOnOrganizationResource
- AccountAdministratorsForOrgExecuteAccountManageCommandsOnAccountResource
- AccountViewersForOrgExecutePaymentSummaryGenerateCommandsOnAccountResource
- AccountViewersForOrgExecuteStorePaymentAdminCommandsOnStoreEntityResource

- AllUsersExecutePaymentOrderWriteCommandsOnOrderResource

Editor de políticas

Recursos de datos:
- StoreAdministratorsForOrgExecuteACPolicyCreateCommandsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACPolicyEditCommandsOnACPolicyResource
- StoreAdministratorsForOrgExecuteACViewPoliciesForUpdateActionsOnOrganizationResource
- StoreAdministratorsForOrgExecuteACViewApplicablePoliciesActionsOnOrganizationResource
- DescendantStoreAdministratorsExecuteACViewPoliciesForOrgActionsOnOrganizationResource

Beans de datos: StoreAdministratorsForOrgExecuteUserGroupSearchViews

Asesor de productos

Beans de datos:
- ProductAdvisorStatisticiansForOrgDisplayProductAdvisorStatisticsDatabeans
- SalesAssistantStatisticiansForOrgDisplaySalesAssistantStatisticsDatabeans
- ProductAdvisorManagersDisplayPAWCBEDatabeanResourceGroup
- GuidedSellManagersDisplayGSWCBEDatabeanResourceGroup

RFQ

Recursos de datos:
- RFQBuyersExecuteRFQCreateCommandsOnStoreEntityDataResourceGroup
- RFQBuyersManageRFQResourcesTheyOwn
- RFQBuyersManageRFQResponsesForRFQsTheyOwn
- RFQAdministratorsAdministerRFQs
- RFQAdministratorsManageRFQResponses
- RFQSalesManagersForOrgCreateRFQResponse
- RFQSalesManagersExecuteRFQResponseManageCommandsOnRFQResponseResource
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQWithPublicAccess TypeResourceGroup
- RFQSalesManagersExecuteRFQResponseAdminCommandsOnRFQResourceGroup

Beans de datos:
- RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
- RFQBuyersDisplayRFQResponseDataBeansViewabletoRFQOwnerResourceGroup
- RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup
- RFQSalesViewersDisplayRFQDataBeanWithPublicAccessTypeResourceGroup
- RFQSalesViewersDisplayRFQDataBeanResourceGroup

Normas

Recursos de datos:
StoreAdministratorsForOrgExecutePersonalizationRuleServiceAdministrationCommands OnStoreEntityResource

Beans de datos:
StoreAdministratorsForOrgDisplayPersonalizationRuleServiceAdministrationDataBeanResourceGroup

Planificador

Recursos de datos:

- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnStoreEntityResource
- StoreAdministratorsForOrgExecuteScheduledJobManageCommandsOnUserResource

Beans de datos: StoreAdministratorsForOrgDisplaySchedulerDataBeansResourceGroup

Commerce Accelerator

Recursos de datos:

- B2CCSAViewUsersForOrgExecuteB2CCSAViewActionsOnStoreEntityResource
- B2BCSAViewUsersForOrgExecuteB2BCSAViewActionsOnStoreEntityResource
- CHSCSAViewUsersForOrgExecuteCHSCSAViewActionsOnStoreEntityResource
- RHSCSAViewUsersForOrgExecuteRHSCSAViewActionsOnStoreEntityResource
- CPSCSAViewUsersForOrgExecuteCPSCSAViewActionsOnStoreEntityResource
- RPSCSAViewUsersForOrgExecuteRPSCSAViewActionsOnStoreEntityResource
- HCPCSAViewUsersForOrgExecuteHCPCSAViewActionsOnStoreEntityResource
- MHSCSAViewUsersForOrgExecuteMHSCSAViewActionsOnStoreEntityResource
- MPSCSAViewUsersForOrgExecuteMPSCSAViewActionsOnStoreEntityResource
- SCPCSAViewUsersForOrgExecuteSCPCSAViewActionsOnStoreEntityResource
- SHSCSAViewUsersForOrgExecuteSHSCSAViewActionsOnStoreEntityResource
- SPSCSAViewUsersForOrgExecuteSPSCSAViewActionsOnStoreEntityResource

Envío

Recursos de datos:
ShippingMembershipAdministratorsForOrgExecuteShippingManageCommandsOnStore
DataResourceGroup

Beans de datos: ShippingMembershipAdministratorsForOrgDisplayShippingDatabeanResourceGroup

Impuestos

Recursos de datos:
TaxationAdministratorsForOrgExecuteTaxationManageCommandsOnStoreDataResourceGroup

Beans de datos: TaxationAdministratorsForOrgDisplayTaxationDatabeanResourceGroup

Ayuda en directo/Espacios de trabajo colaborativos/Atención al cliente

Recursos de datos: Ayuda en directo:

- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnUserDataResources
- LiveHelpAgentsForOrgExecuteLiveHelpRetrieveCommandsOnOrderDataResources

Recursos de datos: Atención al cliente:
CustomerCareAdministratorsForOrgExecuteCustomerCareQueueManageCommandsOnStoreResource

Beans de datos: Ayuda en directo:
LiveHelpAgentsForOrgDisplayCustomerCareDatabeanResourceGroup

Beans de datos: Espacios de trabajo colaborativos:
CollaborativeWorkspaceAdministratorsForOrgDisplayCollaborativeWorkspaceDatabeanResourceGroup

Estado de la tienda

Recursos de datos:

- ChannelManagersExecuteStoreStateChangeCommandsOnStoreResource
- AdministrativeRolesForOrgExecuteStoreStateChangeCommandsOnStoreResource
- AdministratorsForOrgAccessStoreWithCloseOrSuspendStateResourceGroup
- AllUsersAccessStoreWithOpenStateResourceGroup

Gestión de tiendas

Recursos de datos: entrega de informes:
ReportDeliveryManagersForOrgExecuteSetupReportDeliveryCommandsOnStoreDataResourceGroup

Recurso de datos: tienda:

- StoreFrontManagersForOrgExecuteStoreFrontRelatedUpdateOnStoreEntityResource
- StoreProfileManagersForOrgExecuteStoreProfileRelatedUpdateOnStoreEntityResource

Grupos de políticas de control de acceso por omisión

Los grupos de políticas de control de acceso por omisión que se envían con WebSphere Commerce son los siguientes:

- `ManagementAndAdministrationPolicyGroup`: Este grupo de políticas contiene todas las políticas de gestión de miembros y administración de tiendas.
- `GuestShopperManagementPolicyGroup`: Este grupo de políticas contiene todas las políticas relacionados con la gestión de compradores invitados.
- `CommonShoppingPolicyGroup`: Este grupo de políticas contiene todas las políticas relacionadas con compras que son comunes para los escenarios Directo al consumidor y Directo a B2B.
- `B2CPolicyGroup`: Este grupo de políticas contiene todas las políticas de compras específicas de Directo al consumidor.
- `B2BPolicyGroup`: Este grupo de políticas contiene todas las políticas de compras de Directo a B2B.

Nota: El grupo de políticas `ManagementAndAdministrationPolicyGroup` es el grupo de políticas principal que debe aplicarse generalmente a todas las organizaciones. Cuando una organización se suscribe a algún grupo de políticas, también debe suscribir a este grupo de políticas. Para una organización propietaria de una tienda, dependiendo del tipo de tienda, además de al grupo `ManagementAndAdministrationPolicyGroup`, debe suscribirse a `CommonShoppingPolicyGroup`, `B2CPolicyGroup` y `B2BPolicyGroup`. Al grupo de políticas `GuestShopperManagementPolicyGroup` solamente debe suscribirse la organización propietaria de los compradores invitados que es la organización por omisión en un escenario común.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE.UU.

Es posible que IBM no ofrezca en otros países los productos, servicios o características descritos en esta publicación. Póngase en contacto con su representante de IBM local para obtener información acerca de los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo pueda utilizarse ese producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

Cualquier referencia realizada en esta publicación a un programa bajo licencia cIBM no pretende afirmar ni implicar que sólo pueda utilizarse dicho programa bajo licencia de IBM. En lugar del producto, programa o servicio de IBM se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derecho de propiedad intelectual de IBM. Queda bajo la responsabilidad del usuario, la evaluación y verificación del funcionamiento junto con otros productos, excepto los designados expresamente por IBM.

IBM puede tener patentes o aplicaciones pendientes de patente que cubran temas tratados en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing

IBM Corporation
North Castle Drive
Armonk, NY 10504–1785
EE.UU.

Para realizar consultas relacionadas con la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe sus consultas, por escrito, a:

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

El párrafo siguiente no es aplicable al Reino Unido ni a cualquier otro país en el que tales disposiciones contradigan la normativa local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no

contemplan la exclusión de garantías, ni implícitas ni explícitas, en determinadas transacciones, por lo que puede haber usuarios a los que no les afecte esta declaración.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información aquí contenida está sometida a cambios periódicos; dichos cambios se incorporarán en nuevas ediciones de la publicación. IBM se reserva el derecho de realizar cambios y/o mejoras, cuando lo considere oportuno y sin previo aviso, en los productos y/o programas descritos en esta publicación.

Todas las referencias hechas en este documento a sitios Web que no son de IBM se proporcionan únicamente para su información y no representan en modo alguno una recomendación de dichos sitios Web. El contenido de estos sitios Web no forma parte del contenido de este producto de IBM, por lo que la utilización de dichos sitios es responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le envíe del modo que estime conveniente sin incurrir por ello en ninguna obligación para con el remitente.

Los propietarios de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, deberán ponerse en contacto con:

IBM Canada Ltd.
Office of the Lab Director
8200 Warden Avenue
Markham, Ontario
L6G 1C7
Canadá

Dicha información puede estar disponible sujeta a los términos y condiciones apropiados, incluyendo, en algunos casos, el pago de una cantidad.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo según los términos del Contrato de cliente de IBM, el Acuerdo internacional de programas bajo licencia de IBM o cualquier acuerdo equivalente entre las partes.

Cualquier dato de rendimiento que contenga esta publicación se ha determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar de modo significativo. Algunas medidas pueden haberse realizado en sistemas a nivel de desarrollo y no existe garantía de ningún tipo de que estas medidas serán las mismas en los sistemas disponibles generalmente. Asimismo, es posible que algunas medidas se hayan calculado mediante extrapolación. Los resultados reales pueden ser diferentes. Los usuarios de esta publicación deben comprobar los datos aplicables de su entorno específico.

La información sobre productos que no son de IBM se ha obtenido de los distribuidores de dichos productos, de los anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con productos que no son de IBM. Las preguntas sobre las prestaciones de productos no de IBM deben dirigirse a los distribuidores de dichos productos.

Todas las declaraciones sobre futuras tendencias o intenciones de IBM están sujetas a modificación o retirada sin previo aviso y representan únicamente metas y objetivos.

Esta información contiene ejemplos de datos e informes que se utilizan en operaciones comerciales cotidianas. Para ilustrar los ejemplos de la forma más completa posible, éstos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizados en empresas reales es pura coincidencia.

Las imágenes de tarjetas de crédito, marcas registradas y nombres comerciales que se proporcionan con este producto solamente deberán utilizarlos los comerciantes que tienen autorización de los propietarios de la marca de la tarjeta de crédito para aceptar pagos mediante este tipo de tarjeta de crédito.

Licencia de copyright

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente que ilustran las técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir libremente estos programas de ejemplo, sin pagar por ello a IBM, con la finalidad de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a la interfaz de programas de aplicación para la plataforma operativa para la cual están escritos los programas de ejemplo. Estos ejemplos no han sido probados en profundidad bajo todas las condiciones. En consecuencia, IBM no puede garantizar ni afirmar la fiabilidad, solidez o funcionalidad de estos programas. Puede copiar, modificar y distribuir libremente estos programas de ejemplo, sin pagar por ello a IBM con la finalidad de desarrollar, utilizar, comercializar o distribuir programas de aplicación conformes a las interfaces de programas de aplicación de IBM.

Marcas registradas

El logotipo de IBM y los siguientes términos son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países:

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

Domino es una marca registrada de Lotus Development Corporation en los Estados Unidos y/o en otros países.

Microsoft y Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Java, JavaBeans y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de otras empresas.