IBM® WebSphere Commerce®

Guía de control de acceso

Versión 54

IBM® WebSphere Commerce®

Guía de control de acceso

Versión 54

Nota:
Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información del apartado Avisos.

Primera edición (marzo 2002), segunda revisión (abril 2002)

Esta edición se aplica a los productos siguientes:

IBM WebSphere Commerce Business Edition para Windows NT y Windows 2000, Versión 5.4

IBM WebSphere Commerce Business Edition para AIX, Versión 5.4

IBM WebSphere Commerce Business Edition para el software Solaris Operating Environment, Versión 5.4

IBM WebSphere Commerce Studio, Business Developer Edition para Windows NT y Windows 2000, Versión 5.4

IBM WebSphere Commerce Professional Edition para Windows NT y Windows 2000, Versión 5.4

IBM WebSphere Commerce Professional Edition para AIX, Versión 5.4

IBM WebSphere Commerce Professional Edition para el software Solaris Operating Environment, Versión 5.4

IBM WebSphere Commerce Studio, Professional Developer Edition para Windows NT y Windows 2000, Versión 5.4

y a todos los releases y modificaciones posteriores de estos productos, a menos 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. Las publicaciones no se encuentran en la dirección indicada más abajo.

IBM agradece sus comentarios. Envíe sus comentarios mediante alguno de estos métodos:

1. Por correo electrónico a la dirección que se especifica a continuación. Asegúrese de incluir su dirección de correo electrónico completa si desea una respuesta.

   `Internet: hojacom@vnet.ibm.com`

2. Por correo postal a la siguiente dirección:

   IBM, SA
   NLSC
   Av. Diagonal 571, Edif. L'Illa
   08029 Barcelona, España

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.

Dónde encontrar información

WebSphere Commerce™ proporciona información en línea e impresa que describe la solución de comercio electrónico completa. Además, los productos de software que están empaquetados con WebSphere Commerce proporcionan información adicional, que describe las características y funciones específicas del software. Este apartado ofrece una breve visión general de la ubicación de los distintos tipos de información.

Publicaciones de WebSphere Commerce

- *IBM™ WebSphere Commerce, Conceptos básicos, Versión 5.4*
- *IBM™ WebSphere Commerce, Guía del programador, Versión 5.4*
- *IBM™ WebSphere Commerce para Windows NT™ y Windows™ 2000, Guía de iniciación rápida, Versión 5.4*
- *IBM™ WebSphere Commerce Studio Business Developer Edition para Windows NT™ y Windows™ 2000, Guía de instalación, Versión 5.4*
- *IBM™ WebSphere Commerce, Guía de migración, Versión 5.4*

Para obtener actualizaciones de estas publicaciones, consulte la dirección Web siguiente: `http://www.ibm.com/software/webservers/commerce/wc_be/lit-tech-general.html`

Ayuda en línea de WebSphere Commerce

La ayuda en línea de WebSphere Commerce consta de información en línea que puede verse utilizando un navegador Web, así como de extractos de la información en línea compilados en documentos PDF (Portable Document Format) de temas relacionados.

Se puede acceder a la ayuda en línea desde un navegador Web que se ejecute en Internet Explorer, Versión 5.5 o superior utilizando la dirección siguiente:

`http://`*`nombre_sistpral`*`/wchelp/`, donde *`nombre_sistpral`* es el nombre de la máquina de WebSphere Commerce.

Además en Windows, se puede acceder a la ayuda desde el menú **Inicio**, de la siguiente forma:

Inicio– > Programas – > IBM® WebSphere Commerce– > Documentación

Información adicional en la Web

Soporte

Para encontrar información de soporte, incluidos grupos de noticias, preguntas más frecuentes, notas técnicas, información de resolución de problemas y descargas, consulte la siguiente dirección Web:

Business

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

Professional

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

Empresas de software asociadas

Existen muchas empresas de software asociadas que ofrecen productos y servicios para mejorar WebSphere Commerce. Para obtener información sobre estas empresas, visite el siguiente sitio Web: http://www.ibm.com/software/webservers/commerce/community y pulse el enlace Software Developers.

Redbooks™

Para obtener información técnica más avanzada, visite el sitio Web de Redbooks que se encuentra en http://www.ibm.com/redbooks y busque WebSphere Commerce.

Antes de empezar

La publicación *IBM WebSphere Commerce Versión 5.4, Guía de control de acceso* está dirigida a los administradores de sitios que desean gestionar el acceso a su sitio de WebSphere Commerce. Los administradores de tiendas pueden realizar una gestión de acceso limitada para la entidad de organización para la que desempeñan su rol.

Esta guía proporciona una introducción para la gestión de acceso, incluida una visión general de las organizaciones y usuarios, las políticas de control de acceso, su jerarquía y sus relaciones y las políticas por omisión que se empaquetan con el producto. Esta guía proporciona también una amplia gama de escenarios que ayudan a los administradores de sitios que desean realizar personalizaciones básicas en sus políticas existentes y también directrices para comprobar las políticas modificadas y para tratar los temas relacionados con el rendimiento.

Este manual está dividido en las secciones siguientes:

Capítulo 1: Visión general. Una breve visión general de las funciones clave del sistema de control de acceso de WebSphere Commerce y también una descripción de lo que se ha modificado desde el último release de WebSphere Commerce.

Capítulo 2: Iniciación. Una introducción a la gestión de acceso, incluido cómo definir organizaciones y usuarios, cómo se relacionan las organizaciones y los usuarios con las políticas de control de acceso, la estructura básica de una política de control de acceso y cómo leer e identificar los componentes clave de una política en la Consola de administración de WebSphere Commerce y en formato XML.

Capítulo 3: Conceptos de control de acceso Información sobre los conceptos de la estructura de una organización y sus suborganizaciones, el modo en que se otorga acceso a los usuarios a un sistema, descripciones de los roles por omisión y de la terminología relacionada.

Capítulo 4: Personalización de las políticas de control de acceso. Una descripción detallada de las políticas basadas en roles y a nivel de recursos junto con su relaciones y jerarquía.

Capítulo5: Escenarios de control de acceso Diferentes escenarios que le muestran cómo puede realizar modificaciones básicas en las políticas de acceso por omisión que se envían con WebSphere Commerce.

Capítulo 6: Utilización de archivos XML para personalizar las políticas de control de acceso Una descripción de la personalización de los componentes de control de acceso utilizando XML. Incluye procedimientos detallados para cargar información de políticas de los archivos XML a las tablas de base de datos de control de acceso y para extraer la información de las tablas de base de datos de control de acceso y pasarla a archivos XML.

Apéndice: Tabla de políticas de control de acceso por omisión Una lista completa de todas las políticas de control de acceso por omisión que se cargan en el sistema durante la instalación.

Requisitos previos

Esta guía presupone que ha instalado y configurado correctamente IBM WebSphere Commerce, Versión 5.4 en el sitio y que tiene acceso de administrador de sitio para la herramienta Consola de administración de WebSphere Commerce. Los administradores de tienda pueden gestionar las políticas de control de acceso de su entidad de organización con la herramienta Consola de administración de WebSphere Commerce pero no pueden gestionar los componentes de las políticas como, por ejemplo, los grupos de acciones y los grupos de recursos, ya que son entidades de todo el sistema.

Esta guía también presupone que su sistema reúne todos los requisitos previos de software y hardware para ejecutar WebSphere Commerce. Para obtener más información sobre cómo instalar WebSphere Commerce, incluidos los requisitos previos, consulte la publicación *IBM WebSphere Commerce, Versión 5.4, Guía de instalación*.

Convenios utilizados en este libro

Este manual utiliza los convenios siguientes:

La **negrita** indica controles de interfaz gráfica de usuario (GUI), por ejemplo, nombres de campos, botones o elecciones de menú.

El `monoespaciado` indica ejemplos de texto que deben escribirse exactamente tal como se muestran, así como vías de acceso a directorios.

La *cursiva* se utiliza para enfatizar palabras y para indicar variables que el usuario debe sustituir por sus propios valores.

 Indica información adicional que puede ayudarle a completar una tarea.

NT indica información específica de WebSphere Commerce para Windows NT ®.

2000 indica información específica de WebSphere Commerce para Windows ® 2000.

AIX indica información específica de WebSphere Commerce para AIX ®.

Solaris indica información específica de WebSphere Commerce para el software Solaris Operating Environment.

Linux indica información específica de WebSphere Commerce para Linux.

400 indica información específica de WebSphere Commerce para IBM Eserver iSeries™ 400 ® (llamado anteriormente AS/400 ®)

Professional indica información específica de WebSphere Commerce Professional Edition.

Business indica información específica de WebSphere Commerce Business Edition.

Contenido

Capítulo 1. 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 abrir el paso a 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 e-commerce.

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 e-commerce, en el que la entrada a su negocio resulta ampliamente afectada por las relaciones que se inician a través de la Web.

Novedades de WebSphere Commerce Versión 5.4

Para obtener una lista de las características nuevas y de las mejoras añadidas a WebSphere Commerce, consulte la publicación *IBM WebSphere Commerce Versión 5.4, Novedades*.

Interfaz de usuario mejorada

Además de las páginas de edición de políticas a las que puede accederse desde el menú Gestión de acceso de la Consola de administración, WebSphere Commerce proporciona ahora páginas adicionales para ver políticas y sus grupos de acciones, grupos de acceso y grupos de recursos relacionados. Las páginas de visualización de políticas se han integrado de forma transparente con la interfaz de usuario de la Consola de administración y se puede acceder a las mismas mediante los botones que se han añadido a las páginas de edición de políticas existentes.

Control exhaustivo

El release anterior de WebSphere Commerce Suite proporciona un control de acceso menos exhaustivo, que le permitía definir quién podía invocar determinadas funciones en el sistema. Por ejemplo, en el release anterior de WebSphere Commerce Suite, es posible que utilizara el control de acceso menos exhaustivo para permitir que los compradores cancelasen pedidos invocando la función `Cancelar pedido`.

Ahora en WebSphere Commerce, también puede utilizar el control de acceso exhaustivo que le permite definir quién puede invocar determinadas funciones en las instancias de objetos de negocio (a los que también se hace referencia como `recursos`). Utilizando el mismo ejemplo, ahora no sólo puede permitir que los compradores cancelen pedidos sino que puede limitar esta función, de modo que los compradores invoquen la función de cancelar pedido en sus propios pedidos y no en los pedidos de otros usuarios.

La mayor potencia del control de acceso exhaustivo junto con el control de acceso menos exhaustivo anterior le ofrece un mayor margen de gestión de acceso y le permite ajustar las actividades que pueden realizar los usuarios en su sitio.

Componente administrado por separado

En el release anterior de WebSphere Commerce Suite, el control de acceso exhaustivo estaba incorporado en el código del sistema, por lo que era necesario modificar el código para instaurar la personalización de políticas en el nivel de recursos.

Ahora, WebSphere Commerce exterioriza tanto el control de acceso exhaustivo como el menos exhaustivo codificando las políticas de control de acceso en archivos XML que se pueden modificar mediante la interfaz del visor de políticas que se incluye con las herramientas de la Consola de administración o mediante un editor de texto estándar.

Dado que tanto las políticas de control de acceso exhaustivas como las menos exhaustivas están ahora separadas del código del producto, para adaptar la gestión de acceso a las necesidades de su negocio es necesario realizar cambios en la información que contienen los archivos XML y no en el código del producto.

Adaptable a los nuevos procesos de negocio

Debido a la constante evolución del mercado actual, la posibilidad de personalizar rápidamente su entorno de negocio juega un papel importante a la hora de mantener su competitividad, de ajustarse a los cambios del mercado y de adaptarse a los nuevos procesos de negocio. Al exteriorizar las políticas de control de acceso exhaustivas y las menos exhaustivas, cuando deba realizar algún cambio en los niveles de acceso a su sistema podrá hacerlo fácil y rápidamente modificando simplemente las políticas y sin tener que personalizar el código. Y lo que es más importante, al revelar las políticas de control de acceso exhaustivas que anteriormente sólo estaban disponibles a un equipo de servicios bajo contrato, su organización puede ahora modificar las políticas por su cuenta y disminuir el coste adicional que supone personalizar WebSphere Commerce para su sitio Web.

Escalabilidad

A medida que su organización cambia y aumenta de tamaño con el tiempo, el acceso a su sistema debe acomodar también estos cambios. A medida que aumenta el número de empleados, su papel y sus responsabilidades, deben modificarse sus

niveles de acceso adecuadamente para permitirles que efectúen las actividades que deben realizar. Sin embargo, la tarea de realizar un seguimiento de las actividades de cada usuario individual puede resultar difícil, requerir mucho tiempo o no ser de ningún modo práctica.

Sin embargo, con WebSphere Commerce puede gestionar el acceso al sistema de forma implícita, utilizando los grupos de acceso cuyos miembros se definen según un conjunto de *atributos* compartidos y no según sus identidades. A los usuarios se les asignan roles y se les otorga acceso según estos roles. Por ejemplo, a los usuarios A, B y C se les puede asignar un rol de `Comprador` y a todos los compradores se le puede permitir que cancelen los pedidos que no se han enviado, utilizando la política de control de acceso adecuada. Si el usuario A deja la organización, se puede suprimir la información del rol del usuario A, mientras que la política de control de acceso por la que se asocian los roles de usuario con la posibilidad de cancelar pedidos permanece sin modificaciones para los usuarios B y C.

La posibilidad de otorgar a los usuarios acceso al sistema de forma implícita es un método muy útil para gestionar las actividades y requiere muchos menos tiempo y esfuerzo. Además, el esfuerzo que requiere gestionar el control de acceso se convierte en un factor del número de políticas que desea modificar, no del tamaño del sistema, ni del número de usuarios que pertenecen a su organización ni del nivel de las actividades de negocio que lleve a cabo. Las políticas de control de acceso que se ejecuten en el sistema se pueden aplicar tanto a las organizaciones pequeñas como a las de gran tamaño. Como resultado, la posibilidad de escalado de las políticas de control de acceso que se ejecutan en WebSphere Commerce permiten que su empresa continúe creciendo y modificándose sin afectar la estructura ni la eficacia de sus operaciones.

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 para 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 cómo se pueden crear organizaciones y usuarios y una política de control de acceso.

Capítulo 2. Iniciación

En el capítulo anterior se ha descrito el importante rol que juega el control de acceso en e-commerce 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 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 sitios, una de las primeras tareas después de instalar y configurar WebSphere Commerce es definir y gestionar el acceso al sitio de e-commerce. Esto requiere crear organizaciones que participarán en el sitio y también definir a los usuarios que serán miembros de dichas organizaciones.

En algunos casos, las organizaciones que se registrarán en su sitio pueden ser organizaciones de compradores o es posible que en su sitio se registren clientes que tengan con su negocio una relación de tipo empresa a cliente. Independientemente de si está administrando un sitio de empresa a empresa o de empresa a cliente, 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 ya ha configurado sus organizaciones y usuarios, puede ignorar este apartado y pasar al apartado siguiente relacionado con el control de acceso. De lo contrario, utilice este apartado como una guía de planificación.

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:

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

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

También le recomendamos que consulte la publicación *IBM WebSphere Commerce, Conceptos básicos, Versión 5.4*.

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 mujeres 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, administrador de tienda, desarrollador del sitio, vendedor, etc. Consulte el apartado “Roles” en la página 11 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.

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.

Nota: En WebSphere Commerce Professional Edition, solamente puede haber una organización vendedora.

Definición de una organización compradora

Si va a ejecutar un sitio de empresa a empresa, más de una organización compradora puede pertenecer al sitio. Por el contrario, si va a ejecutar un sitio de empresa a cliente, se registrarán compradores invididuales 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.

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

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

Información sobre el control de acceso

Cuando haya terminado de definir las organizaciones y los usuarios que participarán en su sitio de e-commerce, 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 actividades determinadas en el sitio. Estas actividades abarcan desde registrarse a gestionar subastas, actualizar el catálogo de productos y aprobar pedidos, y también cualquier actividad del centenar de actividades necesarias para operar y mantener un sitio de e-commerce.

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.

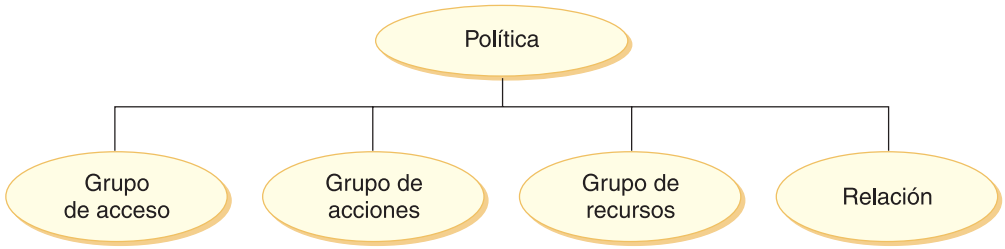
Un *grupo de acceso* es un grupo de usuarios que comparten un acceso común a un conjunto de funciones del sitio. Un grupo de acceso incluye generalmente a los usuarios que comparten atributos comunes como, por ejemplo, el mismo rol, el mismo departamento o el mismo tipo de especialización.

Un *grupo de acciones* es el grupo 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 1. 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 de control de acceso” en la página 9.

¿Cómo puede comenzar a utilizar el control de acceso?

En algunos casos, no es necesario que haga nada. Esto es debido a que las políticas por omisión de WebSphere Commerce se han diseñado para proporcionar una estructura base de control de acceso basada en usuarios típicos del sistema y las actividades que realizan que están asociadas con sus roles dentro de una organización. Las políticas cubren una amplia gama de actividades comunes de negocio, incluidos los 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 33.

Capítulo 3. Conceptos de control de acceso

En WebSphere Commerce el control de acceso es el proceso para verificar que 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 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 e-commerce. Para comprender el componente de control de acceso de WebSphere Commerce, en primer lugar debe comprender la jerarquía organizativa típica de un sitio de e-commerce.

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 compradores o vendedores de las organizaciones 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 organizativa de un sitio de e-commerce de empresa a empresa.

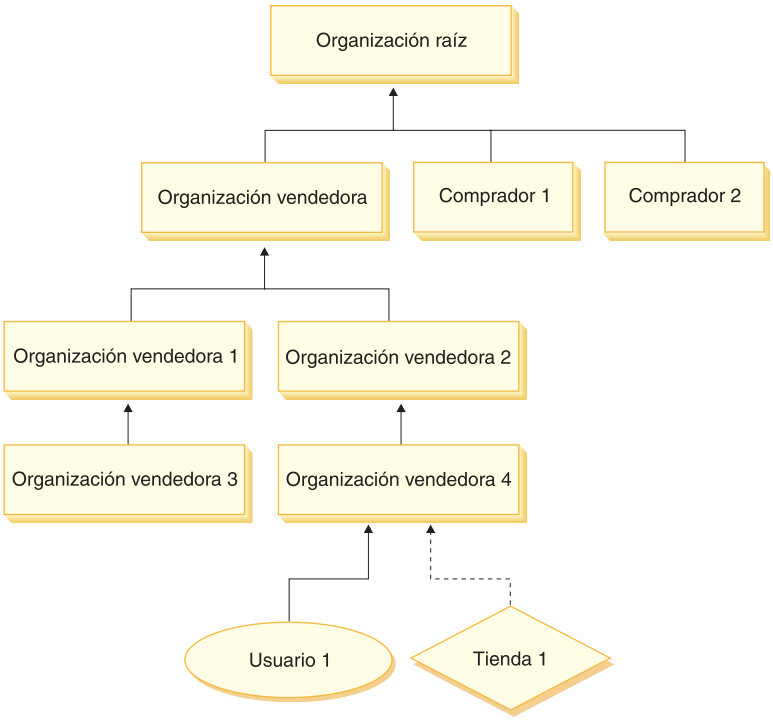


Figura 2. Jerarquía organizativa de un sitio de empresa a empresa

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 la autorización (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 empresa a cliente, no hay organizaciones compradoras. Los clientes de un sitio de empresa a cliente 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 cliente, 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 de una organización vendedora y asigna al Administrador de vendedores la gestión de dicha organización. El Administrador de vendedores 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 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 el apartado “Administrador de sitio” en la página 12.

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. Del mismo modo, un usuario 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 para la organización X, a la organización padre de este usuario también se le debe asignar el rol de jefe de producto. A continuación, se pueden definir las políticas de control de acceso de modo que solamente este usuario pueda realizar las operaciones 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:

- Operaciones de sitio
- Desarrollo de sitio y contenido
- Gestión de marketing
- Gestión de productos
- Gestión de ventas
- Gestión de logística y operaciones
- Gestión de la organización

Operaciones de sitio

WebSphere Commerce da soporte a los siguiente roles para operaciones técnicas:

- Administrador de sitio
- Administrador de tienda

Administrador de sitio

El Administrador de sitio, instala, configura y hace el mantenimiento de WebSphere Commerce, así como el software y hardware asociados. El Administrador responde a los avisos, las alertas y los errores del sistema, y diagnostica y resuelve los problemas del sistema. Normalmente este rol controla el acceso y la autorización (creando y asignando miembros al rol apropiado), gestiona el sitio Web, supervisa el rendimiento y gestiona las tareas de equilibrio de la carga. El Administrador de sitio también puede ser responsable de establecer y mantener varias configuraciones de servidor para diferentes etapas del desarrollo como, por ejemplo, prueba, transición y producción. Este rol también se encarga de las copias de seguridad imprescindibles del sistema y resuelve los problemas de rendimiento.

Administrador de tienda

El Administrador de tienda gestiona los elementos de la tienda y actualiza y publica los cambios en los impuestos, el envío y la información sobre la tienda. El Administrador de tienda también puede gestionar las políticas de control de acceso de la organización. El Administrador de tienda, que suele ser el líder del equipo de desarrollo de la tienda, es el único rol del equipo que tiene la autorización para publicar un archivador de tienda (el Administrador de sitio también puede publicarlo). El Administrador de tienda suele tener conocimientos de Web y conoce a fondo los procedimientos de negocio de la tienda.

Desarrollo de sitio y contenido

WebSphere Commerce da soporte al rol de Desarrollador de tiendas para el desarrollo de sitio y contenido:

Desarrollador de tiendas

Los desarrolladores de tienda crean archivos Java Server Pages y el código personalizado necesario y pueden modificar cualquiera de las funciones estándar que se incluyen con WebSphere Commerce. Una vez creado el archivador de tienda, los desarrolladores de tienda tienen la autorización para efectuar cambios en el mismo, manualmente o mediante los cuadernos Perfil de tienda, Impuestos y Envío. Pero no tienen autorización para publicar el archivador de tienda en WebSphere Commerce Server.

Logística y operaciones

WebSphere Commerce soporta los siguientes roles de gestión de logística y operaciones:

- Director de logística
- Director de operaciones
- Receptor
- Administrador de devoluciones
- Empaquetador

Director de logística

Business El Director de logística, que a veces se denomina Director de envíos, gestiona y negocia el flete o envío de carga desde las empresas de transporte hasta el almacén y a los clientes individuales. Este rol es el responsable de asegurar que la compañía utilice los mejores transportistas al mejor coste para cumplir con la estrategia. El envío es un aspecto importante del servicio al cliente y puede ser un factor clave de éxito para el negocio en línea.

Director de operaciones

B2C Este rol gestiona el proceso de pedidos, asegurando que los pedidos se despachen correctamente, que se reciba el pago y que se envíen los pedidos. El Director de operaciones puede buscar pedidos de clientes, ver detalles y gestionar la información de los pedidos, así como crear y editar devoluciones.

Empaquetador

El Empaquetador elige productos en los centros de despacho de pedidos y los empaqueta para enviarlos a los clientes. El empaquetador también gestiona los comprobantes de requisición de artículos y las listas de embalaje que se utilizan para confirmar el envío de los productos durante el despacho de los pedidos.

Receptor

El Receptor recibe el inventario en el centro de despacho de pedidos, hace un seguimiento de los registros de inventario esperado y de las recepciones ad hoc para productos pedidos y recibe los productos devueltos como resultado de las devoluciones de clientes.

Administrador de devoluciones

El Administrador de devoluciones gestiona la disposición de los productos devueltos.

- Lista las devoluciones
- Lista los productos devueltos
- Dispone de los productos devueltos

Gestión de productos

WebSphere Commerce soporta los siguientes roles de gestión de productos:

- Comprador (parte vendedora)
- Gestor de categorías
- Jefe de producto o Director de comercialización

Comprador (parte vendedora)

El comprador compra mercancía que está a la venta. El comprador maneja las relaciones con los proveedores o suministradores y negocia para obtener el producto deseado con términos favorables para cuestiones tales como la entrega y las opciones de pago. El comprador puede establecer precios. El comprador gestiona el inventario a fin de determinar las cantidades que se deben comprar y asegurarse de que las existencias se reponen correctamente.

Gestor de categorías

El gestor de categorías gestiona la jerarquía de categorías creando, modificando y suprimiendo categorías. La jerarquía de categorías organiza los productos o servicios que ofrece la tienda. El gestor de categorías también gestiona los productos, los registros de inventario esperado, la información de proveedores, el inventario y las razones de devolución.

Jefe de producto/Director de comercialización

El Business Jefe de producto o B2C Director de comercialización hace el seguimiento de las compras de clientes, sugiere descuentos y determina el mejor modo de visualizar, tasar y vender productos en la tienda en línea.

- Realiza todas las tareas del gestor de categorías
- Realiza todas las tareas del director de marketing

Gestión de ventas

WebSphere Commerce soporta los siguientes roles de gestión de relaciones comerciales:

- Director de ventas
- Representante de cuentas
- Supervisor de servicio al cliente
- Representante de servicio al cliente

Director de ventas

Los Directores de ventas adquieren y retienen a los clientes, cumplen con las previsiones de ventas, proporcionan incentivos para aumentar el volumen de negocio con los clientes, contratan gestores, establecen los términos de fijación de precios, trabajan con el jefe de producto para establecer previsiones de inventario y trabajan con el Director de marketing para las promociones.

Representante de cuentas

Los representantes de cuentas trabajan con cuentas individuales para crear relaciones y gestionar los problemas de servicio al cliente. Pueden estar autorizados a realizar cambios de precio en los contratos, negociar contratos y perfiles así como a analizar la rentabilidad por categoría de cuenta.

Supervisor de servicio al cliente

Este rol tiene acceso a todas las tareas de servicio al cliente. El Supervisor de servicio al cliente gestiona las consultas de clientes (por ejemplo, el registro de clientes, los pedidos, las devoluciones y las subastas) y tiene autorización para realizar tareas a las que un Representante de servicio al cliente no puede acceder,

por ejemplo aprobar registros de devoluciones rechazadas por el sistema y ponerse en contacto con los clientes en relación a los problemas de pago (por ejemplo anomalías de autorización de tarjeta de crédito).

Representante de servicio al cliente

Por muy bien que esté diseñado un negocio en línea para proporcionar a un cliente características de autoservicio, habrá algunos tipos de clientes o algunas ocasiones en las que, incluso el cliente con más conocimientos sobre internet, necesitará el contacto personal. La mayoría de los negocios en línea proporcionan un correo electrónico, un fax o el número de una persona de contacto para que el cliente obtenga un servicio personal. El manejo de todas las consultas del cliente es responsabilidad del representante de servicio al cliente.

Gestión de marketing

WebSphere Commerce da soporte al rol de Director de marketing.

Director de marketing

El Director de marketing comunica la estrategia de mercado y los mensajes correspondientes a la marca comercial, a los clientes. Este rol supervisa, analiza y comprende el comportamiento del cliente. Además, el director de marketing crea o modifica los perfiles de clientes para la venta dirigida y crea y gestiona las campañas y promociones. La planificación de sucesos de campaña puede manejarla un equipo compuesto por el Comerciante, el Director de marketing y el Director de comercialización.

Gestión de la organización

WebSphere Commerce da soporte a los siguientes roles de gestión organizativa:

- Administrador de vendedores
- Administrador de compradores
- Aprobador de compradores

Administrador de vendedores

El Administrador de vendedores gestiona la información para la organización vendedora. Crea y administra las suborganizaciones de la organización vendedora y los diversos usuarios de la organización vendedora incluida la asignación de los roles de negocio apropiados.

Administrador de compradores

El Administrador de compradores gestiona la información para la organización compradora. Crea y administra las suborganizaciones de la organización compradora y gestiona los diversos usuarios incluida la aprobación de usuarios como compradores. Se puede crear y gestionar otros roles de la parte compradora, por ejemplo aprobadores de compradores y administradores de organización compradora adicionales.

Aprobador de compradores

Un aprobador de compradores es un individuo de la organización compradora que aprueba los pedidos realizados por el compradores antes de que se someta el pedido para la compra al vendedor.

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
Un 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) es para fines de control de acceso, mientras que un grupo de miembros de tipo Grupo de usuarios (-1) es para 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) es para agrupar usuarios para fines de control de acceso. Un grupo de acceso es un elemento de una política de control de acceso y se define como un grupo de usuarios definidos específicamente para fines 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 compradores o un administrador de vendedores utiliza la Consola de administración de la organización de WebSphere Commerce para asignar roles a los usuarios o para asignar explícitamente usuarios a los grupos de acceso. Los grupos de acceso pueden ser implícitos, explícitos o ambos.

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 `MBRGRP`. 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. 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 satisfacen las condiciones de inclusión en un grupo definido implícitamente, pero que desea excluir, de todos modos.

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 grupos 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 protegible (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 protegible, 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 de organización que posee la política. Las políticas que son propiedad de las entidades de organización antecesoras también se aplican al recurso.

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 el manual *WebSphere Commerce 5.4, Guía del programador* 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 protegible (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 el manual *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 incluir el estado, el ID de tienda, el precio, etc. Por ejemplo, puede crear un grupo de recursos implícito 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, mediante 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, la 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 construcción de cadena de relaciones. Una cadena de relaciones es una construcción 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="something">` 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 el valor de `valor1` es `HIERARCHY`, los valores posibles 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 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 sobre cómo definir grupos de relaciones, consulte el apartado “Definición de grupos de relaciones” en la página 92.

Propiedad de recursos y políticas

Todas las políticas son propiedad de una entidad de organización. Todos los recursos de control de acceso tienen un propietario que generalmente es una entidad de organización; por ejemplo, un pedido es propiedad de la organización que es propietaria de la tienda. Los usuarios también pueden poseer recursos, por ejemplo, un usuario registrado es el propietario de su propia información de registro de usuario. La propiedad de los recursos y las políticas de control de acceso es importante a la hora de determinar qué políticas se aplican a determinados recursos. A un recurso determinado, se le aplican las políticas que pertenecen a su entidad de organización propietaria y a las entidades de organización ascendentes de dicho propietario.

Tipos de políticas de control de acceso

Hay dos tipos de políticas de control de acceso:

- Políticas estándar
- Políticas de plantilla

Políticas estándar

Las políticas estándar tienen un propietario fijo. Por ejemplo, si una política estándar es propiedad de la organización vendedora, solamente se aplicará a los recursos que sean propiedad de la organización vendedora y a los recursos que sean propiedad de sus entidades de organización descendentes, si las hay. Dado que en WebSphere Commerce la organización raíz es la organización antecesora de todas las otras organizaciones, por definición, cualquier política que sea propiedad

de la organización raíz (member ID = -2001) se aplica a todos los recursos del sitio. De este modo, a veces se hace referencia a las políticas estándar que son propiedad de la organización como políticas a nivel de sitio.

Se hace referencia a las políticas estándar que no son propiedad de la organización raíz como políticas a nivel organizativo, ya que no se aplican a todo el sitio; solamente a los recursos que son propiedad del propietario de la política o de cualquiera de sus entidades de organización descendientes. Un administrador de la tienda puede gestionar las políticas de su propia entidad de organización y sus entidades de organización descendientes. Los administradores del sitio pueden modificar todas las políticas.

Políticas de plantilla

Las políticas de plantilla tienen un propietario dinámico. Las políticas de plantilla se aplican dinámicamente a la entidad de organización que es la propietaria del recursos y de sus entidades de organización antecesoras. Por ejemplo, si hay diez organizaciones bajo la organización raíz y cada una de ellas desea asegurarse de que solamente los administradores de tienda puedan modificar los recursos que son propiedad de la organización para la que desempeñan este rol. Hay dos modos de definirlo:

1. Tener una política de plantilla que se aplique dinámicamente a cualquiera de las 10 organizaciones, dependiendo del recurso al que se está accediendo. El criterio para el grupo de acceso de la política de plantilla también puede ser dinámico. Por ejemplo, si un usuario intenta acceder a un recurso que es propiedad de la organización 3, el propietario de la política de plantilla pasará a ser dinámicamente la organización 3 y el grupo de acceso también pasará a estar dinámicamente en el ámbito de la organización 3, es decir, el usuario debe desempeñar el rol de administrador de tienda para la organización 3.
2. Tener 10 políticas, cada una de las cuales será propiedad de 10 organizaciones. El grupo de acceso de la organización 1 especificará el usuario que debe desempeñar el rol de administrador de tienda para la organización 1. El grupo de acceso de la organización 2 debe especificar que el usuario debe desempeñar el rol de administrador de tienda para la organización 2, etc.

La ventaja de la primera solución es que solamente hay una copia física de la política y 10 copias lógicas. Las políticas de plantilla las puede gestionar un administrador de sitio.

Alteración temporal de las políticas de plantillas: Otra característica de las políticas de plantilla es que se pueden alterar temporalmente para las entidades de organización especificadas. Utilizando el ejemplo anterior, si se añade una onceava organización al sitio de WebSphere, pero esta entidad de organización reciente no desea que se le aplique la política de plantilla mencionada, existe un método para hacerlo. Se debe añadir una entrada a la tabla `ACORGPOL` que especifique el ID de política de la política de plantilla y el ID de la entidad de organización de la onceava organización. Esto también se puede llevar a cabo a través de la Consola de administración de WebSphere Commerce, cuando un administrador de la tienda suprime o actualiza una política de plantilla, dentro del contexto de una organización determinada.

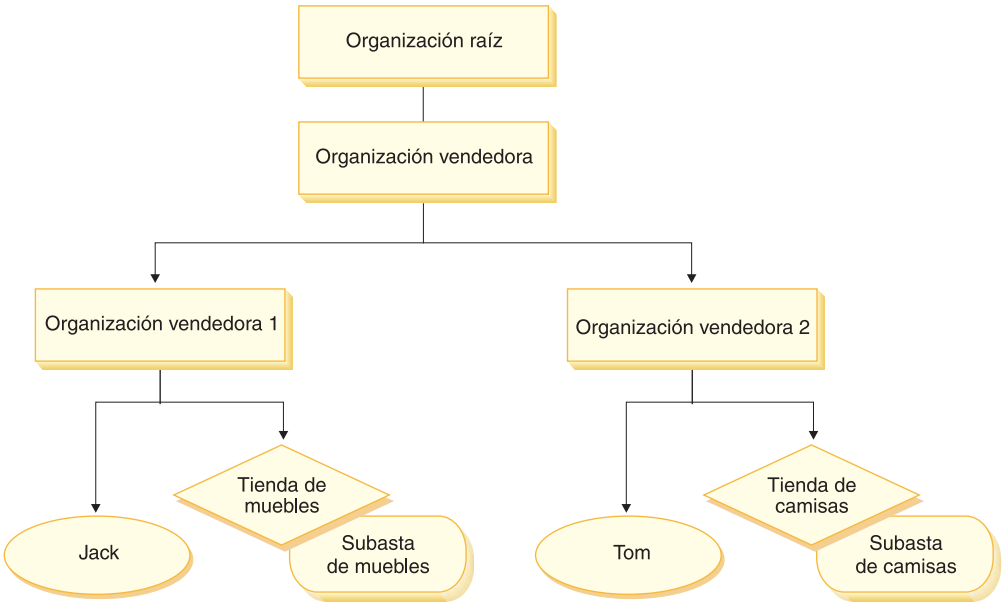
Cuando se altera una política de plantilla para una organización descendiente de la organización raíz, la política de plantilla se continúa aplicando en el nivel de la organización raíz. Si la política de plantilla se altera temporalmente con una política más restrictiva en el nivel de la organización descendiente, deberá alterar también temporalmente la política de plantilla en el nivel de la organización raíz.

El único método de alterar temporalmente una política de plantilla para la organización raíz es a través de la base de datos, ejecutando el siguiente SQL:

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

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, Jack y Tom son vendedores, por lo tanto, ambos pueden modificar subastas.

El control de acceso basado en roles se utilizar 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. Todos los mandatos de controlador deben protegerse mediante control de acceso a nivel de mandato. Además, cualquier vista que se pueda llamar directamente o que pueda iniciarse mediante un redireccionamiento desde otro mandato (en oposición a iniciarla enviándola a la vista) debe protegerse mediante control de acceso a nivel de mandatos.

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 grueso, ya que determinan quién puede ejecutar qué mandato en qué recursos. El ejemplo anterior de una política de control de acceso basadas en roles que permite que los vendedores modifiquen las subastas, se puede ajustar de modo que el control de acceso a nivel de recurso sea: los vendedores pueden modificar las subastas que son propiedad de la organización para la que desempeñan su rol. En la página 24, Jack tiene el rol de vendedor para la organización vendedora 1. Tom tiene el rol de vendedor para la organización vendedora 2. Jack crea una subasta de muebles en la tienda de muebles. Tom crea una subasta de camisas en la tienda de camisas. Jack puede modificar la subasta de muebles, pero *no* la subasta de camisas. Tom 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 recurso 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 recurso 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.

Cómo el control de acceso impide 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

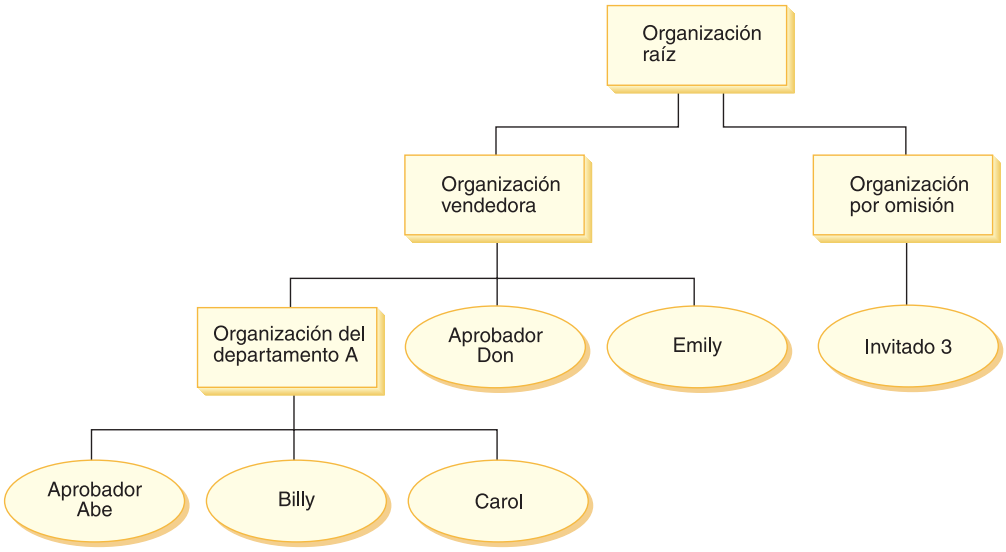
El *Gestor de políticas* es el componente de control de acceso que determina si el usuario actual puede ejecutar la acción especificada en el recurso especificado. Las políticas de control de acceso están especificadas en formato XML. Durante la creación de la instancia, se cargan automáticamente las 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 reinicia WebSphere Commerce también se actualizará la antememoria.

Cuando un usuario intenta efectuar una acción protegida por el control de acceso, 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.

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 le presenta un escenario y se le guía por un ejemplo de cómo evaluar una política de control de acceso 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, consulte el apartado “Tipos de políticas de control de acceso” en la página 22.

El diagrama siguiente muestra gráficamente el escenario:



Jerarquía de organizaciones

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

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, Don y Emily están registrados en la organización vendedora. Abe, Billy y Carol están registrados en la organización del departamento A. El invitado 3 no está registrado pero para fines de control de acceso, pertenece de forma implícita a la organización por omisión.

Roles

Don desempeña el rol de aprobador para la organización vendedora. Abe desempeña el rol de aprobador para 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.
- 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

Este apartado es una guía para evaluar las políticas estándar 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, - ]
```

Es una política estándar basada en roles propiedad de la organización raíz. En esta política, los usuarios registrados pueden ejecutar mandatos `Update Document`.

Política 2:

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

Es una política estándar a nivel de recursos propiedad de la organización raíz. 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, - ]
```

Es una política estándar a nivel de recurso propiedad de la organización vendedora. 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, - ]
```

Es una política estándar a nivel de recursos propiedad de 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 : Billy 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 que son propiedad de 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 Billy 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 Billy es propiedad del departamento A. Por lo tanto, solamente se aplicarán las políticas que son propiedad del departamento A y sus organizaciones antecesoras: las políticas 1, 2, 3 y 4.
2. La política 2 otorga acceso ya que Billy 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 Billy ha pasado las dos comprobaciones de control de acceso, a nivel de mandato y a nivel de recursos, puede actualizar su propio documento.

Escenario 2: Don intenta actualizar el documento de Carol: 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 que son propiedad de 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 Don 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 Carol es propiedad del departamento A. Por lo tanto, solamente se aplicarán las políticas que son propiedad del departamento A y sus organizaciones antecesoras: las políticas 1, 2, 3 y 4.
2. La política 4 otorga acceso ya que Don es miembro del grupo de acceso de Aprobadores de organización vendedora y está realizando la acción de mandato `Execute` en el recurso de documento.

Dado que Don ha pasado las dos comprobaciones de control de acceso, a nivel de mandato y a nivel de recursos, puede actualizar el documento de Carol.

Escenario 3: Abe intenta actualizar el documento de Emily: 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 que son propiedad de 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 Abe 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 Emily es propiedad de la organización vendedora. Por lo tanto, solamente se aplicarán las políticas que son propiedad de la organización vendedora y sus organizaciones antecesoras: las políticas 1, 2 y 3.
2. La política 3 NO otorga acceso ya que Abe NO es miembro del grupo de acceso Aprobadores de la organización vendedora.

Aunque Abe ha pasado la comprobación a nivel de mandato, como no ha pasado la comprobación de control de acceso a nivel de recurso, no puede actualizar el documento de Emily.

Escenario 4: el 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 que son propiedad de 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 invitado NO es miembro del grupo de acceso `Usuarios registrados`.

Comprobación a nivel de recursos:

1. La comprobación a nivel de recurso ni siquiera se lleva a cabo ya que no se ha superado la comprobación a nivel de mandato.

Dado que el invitado 3 no ha pasado la comprobación a nivel de mandato, no puede actualizar su propio documento.

Evaluación de las políticas de plantilla

Este ejemplo está basado en el escenario anterior.

Políticas de control de acceso relacionadas con la actualización de documentos

Cuando se evalúan políticas de control de acceso, se continúan aplicando las políticas de control de acceso 1 y 2 que se utilizaban para evaluar las políticas estándar, sin embargo, las políticas estándar 3 y 4 se sustituyen ahora por las política de plantilla 5. Para obtener más información sobre las políticas 1 y 2, consulte el apartado “Evaluación de las políticas estándar” en la página 28.

Política 5:

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

Esta política es una política de plantilla a nivel de recursos. Los aprobadores de la organización que es la propietaria del documento, pueden actualizar los documentos.

Esta política de plantilla también necesita utilizar un nuevo grupo de acceso con parámetros. A este escenario se añade el grupo de acceso siguiente:

- Aprobadores para la organización: este grupo incluye implícitamente a todos los usuarios que tienen el rol de aprobador para la organización `?`. (El parámetro `?` cambiará de forma dinámica por el propietario de la política a medida que se aplique la política de plantilla durante la ejecución.).

Escenarios

Los escenarios siguientes utilizan solamente las políticas 1, 2 y 5.

Escenario 1: Don intenta actualizar el documento de Carol: 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 que son propiedad de 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. Durante la evaluación de la política, las políticas de plantilla pasan dinámicamente a ser propiedad de la organización que posee el recurso y, posteriormente, de los antecesores de la organización, por lo tanto, también se aplicará la política 5.
2. La política 1 otorga acceso ya que Don 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 Carol es propiedad del departamento A. Por lo tanto, solamente se aplicarán las políticas que son propiedad del departamento A y sus organizaciones antecesoras: las políticas 1 y 2. Durante la evaluación de la política, las políticas de plantilla pasan dinámicamente a ser propiedad de la organización que posee el recurso y, posteriormente, de los antecesores de la organización, por lo tanto, también se aplicará la política 5.
2. La política de plantilla 5 se aplica en primer lugar a la organización que es la propietaria del recurso: el departamento A. En este momento la política 5 esencialmente se comporta como la política 5a:

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

3. La política 5a NO otorga acceso ya que Don NO es miembro del grupo de acceso Aprobadores del departamento A.
4. La política de plantilla 5 se aplicará a continuación en la organización padre del departamento A: la organización vendedora. En este momento la política 5 esencialmente se comporta como la política 5b:

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

5. La política 5b otorga acceso ya que Don es miembro del grupo de acceso de Aprobadores de la organización vendedora y está realizando la acción de mandato `Execute` en el recurso de documento.

Dado que Don ha pasado las dos comprobaciones de control de acceso, a nivel de mandato y a nivel de recursos, puede actualizar el documento de Carol.

Escenario 2: Abe intenta actualizar el documento de Emily: 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 que son propiedad de 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. Durante la evaluación de la política, las políticas de plantilla pasan dinámicamente a ser propiedad de la organización que posee el recurso y, posteriormente, de los antecesores de la organización, por lo tanto, también se aplicará la política 5.
2. La política 1 otorga acceso ya que Abe 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 Emily es propiedad de la organización vendedora. Por lo tanto, solamente se aplicarán las políticas que son propiedad de la organización vendedora y sus organizaciones antecesoras: las políticas 1 y 2. Durante la evaluación de la política, las políticas de plantilla pasan dinámicamente a ser propiedad de la organización que posee el recurso y, posteriormente, de los antecesores de la organización, por lo tanto, también se aplicará la política 5.
2. La política de plantilla 5 se aplica en primer lugar a la organización que es la propietaria del recurso: la organización vendedora. En este momento la política 5 esencialmente se comporta como la política 5a:

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

3. La política 5a NO otorga acceso ya que Abe NO es miembro del grupo de acceso Aprobadores de la organización vendedora.
4. La política de plantilla 5 se aplicará a continuación a la organización padre de la organización vendedora: la organización raíz. En este momento la política 5 esencialmente se comporta como la política 5b:

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

5. La política 5b NO otorga acceso ya que Abe NO es miembro del grupo de acceso Aprobadores de la organización raíz.
6. La organización raíz no tiene una organización padre, por lo tanto, la política de plantilla 5 se ha evaluado por completo.

Aunque Abe ha pasado la comprobación a nivel de mandato, como no ha pasado la comprobación de control de acceso a nivel de recurso, no puede actualizar el documento de Emily.

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.

En el primer ejemplo, describiremos cómo puede leerse la política utilizando la Consola de administración de WebSphere Commerce, identificaremos sus componentes y describiremos 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 WebSphere Commerce para estudiar una política e identificar los componentes que la definen. También utilizaremos estos componentes para describir de forma general la política.

Análisis de la política en la Consola de administración

1. Inicie la sesión en la Consola de administración de WebSphere Commerce. En el menú Gestión de acceso, seleccione **Políticas**.
2. Compruebe que el menú desplegable Ver esté establecido para su organización.
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 acciones siguientes o mandatos, 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) al que se aplica 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. Deje la página Criterios sin realizar cambios. 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, AuctionAdministrator. ForOrg indica que la política se aplica a las organizaciones. 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 observa una política en la Consola de administración de WebSphere Commerce, está utilizando la interfaz para ver y realizar cambios en 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.

La mayor parte del tiempo utilizará la interfaz de usuario de la Consola de administración de WebSphere Commerce para gestionar políticas. Sin embargo, si desea ver una política en formato XML, o si desea realizar una modificación avanzada, la política en un archivo XML tendrá este aspecto:

```
<!-- AuctionAdministrators
manage Auctions (Retract/delete auction,
Modify auction, Close Auction)
-->
<Policy
 Name="AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource"
OwnerID="RootOrganization"
UserGroup="AuctionAdministratorsForOrg"
ActionGroupName="AuctionManage"
ResourceGroupName="AuctionDataResourceGroup"
PolicyType="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, a nivel de sitio, de plantilla o de organización.

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 recurso. 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 recurso 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 acción está asociada 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 el Capítulo 5, “Escenarios de personalización” en la página 47, 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.

Capítulo 4. Personalización de las políticas de control de acceso

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 de control de acceso” en la página 9 para obtener más información.

Identificación de las políticas afectadas por un cambio

En el capítulo anterior, hemos descrito las políticas que 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

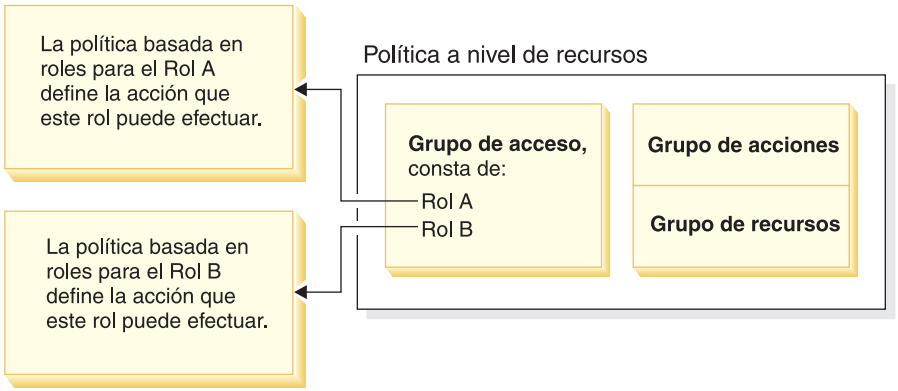
En WebSphere Commerce, cada acción que puede llevar a cabo un usuario se asigna a uno o varios roles mediante las políticas basadas en roles, como se describe a continuación:

- Cada rol por omisión tiene un grupo de acceso correspondiente. Por ejemplo, el grupo de acceso del rol de Administrador de tienda es `StoreAdministrators`.
- 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. Los mandatos de vista se correlacionan con las vistas de la tabla VIEWREG. Por ejemplo, `StoreListView` muestra una página Web con la lista de las tiendas del sistema.

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.

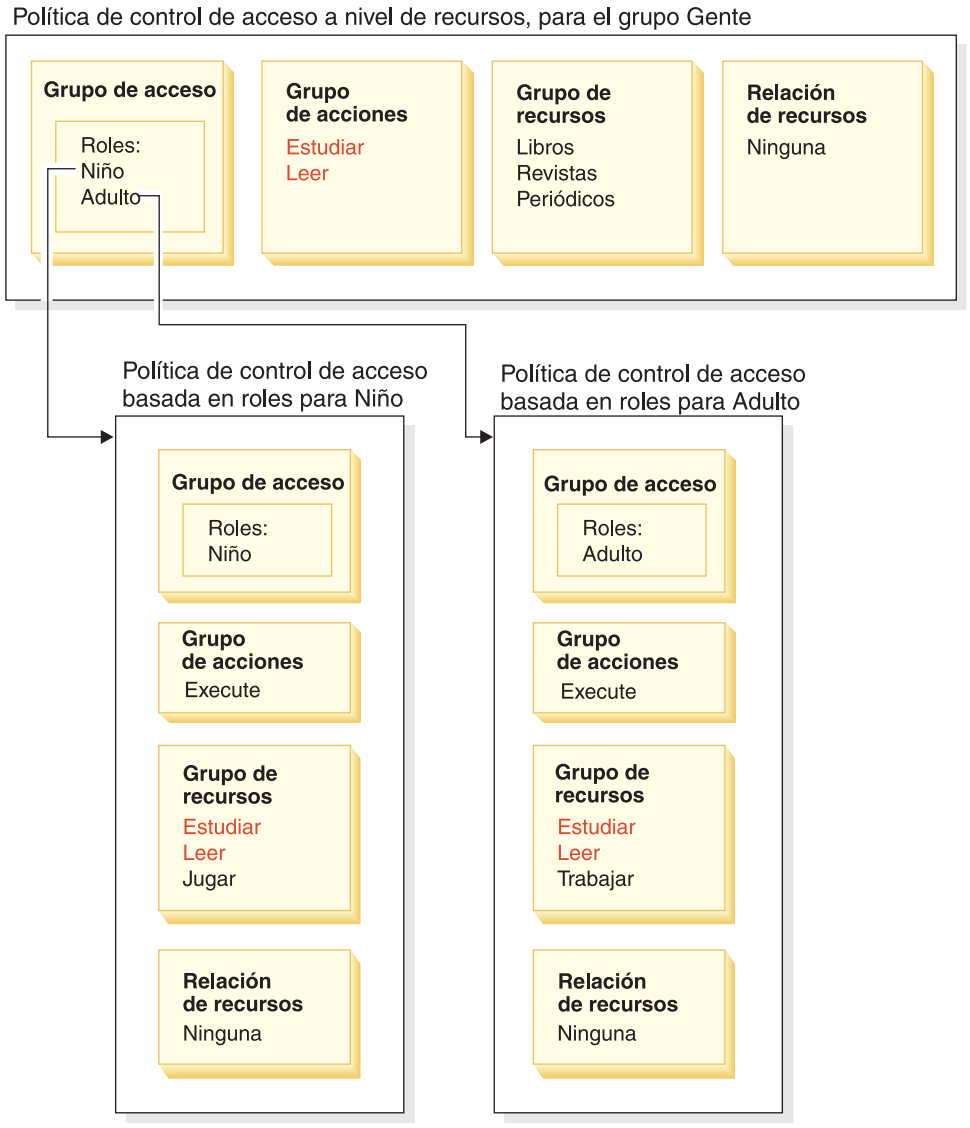
Las políticas a nivel de recursos para mandatos de controlador están relacionadas directamente con determinadas políticas basadas en roles para mandatos de controlador. En la política a nivel de recursos, el mandato del controlador forma parte del grupo de acciones pero en la política basada en roles, 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 3. Relación entre una política a nivel de recurso 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 4. 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 desde 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 1 resume los cambios adicionales que deberá realizar cuando cree, suprima o cambie una política a nivel de recursos.

Tabla 1. Cambios adicionales que son necesarios cuando se cambia una política a nivel de recursos que utiliza roles.

Cuando realiza este cambio en una política a nivel de recursos:	**También debe realizar el cambio siguiente si el grupo de acceso del 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: `SalesManagersExecuteSalesManagerViews`.

En las políticas basadas en roles para vistas, el grupo de acciones contiene una lista de las vistas que los usuarios que poseen dicho rol pueden ejecutar.

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:
`AuctionAdministorsForOrgExecuteAuctionCreateCommandsOnStoreEntityResource`.

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 11.
- 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, seleccione **Gestión de acceso > Grupos de acceso** en la Consola de administración.
- Dependiendo del valor que seleccione para Vista, la página de políticas mostrará las políticas a nivel de sitio o las políticas específicas de una organización determinada:
  - Si el campo Vista lo establece en `Organización raíz`, se mostrarán las políticas a nivel de sitio y las versiones maestras de las políticas de plantilla.
  - Si el campo Vista lo establece en el nombre de una organización, se mostrarán las políticas definidas únicamente para la organización y las políticas de plantilla que dicha organización puede modificar.
- Cambie el nombre de cualquier política por omisión, de modo que el nombre de la política por omisión 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: La Consola de administración de WebSphere Commerce 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 nuevas, recursos, atributos, relaciones, grupos de relaciones.
2. Definir grupos de recursos implícitos complejos y grupos de acceso implícitos complejos.

Después de modificar la política

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 subastas 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. El Apéndice describe los diferentes archivos XML relacionados con las políticas de control de acceso y los grupos de acceso. También describe cómo extraer los cambios realizados en las políticas de las bases de datos y pasarlos a los archivos XML, y cómo cargar la información de políticas desde los archivos XML a las bases de datos.

Capítulo 5. Escenarios de personalización

Los escenarios de personalización que se muestran más adelante le permiten aplicar lo que ha aprendido sobre las políticas de control de acceso y realizar diversos cambios en las políticas por omisión. 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 2. 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 48
Contratos	"Escenario de contratos 1: suprimir la posibilidad de que los administradores de contratos puedan añadir o suprimir adjuntos de contratos" en la página 52
Pedidos	"Escenario de pedidos 1: permitir que solamente los compradores puedan crear pedidos" en la página 55
Miembros	"Escenario de miembros 1: suprimir la posibilidad de que el usuario pueda autorregistrarse" en la página 61
Cupones	"Escenario de cupones 1: permitir que solamente los compradores puedan canjear cupones" en la página 66
Suministros	"Escenario de suministros 1: permitir que los jefes de compras gestionen el carro de la compra de suministros para los pedidos creados por su organización" en la página 70
Inventario	"Escenario de inventario 1: permitir que los administradores del centro de formalización de pedidos puedan actualizarlos pero no suprimirlos" en la página 73
Business intelligence	"Escenario de Business intelligence 1: permitir que los auditores vean los informes de business intelligence" en la página 74

Si está buscando un escenario que describa un tipo de cambio determinado, consulte la tabla siguiente, que muestra una referencia cruzada de los escenarios según el tipo de personalización descrito.

Tabla 3. Escenarios de personalización organizados por tipo de personalización

Personalización	Vea la página
Añadir un rol a un grupo de acceso de política	68
Cambiar un grupo de acceso de política	71,73
Cambiar una relación de recursos de una política	57,70
Cambiar una política para que utilice un grupo de acceso diferente	51,55,57,62,66,68
Crear un nuevo grupo de acceso y utilizarlo en una política	60,63
Crear un grupo de acciones nuevo y utilizarlo en una política	63,71
Crear una política a nivel de recursos nueva	54,71
Crear una política basada en roles nueva	63,74
Crear un nuevo rol y utilizarlo en una política a nivel de recursos	63,74
Suprimir una política	49,50,62
Suprimir una acción de un grupo de acciones de una política	3,53

Tabla 3: Escenarios de personalización organizados por tipos de personalización

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. Busque el apartado de Subastas en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es:

   ```
   AuctionAdministratorsForOrgExecuteAuctionManageCommandsOnAuctionResource
   ```

2. En la Consola de administración, 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— `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 recursos.
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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

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

Por omisión, los administradores 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 administradores 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. Busque el apartado de Subastas en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es:

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.

3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. En la lista de políticas, seleccione lo siguiente:

   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource
5. Pulse **Suprimir**.

Actualizar el registro de políticas con los cambios

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

Escenario de subastas 3: suprimir la posibilidad de que los administradores de subastas puedan retractar las ofertas de subasta de una organización

Por omisión, los administradores de subastas de una tienda pueden retractar las ofertas que se han sometido en sus subastas. En algunos casos, como administrador de sitio, es posible que desee cambiar esta política para una organización determinada. Para realizar este cambio, debe suprimir la política de plantilla que autoriza esta acción para esta organización.

Nota: En WebSphere Commerce Professional Edition, solamente hay tres organizaciones, la organización raíz, la organización por omisión y la organización vendedora.

Después de suprimir la política, el administrador de subastas de dicha organización ya no podrá retractar las ofertas de subasta. Los administradores de subastas de las otras organizaciones no se verán afectados por este cambio.

Para suprimir la política, deberá realizar lo siguiente:

- Utilice el Apéndice para buscar la política a nivel de recursos que autoriza la retracción de las ofertas de subasta.
- Localice la política en la lista de políticas de la organización.
- Suprima la política.

Pasos que debe realizar

Suprimir la política

1. Busque el apartado de Subastas en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es:

   `AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource`
2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione la organización cuya política desea suprimir. Cuando seleccione una organización determinada, en lugar de la `Organización raíz`, los cambios que realice en la política se aplicarán solamente a dicha organización y no a todas las organizaciones del sitio.
4. En la lista de políticas, seleccione lo siguiente:

   AuctionAdministratorsForOrgExecuteAdminRetractBidCommandsOnAuctionResource
5. Pulse **Suprimir**.

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

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

Escenario de subastas 4: 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. Busque el apartado de Subastas en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es: `RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource`.
2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
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 > Grupo 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 el rol de comprador (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(buyside)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. Pulse **Configuración >Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

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

Por omisión, los administradores 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 administradores 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 administrador de contratos. Para suprimir la autorización que tienen los administradores 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 administradores 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. Busque el apartado de Contratos en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es:

   `ContractAdministratorsForOrgExecuteContractManageCommandsOnContractResource`
2. En la Consola de administración, 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— `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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. 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. Busque el apartado Contratos del Apéndice para buscar 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, 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— `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 **Nuevo** 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 políticas, seleccione **Política de plantilla** 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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

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 limitar la creación de pedidos a los miembros de una organización compradora que tengan el rol de `comprador`, realice 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 modo que dejen de ser todos los usuarios y pasen a ser aquellos 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 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 pedidos.
- Actualice este grupo de recursos de la política basada en roles para que incluya el mandato para crear pedidos.

Nota: Esta política es una política de plantilla a nivel de recursos. En este escenario, se ha modificado la copia maestra de esta plantilla al nivel de la organización raíz. Si desea modificarla solamente para una organización determinada que no sea la organización raíz, antes de cambiar la política tendrá que cambiar la vista por la de otra organización. Esto hará que la política de plantilla se altere temporalmente solamente para esta organización. De este modo, se creará una política estándar nueva para esta organización, que tendrá el grupo de acceso de usuarios compradores (parte compradora) más restringido. Dado que la política de plantilla menos restringida continúa aplicándose a nivel de la organización raíz, también deberá alterarse temporalmente a este nivel. Actualmente, el único modo de hacerlo es actualizando manualmente la tabla ACORGPOL en la base de datos y ejecutando las sentencias SQL siguientes:

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

Pasos que debe realizar

Identificar la política a nivel de recursos

1. Busque el apartado de Pedidos en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es: `AllUsersExecuteOrderCreateCommandsOnStoreResource`.
2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
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
```

   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(buyside)ExecuteBuyers(buyside)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. Anote el nombre del grupo de recursos—`Buyers(buyside)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(buyside)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
```

6. Pulse **Añadir.**
7. Pulse **Terminar**.

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

1. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. 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. Busque el apartado de Pedidos en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es: `AllUsersExecuteOrderWriteCommandsOnOrderResource`.
2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
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. 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 modificar pedidos

1. Pulse **Gestión de acceso > Grupo 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
```

Debe añadir estos mandatos al grupo de recursos que contiene la lista de mandatos que puede ejecutar un comprador.

Notas:

a. El mandato `com.ibm.commerce.orderitems.commands.AdminOrderItemUpdateCmd`, no es necesario.

b. 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 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
   ```
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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. 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. Busque el apartado Pedidos del Apéndice para buscar 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, 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—`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 **Nuevo** 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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. 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. Busque el apartado Miembros del Apéndice para buscar la política a nivel de recursos que autoriza el autorregistro de los usuarios. La política es: `GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource`.
2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. En la lista de políticas, seleccione **GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource**
5. Pulse **Suprimir**.

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

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

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. Busque el apartado Miembros del Apéndice para buscar 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, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. 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 autoriza a los operadores de miembros a registrar 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 `MemberRegistrationCommands`, que incluya los mandatos 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, 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 incluirse en la propia organización de los usuarios.
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. Busque el apartado Miembros del Apéndice para buscar la política a nivel de recursos que autoriza a los administradores de miembros a registrar usuarios. La política es:

   ```
   MembershipAdministratorsForOrgExecuteUserAdminRegistration
   CommandsOnOrganizationResource
   ```

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 **Nuevo**.
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**.

Modificar la política a nivel de recursos de modo que utilice el nuevo grupo de acceso

1. En la lista de políticas, seleccione lo siguiente:

   MembershipAdministratorsForOrgExecuteUserAdminRegistration CommandsOnOrganizationResource
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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

Escenario de cupones 1: permitir que solamente los compradores puedan canjear cupones

Por omisión, todos los usuarios registrados 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 modo que dejen de ser todos los usuarios registrados y pasen a ser aquellos que tienen el rol de `comprador`.
- Identifique el mandato para canjear cupones.
- 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 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. Busque el apartado de Cupones en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es:

   `RegisteredApprovedUsersExecuteCouponRedemptionCommandsOnCouponWalletResource`
2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
4. En la lista de políticas, seleccione lo siguiente:

RegisteredApprovedUsersExecuteCouponRedemption CommandsOnCouponWalletResource

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 > Grupo 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(buyside)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. Anote el nombre del grupo de recursos: `Buyers(buyside)CommandsResourceGroup`. Este 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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

Escenario de cupones 2: permitir que los administradores de cupones y los administradores de tienda 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 administradores de tienda 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 administrador de tienda 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 administradores de tienda crear promociones de cupones.

Este escenario describe el primer método. Le muestra cómo puede añadir el rol de administrador de tienda a la política a nivel de recurso 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 `administrador de tienda`.
- 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 los `administradores de tienda`. Esta política define los mandatos que pueden ejecutar los usuarios que tienen el rol de `administrador de tienda`. 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. Busque el apartado de Cupones en el Apéndice, para identificar la política a nivel de recursos que debe modificarse. La política es:

   CouponAdministratorsForOrgExecuteCouponPromotionCreateCommands OnStoreEntityResource
2. En la Consola de administración, 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 —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 la 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 **Administrador de tienda**.
6. Pulse **Para organización** para especificar que el rol debe incluirse en la propia organización de los usuarios.
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 administrador de tienda.

Identificar la política basada en roles para administradores de tienda

1. Busque en el apartado de políticas basadas en roles del Apéndice la política basada en roles para administradores de compradores. La política es: StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup.
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—StoreAdministratorsCmdResourceGroup. Este 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 **StoreAdministratorsCmdResourceGroup**.
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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

Escenario de suministros 1: permitir que los jefes de compras gestionen el carro de la compra de suministros 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 de suministros 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 suministros 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 de suministros a gestionar sus carros de la compra de suministros.
- Cambiar 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. Busque el apartado Suministros del Apéndice para buscar la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de suministros de los pedidos. La política es:

   ```
   ProcurementShoppingCartManagersExecuteProcurementShopping
   CartManageOnOrderResource
   ```

2. En la Consola de administración, pulse **Gestión de acceso > Políticas**.
3. En Vista, seleccione **Organización raíz** para visualizar las políticas a nivel de sitio.
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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.

3. Pulse **Actualizar**.

Escenario de suministros 2: permitir que los administradores de compradores de suministros sometan el carro de la compra de suministros 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 de suministros 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 de suministros que contienen pedidos creados por ellos pero otorgar a los administradores de compradores de suministros 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 de suministros 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 de suministros 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 de suministros del grupo de acciones de la política.
- Defina un nuevo grupo de acciones que contenga el mandato para someter un carro de la compra de suministros. Utilizará este grupo de acciones para definir la nueva política a nivel de recursos que autoriza a los administradores de compradores de suministros a someter los carros de la compra de suministros 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 de suministros a someter los carros de la compra de suministros 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. Busque el apartado Suministros del Apéndice para buscar la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de suministros de los pedidos. La política es:

   ```
   ProcurementShoppingCartManagersExecuteProcurement
   ShoppingCartManageOnOrderResource
   ```

2. En la Consola de administración, 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 de suministros.
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 > Grupo 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 a nivel de sitio.
3. Pulse **Nuevo** 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 políticas, seleccione **Política de plantilla** 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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

Escenario de inventario 1: permitir que los administradores del centro de formalización de pedidos puedan actualizarlos pero no suprimirlos

Por omisión, los administradores del centro de formalización de pedidos tienen autorización para actualizar o suprimir los centros de formalización 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 formalización de pedidos del grupo de acciones de la política.

Pasos que debe realizar

Suprimir la acción para suprimir un centro de formalización de pedidos

1. Busque el apartado Suministros del Apéndice para buscar la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de suministros de los pedidos. La política es:

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenter
   ManageCommandsOnFulfillmentResource
   ```

2. En la Consola de administración, 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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. Pulse **Actualizar**.

Escenario de inventario 2: permitir que solamente los jefes de logística y los jefes de operaciones puedan crear, actualizar o suprimir los centros de formalización de pedidos

Por omisión, los administradores del centro de formalización de 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 formalización de pedidos incluye los roles: vendedor, jefe de logística y jefe de operaciones. Es posible que en algunos casos desee que los vendedores no tengan autorización para ser administradores del centro de formalización 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 formalización de pedidos`.

Pasos que debe realizar

Suprimir el rol de vendedor del grupo de acceso

1. Busque el apartado Suministros del Apéndice para buscar la política a nivel de recursos que autoriza a los jefes de compras a gestionar los carros de la compra de suministros de los pedidos. La política es:

   ```
   FulfillmentCenterManagersForOrgExecuteFulfillmentCenterManage
   CommandsOnFulfillmentResource
   ```

2. En la Consola de administración, 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. Pulse **Configuración > Registro**.
2. En la lista de registros, seleccione **Políticas de control de acceso**.
3. 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 y, para este rol, cree un nuevo grupo de acceso, un nuevo grupo de recursos y una nueva política basada en roles.
- Añada un rol al grupo de acceso de la política a nivel de recursos.
- Defina un nuevo rol llamado `Auditor`.
- Defina un nuevo grupo de acceso, llamado `Auditors`, que incluya el rol de auditor.
- 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.

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, 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. Busque el apartado Business Intelligence del Apéndice para buscar 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, 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—`ViewBusinessIntelligenceReport`. Este es el grupo de acciones que debe visualizar para identificar las acciones para registrar miembros.
6. Pulse **Gestión de acceso > Grupo 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 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. 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 **Nuevo**.
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 incluirse en la propia organización de los usuarios.
7. Pulse **Añadir**.
8. Pulse **Aceptar**.

Actualizar el registro de políticas con los cambios

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

Capítulo 6. Utilización de archivos XML para personalizar las políticas de control de acceso

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 directamente los archivos XML.

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 del manual *IBM WebSphere Commerce, Guía del programador*. 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 *IBM WebSphere Commerce, Guía del programador*, 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:

- Proteger un nuevo mandato o vista
- Crear o modificar una relación
- Crear o modificar un grupo de relaciones
- Proteger un nuevo recurso
- Crear o modificar atributos
- Crear o modificar grupos de acceso utilizando criterios complejos
- Crear o modificar grupos de recursos utilizando criterios complejos

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 4. Archivos XML de WebSphere Commerce para el control de acceso

Nombre de archivo	Descripción
ACUserGroups_de_DE.xmll ACUserGroups_en_US.xml ACUserGroups_es_ES.xml ACUserGroups_fr_FR.xml ACUserGroups_it_IT.xml ACUserGroups_ja_JP.xml ACUserGroups_ko_KR.xml ACUserGroups_pt_BR.xml ACUserGroups_zh_CN.xml ACUserGroups_zh_TW.xml	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 la información de control de acceso que ha se modificado.
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.

Tabla 4. Archivos XML de WebSphere Commerce para el control de acceso (continuación)

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.

Personalización de archivos XML

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">
</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.

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 la definición de 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 basada en roles, efectúe lo siguiente:

1. Cree una nueva definición de acción en el archivo XML que tenga el nombre de vista MyNewView.

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

2. Determine qué roles deben tener acceso a esta vista y asocie la nueva acción a los grupos de acciones correspondientes del archivo XML:

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

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

   </ActionGroup>
   ```

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 104.
4. En la Consola de administración, actualice el registro de políticas de control de acceso.

Dado que ya existe una política basada en roles que incluye este grupo de acciones, ahora puede utilizarse la vista.

Añadir una vista nueva mediante una política nueva

Para añadir una vista nueva a la que se pueda acceder mediante un nuevo rol que no tenga una política basada en roles existente, efectúe lo siguiente:

1. Cree una nueva definición de acción en el archivo XML que tenga el nombre de vista MyNewView.

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

2. Cree un nuevo grupo de acciones que se asociará al nuevo rol:

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

3. Asocie la nueva acción al nuevo grupo de acciones:

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

   <ActionGroupAction Name="MyNewView"/>

   </ActionGroup>
   ```

4. Cree una política que haga referencia al nuevo grupo de acciones:

   ```
   <Policy Name="XYZExecuteXYZViews"
   OwnerID="RootOrganization"
   UserGroup="XYZ"
   ActionGroupName="XYZViews"
   ResourceGroupName="ViewCommandResourceGroup">
   </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 104.
6. En la Consola de administración, actualice el registro de políticas de control de acceso.

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 “Implementación del control de acceso a nivel de recursos” en la página 86. 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">
</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 de recursos `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 (protegible). Para obtener más información acerca de estas interfaces, consulte el manual *IBM WebSphere Commerce, Guía del programador*.

Añadir un mandato de controlador nuevo mediante las políticas existentes

Para añadir un nuevo mandato de controlador al que pueda accederse mediante roles que tienen políticas de mandatos de controlador basados en roles existentes, efectúe lo siguiente:

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 qué roles deben tener acceso al mandato y asocie el nuevo recurso a los grupos de recursos correspondientes del archivo XML:

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

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

</ResourceGroup>
```

3. 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 104.
4. En la Consola de administración, actualice el registro de políticas de control de acceso.

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.

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, efectúe lo siguiente:

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 84.
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="XYZExecuteXYZsCmdResourceGroup"
OwnerID="RootOrganization"
UserGroup="XYZ"
ActionGroupName="ExecuteCommandActionGroup"
ResourceGroupName="XYZCmdResourceGroup">
</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 104.
6. En la Consola de administración, actualice el registro de políticas de control de acceso.

Ahora puede utilizar el mandato de controlador si no está realizando la comprobación a nivel de recursos.

Implementación del control de acceso a nivel 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 ampliación de otro mandato que está realizando una comprobación a nivel de recursos.
- 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="template">
</Policy>
```

Donde:

`Name`: el nombre de la política.

`PolicyType`: el tipo de política. Es una política de plantilla 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. Es una política de plantilla y cambiará dinámicamente para ser la entidad de organización propietaria del recurso y sus antecesores, cuando el gestor de políticas de control de acceso aplique 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 entidad de organización del recurso y sus antecesores 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 las 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, Guía del programador*.

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, Guía del programador*

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">
```

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 *IBM WebSphere Commerce, Guía del programador*.

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 al atributo y el elemento Type identifica el tipo de datos del atributo. Los valores posibles del atributo son:

- String
- Integer
- Double
- Durrency
- 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="valor"
OwnerID="valor">
<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="valor"/>
</openCondition>
```

Donde:

`<parameter name="Relationshiop" value="algún valor">`: una serie que representa la relación entre el usuario y el recurso.

`name`: corresponde al parámetro de relación del método `fulfills()` en el recurso protegible.

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, `<parmeter 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 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 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 92

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_inst_wc*`/xml/policies/xml/ACUserGroups_entorno_nacional.xml`. Este archivo sigue la DTD especificada por *dir_inst_wc*`/xml/policies/dtd/ACUserGroups_es_ES.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 acceso, 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 5. 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. • `?`: cuando se utiliza en una política de plantilla.
`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
`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

Tabla 5. Nombres de condiciones simples (Simplecondition) a las que se da soporte (continuación)

org	Especifica que el usuario debe estar registrado en esta organización padre. Se almacena en la tabla MBRREL.	= !=	• Cualquier valor de ORGENTITY_ID en la tabla ORGENTITY. • ?- si se trata de una política de plantilla.	ninguno	no disponible

Nota: El signo ? cambiará de forma dinámica por la entidad de organización que es la propietaria del recurso y posteriormente cuando se aplique la política de plantilla durante la ejecución se cambiará por sus antecesores. Los grupos de acceso definidos con el signo ? solamente funcionan con políticas de plantilla.

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 `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 parámetro. Esto funciona

solamente en políticas de plantilla. En este ejemplo, el usuario debe tener el rol de Administrador de ventas, Administrador de cuentas o Vendedor, en la entidad de organización propietaria del recurso especificado en la política de plantilla.

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

registrationStatus: 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, el usuario debe tener los valores 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_inst_wc*/xml/policies/xml/defaultAccessControlPolicies.xml define las políticas de control de acceso por omisión que pueden adquirirse. Sigue la DTD especificada por:
dir_inst_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 id_miembro 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, que se especifica 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 están definidos en el archivo dir_inst_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 recursos que se especifica en la columna GRPNAME de la tabla ACRESGRP. Se utiliza para obtener el ID de grupo de recursos correspondiente (ACRESGRP_ID) que se almacenará 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 template (POLICYTYPE se establece en 1 en la tabla ACPOLICY). Si no se especifica este atributo, el valor de tipo de política no se modificará. Por omisión, el valor de esta columna es nulo. Cualquier valor distinto a 1 implica un tipo de política que no es de plantilla. Para obtener más información sobre los tipos de políticas, consulte el Capítulo 3, "Conceptos de control de acceso" en la página 9.

RelationName (opcional): 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, Relationship Group, 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">
</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">
</Policy>
```

Políticas a nivel de recursos:

Para mandatos: En este ejemplo, los usuarios que pertenecen al grupo de acceso RegisteredApprovedUsers 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="RegisteredApprovedUsersExecuteCouponRedemptionCommandsOn
WalletResource"
OwnerID="RootOrganization"
UserGroup="RegisteredApprovedUsers"
```

```
ActionGroupName="CouponRedemption"
ResourceGroupName="CouponWalletResourceGroup"
RelationName="creator">
</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">
</Policy>
```

Políticas de plantilla: En este ejemplo, los usuarios pertenecientes al grupo de acceso `MembershipAdministratorsForOrg`, pueden realizar las acciones especificadas por el grupo de acciones `ApproveGroupUpdate` en los recursos especificados por `OrganizationDataResourceGroup` .

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

Cuando se aplica esta política de plantilla, el propietario de la política cambiará dinámicamente de la organización raíz, RootOrganization, a la entidad de organización propietaria del recurso y, posteriormente, a las entidades de organización antecesoras, hasta incluir la organización raíz. Al analizar la definición del grupo de acceso `MembershipAdministratorsForOrg` se revelará la condición siguiente para los miembros:

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

Nota: La `simpleCondition` de `role` se califica mediante `org = ?`. Este signo **?** se sustituye dinámicamente junto con el propietario de la política, como se ha explicado anteriormente. Este comportamiento dinámico solamente está disponible en políticas de plantilla. Por lo tanto, en este ejemplo los usuarios que tienen el rol de `Administrador de compradores` o `Administrador de`

vendedores para la entidad de organización propietaria del recurso, satisfacen la condición de ser miembros de este grupo de acceso.

Datos de política que pueden traducirse

A continuación se muestra una plantilla de elementos de control de acceso traducibles que como mínimo deben definirse en el archivo defaultAccessControlPolicies_*entorno_nacional*.xml.

```
<?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>-->
<!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-->
```

```
<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_inst_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="La vistas para cargar botones en la página de ajuste de pedido
cuando se formaliza un pedido desde Commerce Acclerator"
/>
```

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"
OnwerID="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.

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 45.

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.

Nota: Si crea archivos XML personalizados, tendrá que copiarlos en *<dir_inst_wc>*/xml/policies/xml para poder cargarlos en las bases de datos.

En 400 : si crea archivos XML personalizados, deberá utilizar la vía de acceso completa al DTD del archivo. Las DTD de políticas de control de acceso están almacenadas en /QIBM/ProdData/WebCommerce/xml/policies/dtd.

Para cargar los grupos de acceso y las políticas de control de acceso, ejecute los mandatos siguientes:

En NT 2000

1. Desde el directorio *<dir_inst_wc>*\bin, ejecute los archivos de mandatos siguientes según sea necesario, en el orden que se listan:
   - Para cargar las definiciones de grupos de usuarios (acceso), ejecute el archivo de mandatos **acugload**. **Sintaxis**: acugload.cmd *<nombre basedatos> <usuario basedatos> <contraseña usuario basedatos> <archivo xml UserGroups>* **Ejemplo**: acugload mall dbuser dbusrpwd ACUserGroups_es_ES.xml
   - Para cargar el archivo de políticas de control de acceso principal, ejecute el archivo de mandatos **acpload**. **Sintaxis:** acpload.cmd *<nombre basedatos> <usuario basedatos> <contraseña usuario basedatos> <archivo xml políticas>* **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 basedatos> <usuario basedatos> <contraseña usuario basedatos> <archivo xml políticas NLS>* **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_inst_wc>*\logs contienen anotaciones de error.

En AIX Solaris Linux

El ID de usuario de base de datos debe tener autorización para leer, grabar y ejecutar en *<dir_inst_wc>*/xml/policies, *<dir_inst_wc>*/bin y *<dir_inst_wc>*/properties/utilities y también en sus subdirectorios y archivos.

1. Inicie la sesión con el ID de usuario de base de datos.
2. Desde el directorio *<dir_inst>*/bin, ejecute los scripts del shell siguientes según sea necesario 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 basedatos> <usuario basedatos> <contraseña* usuario*basedatos> <nombrearchivo xml UserGroups>* **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 basedatos> <usuario basedatos> <contraseña usuario basedatos> <nombrearchivo xml políticas>* **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 basedatos> <usuario basedatos> <contraseña usuario basedatos> <NLS Nombrearchivo xml Policies>* **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_inst_wc>*`/logs` contienen anotaciones de error.

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.

En 400

En la línea de mandatos, ejecute los mandatos siguientes según sea necesario, en el orden indicado.

- Para cargar las definiciones de grupos de usuarios (acceso), ejecute el mandato `LODWCSUG`. **Sintaxis:** LODWCSUG DATABASE(*<nombre basedatos>*) SCHEMA(*<nombre_esquema>*) PASSWD(*<contraseña_instancia>*) INSTROOT(*<raíz_instancia>*) INFILE(*<vía completa al archivo XML>*)
- Para cargar el archivo de políticas de control de acceso principal, ejecute el mandato `LODWCSAC`. **Sintaxis:** LODWCSAC DATABASE (<nombre basedatos>) SCHEMA (<nombre_esquema>) PASSWD (<contraseña_instancia>) INSTROOT (<raíz_instancia>) INFILE (*<vía completa al archivo XML>*)
- Para cargar los nombres de visualización y el archivo de descripciones, ejecute el mandato `LODWCSACD`. **Sintaxis:** LODWCSACD DATABASE(*<nombre basedatos>*) SCHEMA(*<nombre_esquema>*) PASSWD (*<contraseña_instancia>*) INSTROOT(*<raíz_instancia>*) INFILE(*<vía completa al archivo XML>*)

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.

En NT 2000

1. Desde el directorio *<dir_inst_wc>*`\bin`, ejecute el siguiente mandato `acpextract`:

   ```
   acpextract.cmd <nombre basedatos> <usuario basedatos> <contraseña usuario basedatos>
   ACPoliciesfilter.xml
   ```

   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_LOCALE.xml`: el archivo de políticas de control de acceso que depende del idioma y que contiene los nombres de visualización y las descripciones.

2. Consulte el archivo *<dir_inst_wc>*`\logs\acpextract.log` por si se han producido errores de proceso.

En AIX Solaris Linux

1. Inicie la sesión con el ID de usuario de base de datos.
2. Desde el directorio *<dir_inst_wc>*`\bin`, ejecute el siguiente script del shell `acpextract`:

```
acpextract.sh <nombre basedatos> <usuario basedatos>
<contraseña usuario basedatos> ACPoliciesfilter.xml
```

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. Consulte el archivo *<dir_inst_wc>*`\logs\acpextract.log` por si se han producido errores de proceso.

En 400

1. En la línea de mandatos, ejecute el mandato `EXTWCSAC` siguiente:

```
EXTWCSAC DATABASE (<nombre basedatos>)
 SCHEMA (<nombre_esquema>) PASSWD (<usuario basedatos>)
INSTROOT (<raíz_instancia>) FILTER (<archivo XML de entrada>) OUTDIR
(<directorio de salida para nuevos archivos>)
```

Se crearán los archivos siguientes en el directorio especificado mediante 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_LOCALE.xml`: el archivo de políticas de control de acceso que depende del idioma y que contiene los nombres de visualización y las descripciones.

Apéndice. Políticas de control de acceso por omisión

El Apéndice lista las políticas por omisión que se proporcionan con WebSphere Commerce. 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 6.

Políticas	**Comienza en**
Políticas basadas en roles	"Políticas basadas en roles" en la página 110
Políticas a nivel de recursos por área de negocio:	"Políticas a nivel de recursos por área de negocio" en la página 111
Pedidos	"Pedidos" en la página 111
Intercambio (contratos)	"Intercambio (Contratos)" en la página 112
Aprobaciones	"Aprobaciones" en la página 113
Subastas	"Subastas" en la página 113
Business Intelligence	"Business Intelligence" en la página 113
Miembros	"Miembros" en la página 114
Consola de administración de comprador	"Consola de administración de comprador" en la página 114
Campañas	"Campañas" en la página 115
Catálogo	"Catálogo" en la página 115
Conectividad y notificación	"Conectividad y notificación" en la página 115
Suministros	"Suministros" en la página 116
Cupones	"Cupones" en la página 116
Perfiles de clientes	"Perfiles de clientes" en la página 116
Descuentos	"Descuentos" en la página 117
Inventario	"Gestión de inventario" en la página 117
Inventario planificado	"Inventario planificado" en la página 117
Gestión de inventario	"Gestión de inventario" en la página 118
Gestión de pedidos	"Gestión de pedidos" en la página 118
Pagos	"Pago" en la página 119

Tabla 6. (continuación)

Las páginas de la Consola de administración para editar políticas, grupos de acceso, grupos de recursos y grupos de acciones	"Páginas de la Consola de administración para editar políticas, grupos de acceso, grupos de recursos y grupos de acciones" en la página 119
Asesor de productos	"Asesor de productos" en la página 119
RFQ	"RFQ" en la página 120
Normas	"Normas" en la página 120
Planificador	"Planificador" en la página 120

Políticas basadas en roles

Tabla 7.

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

Tabla 7. (continuación)

ProductManagersExecuteProductManagersCmdResourceGroup
ProductManagersExecuteProductManagersViews
ReceiversExecuteReceiversCmdResourceGroup
ReceiversExecuteReceiversViews
ReturnsAdministratorsExecuteReturnsAdministratorsCmdResourceGroup
ReturnsAdministratorsExecuteReturnsAdministratorsViews
SalesManagersExecuteSalesManagersCmdResourceGroup
SalesManagersExecuteSalesManagersViews
SellerAdministratorsExecuteSellerAdministratorsCommands
SellerAdministratorsExecuteSellerAdministratorsViews
SellersExecuteSellersCmdResourceGroup
SellersExecuteSellersView
SiteAdministratorsCanDoEverything
StoreAdministratorsExecuteStoreAdministratorsCmdResourceGroup
StoreAdministratorsExecuteStoreAdministratorViews

Políticas a nivel de recursos por área de negocio

Pedidos

Tabla 8.

Recursos de datos	
Pedido	AllUsersExecuteOrderCreateCommandsOnStoreResource
	AllUsersExecuteOrderPrepareCommandsOnOrderResource
	AllUsersExecuteOrderProcessOnOrderResource
	AllUsersExecuteOrderReadCommandsOnOrderResource
	AllUsersExecuteOrderWriteCommandsOnOrderResource
	AllUsersExecuteReturnAgainstOrderOnOrderResource
	AllUsersExecuteScheduledOrderCancelOnOrderResource
	OrderManagersForOrgExecuteOrderManageCommandsOnOrderResource
Lista de solicitudes	AllUsersExecuteRequisitionListCreateCommandsOnStoreEntityResource
	AllUsersExecuteRequisitionListExclusiveProcessCommands OnPrivateRequisitionListResource
	AllUsersExecuteRequisitionListExclusiveReadCommandsOn PrivateRequisitionListResource
	AllUsersExecuteRequisitionListSharedProcessCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListSharedReadCommandsOn SharedRequisitionListResource
	AllUsersExecuteRequisitionListWriteCommandsOn RequisitionListResource

Tabla 8. (continuación)

Artículo de interés	AllUsersExecuteInterestItemReadCommandsOnInterestItemListResource
	AllUsersExecuteInterestItemWriteCommandsOnInterestItemListResource
RMA (Autorización de devolución de artículos)	AllUsersExecuteRMACreateCommandsOnStoreResource
	AllUsersExecuteRMAProcessCommandsOnRMAResource
	AllUsersExecuteRMAReadCommandsOnRMAResource
	AllUsersExecuteRMAWriteCommandsOnRMAResource
	RMAApproversForOrgExecuteRMAApproveCommandsOnRMAResource
	RMADisposersForOrgExecuteRMADisposeCommandsOnRMAResource
	RMAManagersForOrgExecuteRMAManageCommandsOnRMAResource
	RMAReceiversForOrgExecuteRMAReceiveCommandsOnRMAResource
	StoreAdministratorsForOrgExecuteRMACreditCommandsOnStoreEntityResource
Beans de datos	
Pedido	AllUsersDisplayApprovalsOrderDataBeansResourceGroup
	AllUsersDisplayOrderDatabeanResourceGroup
Lista de solicitudes	AllUsersDisplaySharedRequisitionListDataBeansIfSame OrganizationalEntityAsCreator
Artículo de interés	AllUsersDisplayInterestItemDatabeanResourceGroup
RMA	AllUsersDisplayRMADatabeanResourceGroup

Intercambio (Contratos)

Tabla 9.

Recurso de datos	
Contrato	ContractAdministratorsForOrgExecuteContractCreateCommandsOn MemberResource
	ContractAdministratorsForOrgExecuteContractManageCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractDeployCommandsOn ContractResource
	ContractOperatorsForOrgExecuteContractSubmitCommandsOn ContractResource
	ContractViewersExecuteContractDisplayCommandsOnContractResource
Política de negocio	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy CreateCommandsOnStoreResoure
	BusinessPolicyAdministratorsForOrgExecuteBusinessPolicy ManageCommandsOnBusinessPolicyResourcee

Tabla 9. (continuación)

Beans de datos	AccountHandlersDisplayTradingDatabeanResourceGroup

Aprobaciones

Tabla 10.

Recursos de datos	
	AllUsersExecuteAllUsersActionGroupCommandsOnOrderResource
	AllUsersExecuteApproveCommandsOnApprovalResource
	AllUsersExecuteCancelApproveCommandsOnApprovalResource

Subastas

Tabla 11.

Recursos de datos	
Subasta	AuctionAdministratorsForOrgExecuteAdminRetractBidCommands OnAuctionResource
	AuctionAdministratorsForOrgExecuteAuctionCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionManageCommands OnAuctionResource
Estilo de subasta	AuctionAdministratorsForOrgExecuteAuctionStyleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteAuctionStyleManageCommands OnAuctionStyleResource
Norma de control de ofertas	AuctionAdministratorsForOrgExecuteBidControlRuleCreateCommands OnStoreEntityResource
	AuctionAdministratorsForOrgExecuteBidControlRuleManageCommands OnBidControlRuleResource
Oferta de compra	RegisteredApprovedUsersExecuteBidCreateCommandsOnAuctionResource
	RegisteredApprovedUsersExecuteBidManageCommands OnBidResourcesTheyOwn
Oferta automática	RegisteredApprovedUsersExecuteAutoBidCreateCommands OnAuctionResource
	RegisteredApprovedUsersExecuteAutoBidManageCommands OnAutoBidResourcesTheyOwn
Beans de datos	AuctionDatabeanOwnersDisplayAuctionDatabeans

Business Intelligence

Tabla 12.

Recursos de datos	
	BusinessAnalystsForOrgExecuteViewContext ListCommandsOnStoreEntityResource

Tabla 12. (continuación)

	IntelligenceReportViewersForOrgExecuteViewBusinessIntelligenceReport CommandsOnStoreEntityResource

Miembros

Tabla 13.

Recursos de datos	
Usuario	GuestsExecuteUserSelfRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteUserAdminRegistration CommandsOnOrganizationResource
	MembershipAdministratorsForOrg ExecuteUserAdminUpdateCommandsOnUserResource
	NonRejectedUsersExecuteUserSelfRegistration ContinuationCommandsOnUserResource
Organización	MembershipAdministratorsForOrgExecute OrgEntityRegistrationCommandsOnOrganizationResource
	MembershipAdministratorsForOrgExecuteOrg EntityUpdateCommandsOnOrganizationResource
Dirección	MembershipAdministratorsForOrg ExecuteAddressManageCommandsOnMemberResource
	NonRejectedUsersExecuteAddressManageCommandsOn UserResource
Rol	MembershipAdministratorsForOrgExecute RoleManageCommandsOnUserResource
	OrganizationRoleAdministratorsExecute RoleManageCommandsOnOrganizationResource
Grupo de miembros	MemberGroupAdministratorsForOrgExecute MemberGroupCreateCommandsOnMemberResource
	MemberGroupManagersForOrgExecute MemberGroupManageCommandsOnMemberGroupResource
Beans de datos	MembershipAdministratorsForOrgDisplay OrganizationDatabeanResourceGroup
	MembershipViewersForOrgDisplayMembershipDatabeanResourceGroup

Consola de administración de comprador

Tabla 14.

Recursos de datos	
Grupos de aprobación	MembershipAdministratorsForOrgExecute ApproveGroupUpdateCommandsOnOrganizationResource
Grupo de miembros	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnMemberGroupResource
	MembershipAdministratorsForOrgExecute MemberGroupMemberUpdateCommandsOnUserResource

Campañas

Tabla 15.

Recursos de datos	
	CampaignManagersForOrgExecute CampaignRelatedCreateCommandsOnStoreEntityResource
	CampaignManagersForOrgExecute CampaignUpdateCommandsOnCampaignResource
	CampaignManagersForOrgExecute CollateralUpdateCommandsOnCollateralResource
	CampaignManagersForOrgExecute EMarketingSpotUpdateCommandsOnEMarketingSpotResource
	CampaignManagersForOrgExecute InitiativeUpdateCommandsOnInitiativeResource
Beans de datos	CampaignManagersForOrgDisplayCampaignDatabeanResourceGroup

Catálogo

Tabla 16.

Recursos de datos	
	CatalogEntryManagersForOrgExecute CatalogEntryManageCommandsOnCatalogEntryResource
	CatalogEntryManagersForOrgExecute CatalogEntryRelationManageCommandsOnCatalogResource
	CatalogEntryManagersForOrgExecute StoreCatalogEntryManageCommandsOnStoreEntityResource
	CatalogGroupManagersForOrgExecute CatalogGroupManageCommandsOnCatalogGroupResource
	CatalogGroupManagersForOrgExecute ProductSetAddCommandsOnCatalogResource
	CatalogGroupManagersForOrgExecute ProductSetManageCommandsOnProductSetResource
	CatalogManagersForOrgExecute CatalogManageCommandsOnCatalogResource
	CatalogManagersForOrgExecute StoreCategoryManageCommandsOnCatalogResource
Beans de datos	CatalogGroupManagersForOrgDisplay CatalogGroupDataBeansResourceGroup
	ProductAdministratorsForOrgDisplayProductDataBeansResourceGroup

Conectividad y notificación

Tabla 17.

Recursos de datos	
	BackendOrderAdministratorsForOrgExecute BackendOrderStatusCreateCommandsOnOrderDataResource

Tabla 17. (continuación)

	BackendPickPackersForOrgExecute BackendPickPackListCommandsOnFulfillmentCenterDataResource
	StoreAdministratorsForOrgExecute MessagingAdminCommandsOnStoreEntityResource
Beans de datos	StoreAdministratorsForOrgDisplayMessagingDataBeans

Suministros

Tabla 18.

Recursos de datos	
	ProcurementAdministratorsForOrgExecute ProcurementAuthenticationAndRegistrationOnOrderDataResource
	ProcurementShoppingCartManagersExecute ProcurementShoppingCartManageOnOrderResource

Cupones

Tabla 19.

Recursos de datos	
	CouponAdministratorsForOrgExecute CouponPromotionCreateCommandsOnStoreEntityResource
	CouponAdministratorsForOrgExecuteCouponPromotionDeleteCommands OnCouponPromotionResource
	RegisteredApprovedUsersExecute CouponDeleteCommandsOnCouponWalletResource
	RegisteredApprovedUsersExecute CouponRedemptionCommandsOnCouponWalletResource
	StoreAdministratorsForOrgExecute ScheduledCouponCmdsOnStoreResource
Beans de datos	CouponAdministratorsForOrgDisplayECouponPromotionListBeans

Perfiles de clientes

Tabla 20.

Recursos de datos	
	CustomerProfileEditorsForOrgExecute SegmentManageCommandsOnStoreEntityResource
Beans de datos	CustomerProfileEditorsForOrgDisplay SegmentationDatabeansResourceGroup

Descuentos

Tabla 21.

Recursos de datos	
	DiscountAdministratorsForOrgExecute DiscountAssociateCommandsOnCalculationCodeResource
	DiscountAdministratorsForOrgExecute DiscountCreateCommandsOnStoreEntityResource
	DiscountAdministratorsForOrgExecute DiscountDeployCommandsOnCalculationCodeResource
Beans de datos	DiscountViewersForOrgDisplayDiscountDatabeans

Gestión de inventario

Tabla 22.

Recursos de datos	
	ExpectedInventoryManagersForOrgExecute InventoryManageCommandsOnStoreEntityResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterCreateCommandsOnOrganizationResource
	FulfillmentCenterManagersForOrgExecute FulfillmentCenterManageCommandsOnFulfillmentResource
	InventoryAdjustersForOrgExecute InventoryAdjustCommandsOnStoreEntityResource
	PickBatchInventoryManagersForOrgExecuteReleaseReadyShipCommands OnFulfillmentCenterResource
	PickPackGeneratorsForOrgExecute PickPackGenerateCommandsOnFulfillmentCenterResource
	ReturnReasonsManagersForOrgExecute ReturnReasonsCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorCreateCommandsOnStoreEntityResource
	VendorInventoryManagersForOrgExecute VendorManageCommandsOnVendorResource
Beans de datos	StoreAdministratorsForOrgDisplay OrderFulfillmentStatusDataBeansResourceGroup

Inventario planificado

Tabla 23.

Recursos de datos	
	StoreAdministratorsForOrgExecute InventoryScheduledCommandsOnStoreEntityResource

Gestión de inventario

Tabla 24.

Beans de datos	
	ExpectedInventoryManagersForOrgDisplay ExpectedInventoryDataBeansResourceGroup
	FulfillmentCenterManagersForOrgDisplay FulfillmentCenterDataBeansResourceGroup
	PickBatchInventoryManagersForOrgDisplay PickBatchInventoryDataBeansResourceGroup
	ProductFindInventoryManagersForOrgDisplay ProductFindInventoryDataBeansResourceGroup
	ReceiverOrderManagersForOrgDisplay ReceiverOrderManagementDataBeansResourceGroup
	ReturnReasonsManagersForOrgDisplay ReturnReasonsOrderManagementDataBeansResourceGroup
	ReturnsAdminOrderManagersForOrgDisplay ReturnsAdminOrderManagementDataBeansResource
	SuperUserOrderManagersForOrgDisplay SuperUserOrderManagementDataBeansResourceGroup
	VendorInventoryManagersForOrgDisplay VendorInventoryDataBeansResourceGroup

Gestión de pedidos

Tabla 25.

Recursos de datos	
	CustomerOrderManagersExecute CustomerServiceCustomerWriteCommandsOnUserResource
	CustomerOrderManagersForDefaultOrgExecute CustomerServiceCustomerWriteCommandsOnUse
	CustomerOrderManagersForOrgExecute CustomerServiceOrderCreateCommandsOnStoreEntityResource
	CustomerOrderManagersForOrgExecute CustomerServiceOrderWriteCommandsOnOrderResource
	CustomerOrderManagersForOrgExecute CustomerServiceReturnCreateCommandsOnStoreEntity
	CustomerOrderManagersForOrgExecute CustomerServiceReturnWriteCommandsOnRMAResource
Beans de datos	CustomerOrderManagersDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForDefaultOrgDisplay CustomerUserManagementDatabeans
	CustomerOrderManagersForOrgDisplay CustomerOrderManagementDatabeans
	LogisticsManagersForOrgDisplay OrdersAndReturnsListsDatabeans
	ReturnsManagersForOrgDisplayReturnsListsDatabean

Tabla 25. (continuación)

	UserOrderManagersDisplayUserDatabeans
	UserOrderManagersForDefaultOrgDisplayUserDatabeans

Pago

Tabla 26.

Recursos de datos	
	AccountAdministratorsForOrgExecute AccountManageCommandsOnAccountResource
	AccountManagersForOrgExecute AccountCreateCommandsOnOrganizationResource
	AccountViewersForOrgExecute PaymentSummaryGenerateCommandsOnAccountResource
	AccountViewersForOrgExecute StorePaymentAdminCommandsOnStoreEntityResource
	AllUsersExecutePaymentOrderWrite CommandsOnOrderResource

Páginas de la Consola de administración para editar políticas, grupos de acceso, grupos de recursos y grupos de acciones

Tabla 27.

Recursos de datos	
	DescendantStoreAdministratorsExecute ACViewPoliciesForOrgActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyCreateCommandsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACPolicyEditCommandsOnACPolicyResource
	StoreAdministratorsForOrgExecute ACViewApplicablePoliciesActionsOnOrganizationResource
	StoreAdministratorsForOrgExecute ACViewPoliciesForUpdateActionsOnOrganizationResource
Beans de datos	StoreAdministratorsForOrgExecute UserGroupSearchViews

Asesor de productos

Tabla 28.

Beans de datos	
	ProductAdvisorStatisticiansForOrgDisplay ProductAdvisorStatisticsDatabeans
	SalesAssistantStatisticiansForOrgDisplay SalesAssistantStatisticsDatabeans

RFQ

Tabla 29.

Recursos de datos	
	RFQAdministratorsAdministerRFQs
	RFQAdministratorsManageRFQResponses
	RFQBuyersEvaluateRFQResponsesForRFQsTheyOwn
	RFQBuyersForOrgExecuteRFQCreate CommandsOnStoreEntityDataResourceGroup
	RFQBuyersManageRFQResourcesTheyOwn
	RFQBuyersManageRFQResponsesForRFQsTheyOwn
	RFQSalesManagersExecuteRFQResponse ManageCommandsOnRFQResponseResource
	RFQSalesManagersForOrgCreateRFQResponse
Beans de datos	RFQBuyersDisplayRFQDataBeanResourceGroupTheyOwn
	RFQBuyersDisplayRFQResponseDataBeans ViewabletoRFQOwnerResourceGroup
	RFQSalesViewersDisplayRFQDataBeanResourceGroup
	RFQSalesViewersDisplayRFQResponseDataBeanResourceGroup

Normas

Tabla 30.

Recursos de datos	
	StoreAdministratorsForOrgExecutePersonalization RuleServiceAdministrationCommandsOnStoreEntityResource
Beans de datos	StoreAdministratorsForOrgDisplay PersonalizationRuleServiceAdministrationDataBeanResource

Planificador

Tabla 31.

Recursos de datos	
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnStoreEntityResource
	StoreAdministratorsForOrgExecute ScheduledJobManageCommandsOnUserResource
Beans de datos	StoreAdministratorsForOrgDisplay SchedulerDataBeansResourceGroup

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los Estados Unidos.

Es posible que IBM no proporcione los productos, servicios o características a los que hace referencia este documento en otros países. 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 implica que sólo pueda utilizarse ese producto, programa o servicio de IBM. En su lugar puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere 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.

IBM puede tener patentes o aplicaciones pendientes de patente que cubran temas tratados en este documento. La posesión 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:

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:

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 dicha norma.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información aquí contenida está sometida a cambios periódicos; tales cambios se irán incorporando 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:

Manager, e-Commerce Product Development IBM
17 Skyline Drive
Hawthorne, NY 10532
EE.UU.

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 esta información, y todo el material bajo licencia disponible para el mismo, bajo los términos del Contrato de cliente IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM o de cualquier acuerdo equivalente entre IBM y el cliente.

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.

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.

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.

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

Los siguientes términos son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países:

DB2 DB2 Universal Database

IBM WebSphere

Lotus, Domino y Go Webserver, son marcas registradas de Lotus Development Corporation en los Estados Unidos y/o en otros países.

Microsoft™, Windows™ y Windows NT™ son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Pentium™ es una marca registrada de Intel Corporation en los Estados Unidos y/o en otros países.

Solaris Operating Environment, JDBC, Java™ y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y otros países.

Blaze Advisor, Blaze Expert, Blaze Presenter, Blaze Accessor, Blaze Enterprise, OOScript y Smartlets son marcas registradas de Blaze Software Inc., en los Estados Unidos y/o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de otras empresas.

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.