IBM WebSphere Commerce

Guía de seguridad

Versión 54

IBM WebSphere Commerce

Guía de seguridad

Versión 54

Nota:
Antes de utilizar esta información y el producto al que da soporte, lea la información general del apartado "Avisos" en la página 117.

Primera edición, primera revisión (mayo de 2002).

Esta edición se aplica a la versión 5.4 de IBM WebSphere Commerce, así como a todos los releases y las modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones. Asegúrese de utilizar la edición correcta para el nivel del producto.

Efectúe el pedido de publicaciones a través del representante de IBM o de la sucursal de IBM que atiende a su localidad. No hay stock de publicaciones 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 indica a continuación. Asegúrese de incluir su dirección de red completa si desea una respuesta.

   `Internet: hojacom@vnet.ibm.com`

2. Por FAX, utilice el número siguiente:

   `(34) 93 321 6134`

3. Por correo postal a la dirección siguiente:

   IBM, S.A.
   National Language Solutions Center
   Av. Diagonal 571. Edif. L'Illa
   08029 Barcelona
   España

Cuando se envía información a IBM, se otorga a IBM un derecho no exclusivo para utilizar o distribuir la información del modo que estime apropiado sin incurrir por ello en ninguna obligación con el remitente.

Contenido

Prefacio

Este documento describe las características de seguridad de WebSphere Commerce 5.4 y el modo de configurar dichas características.

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

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

Observe que muchas secciones de este manual provienen de otros documentos de la biblioteca de información de WebSphere Commerce 5.4 como, por ejemplo, la ayuda en línea de WebSphere Commerce 5.4, y las publicaciones *WebSphere Commerce 5.4, Guía de instalación* y *WebSphere Commerce 5.4, Guía del programador*. Concretamente:

- La información en el Capítulo 3, "Autorización (Control de acceso)" en la página 15 también está documentada en la publicación *WebSphere Commerce 5.4, Guía de control de acceso*.
- La información en el Capítulo 4, "Mejora de la seguridad del sitio" en la página 41 y el Capítulo 6, "Gestión de sesiones" en la página 67 también está documentada en la ayuda en línea de WebSphere Commerce 5.4. La información en el Capítulo 5, "Habilitación de la seguridad de WebSphere Application Server" en la página 57 también está documentada en la publicación *WebSphere Commerce 5.4, Guía de instalación*.
- La información en la Parte 3, "Tareas de seguridad del administrador del sistema" en la página 73 también está documentada en la publicación *WebSphere Commerce 5.4, Guía de instalación*.
- La información en la Parte 4, "Tareas de seguridad del desarrollador de WebSphere Commerce" en la página 91 también está documentada en la publicación *WebSphere Commerce 5.4, Guía del programador*.

Importante

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

Cómo está organizada la información en este documento

Este documento se divide en las partes siguientes:

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

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

- La Parte 2, "Tareas de seguridad del administrador de sitio de WebSphere Commerce" en la página 39, describe las tareas de administración de sitio de WebSphere Commerce que pertenecen a la seguridad del sitio. Esta parte será de interés para cualquier persona que realice tareas de administración de sitio relacionadas con la seguridad del sitio.
- La Parte 3, "Tareas de seguridad del administrador del sistema" en la página 73, describe tareas de administración del sistema WebSphere Commerce relacionadas con la seguridad del sistema. Esta parte será de interés para cualquier persona que realice tareas de administración del sistema y que esté preocupada por la seguridad del sistema.
- La Parte 4, "Tareas de seguridad del desarrollador de WebSphere Commerce" en la página 91, describe el control de acceso de WebSphere Commerce desde el punto de vista de un desarrollador. Esta parte será de interés para cualquier persona que desee conocer los conceptos de control de acceso implementando políticas de control de acceso en el código.

Valoración continua de la seguridad

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

Mejoras de la seguridad en WebSphere Commerce 5.4

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

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

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

Mejoras para el administrador de sitio

A continuación se indican mejoras de seguridad de WebSphere Commerce 5.4 que están generalmente destinadas a un administrador de sitio:

Control de acceso

- **Infraestructura de control de acceso** — Una mejora clave es la implementación de una nueva estructura de control de acceso en WebSphere Commerce 5.4. Esta nueva infraestructura utiliza políticas de control de acceso para determinar si a un determinado usuario se le permite realizar una acción determinada en un recurso determinado. La nueva infraestructura de control de acceso proporciona control de acceso detallado. Funciona conjuntamente con el control de acceso

proporcionado por WebSphere Application Server, pero no lo sustituye. La nueva infraestructura de control de acceso se describe detalladamente en el Capítulo 11, “Control de acceso” en la página 93.

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

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

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

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

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

- **Cross-site scripting** — Rechazan cualquier petición de usuario que contenga atributos o caracteres que se hayan designado como no permitidos, utilizando el nodo de protección contra la vulnerabilidad Cross Site Scripting del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.

Autenticación

- **Almacenamiento de contraseñas** — WebSphere Commerce 5.4 cifra y almacena el resumen unidireccional de contraseñas utilizando el esquema de generación aleatoria SHA-1 de la base de datos de WebSphere Commerce, en lugar de almacenar las propias contraseñas. Esto asegura que nadie pueda descifrar las contraseñas de usuario, incluidos el administrador de sitio o del sistema.
- **Invalidación de contraseñas** — Requiere que los usuarios cambien sus contraseñas cuando se están conectando al sistema por primera vez, utilizando el nodo de Invalidación de contraseña del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.
- **Política de cuentas** — Configure una política de cuentas para el sitio a fin de definir las políticas relacionadas con las cuentas que se están usando, empleando la página Política de cuentas de la Consola de administración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.
- **Política de contraseñas** — Configure una política de contraseñas para el sitio a fin de controlar las características de selección de contraseña del usuario utilizando la página Política de contraseñas de la Consola de

administración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.

- **Política de bloqueo de cuentas** — Configure una política de bloqueo de cuentas para el sitio a fin de reducir las posibilidades de que se comprometa una cuenta de usuario utilizando la página de Política de bloqueo de cuentas de la Consola de administración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.

Autorización

Mandatos protegidos por contraseña — Requieren que los usuarios entren sus contraseñas si están ejecutando peticiones que ejecutan mandatos que se han designado utilizando el nodo de Mandatos protegidos por contraseña del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.

Datos cifrados

Herramienta de actualización de base de datos — Actualiza los datos cifrados tales como contraseñas e información de tarjeta de crédito así como la clave de comerciante en una base de datos de WebSphere Commerce, utilizando el nodo de Herramienta de actualización de base de datos del Gestor de configuración de WebSphere Commerce. Esto se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.

Gestión de sesiones

Tiempo de espera de conexión — Desconecta a un usuario que está inactivo durante un extenso periodo de tiempo y solicita que se vuelva a conectar al sistema, utilizando el nodo de Tiempo de espera de conexión. Esta mejora se invoca mediante el Gestor de configuración de WebSphere Commerce y se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.

Anotación cronológica

Registro de accesos — Identifica rápidamente cualquier amenaza para la seguridad de WebSphere Commerce habilitando el registro de accesos. Esta mejora se invoca mediante el Gestor de configuración de WebSphere Commerce y se describe detalladamente en el Capítulo 4, “Mejora de la seguridad del sitio” en la página 41.

Mejoras para el administrador del sistema

A continuación se indican mejoras de seguridad de WebSphere Commerce 5.4 que están generalmente destinadas a un administrador de sitio:

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

Mejoras para el programador de WebSphere Commerce

Una mejora clave es la implementación de una nueva infraestructura de control de acceso en WebSphere Commerce 5.4. Esta nueva infraestructura utiliza políticas de control de acceso para determinar si a un determinado usuario se le permite realizar una acción determinada en un recurso determinado. La nueva infraestructura de control de acceso proporciona control de acceso detallado. Funciona conjuntamente con el control de acceso proporcionado por WebSphere Application Server, pero no lo sustituye. La nueva infraestructura de control de acceso se describe detalladamente en el Capítulo 11, “Control de acceso” en la página 93.

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

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

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

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

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

Mejoras de seguridad en WebSphere Commerce Suite 5.1 Pro Edition

Mientras que Commerce Suite 5.1 representaba una nueva arquitectura de e-commerce y era una reescritura completa de Commerce Suite 4.1 basado en C++, contenía al mismo tiempo todas las características de seguridad de las versiones anteriores de WebSphere Commerce Suite y añadía mejoras de seguridad nuevas. WebSphere Commerce 5.4 ha heredado dichas mejoras.

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

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

Mejoras generales en la seguridad

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

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

Gestión de sesiones

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

Autenticación

Las contraseñas de sistema y de aplicación necesarias para el servidor WebSphere Commerce Suite durante la ejecución se han cifrado de forma segura, utilizando una clave de 12 bits especificada por el comerciante, y se almacenan en los archivos de configuración de WebSphere Commerce Suite. La información confidencial que aparece en el recuadro de entrada de URL de los usuarios está cifrada para proteger a los compradores frente a la divulgación no autorizada de dicha información.

Anotación cronológica

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

Convenios utilizados en este manual

Este manual utiliza los convenios de resaltado siguientes:

- Los caracteres en **negrita** indican mandatos o controles de interfaz gráfica de usuario (GUI), por ejemplo nombres de campos, iconos o elecciones de menú.
- Los caracteres en `monoespaciado` indican ejemplos de texto que se deben escribir exactamente como se muestran, nombres de archivos y nombres y vías de acceso de directorios.
- Los caracteres en *cursiva* se utilizan para dar énfasis a las palabras. La cursiva también indica nombres que se deben sustituir por los valores apropiados para el sistema. Cuando vea alguno de los nombres siguientes, sustitúyalo por el valor del sistema tal como se describe:

nombre_sistpral
Nombre de sistema principal totalmente calificado de la máquina de WebSphere Commerce Studio (por ejemplo, `ibm.com` está totalmente calificado).

Windows

unidad Letra que representa la unidad en la que ha instalado el producto o el componente que se está describiendo (por ejemplo `C:`).

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

Windows indica información específica de WebSphere Commerce para Windows NT y Windows 2000.

AIX indica información específica de WebSphere Commerce para AIX.

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

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

Linux indica información específica de WebSphere Commerce para Linux.

Professional indica información específica de WebSphere Commerce Professional Edition.

Business indica información específica de WebSphere Commerce Business Edition.

Dónde encontrar más información

Para obtener información sobre WebSphere Commerce 5.4, consulte el sitio Web siguiente:

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

Para obtener información relacionada con Commerce Studio, Professional Developer Edition 5.1 o con releases anteriores de WebSphere Commerce Studio, consulte el sitio Web siguiente:

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

Parte 1. Modelo de seguridad de WebSphere Commerce

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

Capítulo 1. Introducción al modelo de seguridad de WebSphere Commerce

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

Visión general

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

¿Qué es la autenticación?

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

El sistema WebSphere Commerce tiene sus propias contraseñas para la administración. Estas contraseñas deben cambiarse periódicamente como parte de una política de seguridad de todo el sitio de WebSphere Commerce. Para conocer los detalles de cómo cambiar las contraseñas del sistema WebSphere Commerce 5.4, consulte el Capítulo 7, “Establecimiento y cambio de contraseñas” en la página 75.

¿Qué es la autorización?

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

- Para proteger los Enterprise JavaBeans (beans EJB) de WebSphere Commerce frente al acceso no autorizado. Este proceso se describe en el Capítulo 5, “Habilitación de la seguridad de WebSphere Application Server” en la página 57.
- Para asegurar que sólo las partes autorizadas puedan ejecutar grupos diferentes de mandatos de WebSphere Commerce. Este proceso se describe en el Capítulo 11, “Control de acceso” en la página 93.

¿Qué son las políticas de control de acceso?

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

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

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

El modelo de control de acceso para WebSphere Commerce 5.4 se basa en la imposición de políticas de control de acceso. Las políticas de control de acceso las impone el Gestor de políticas de control de acceso. En general, cuando un usuario intenta acceder a un recurso protegido, el gestor de políticas de control de acceso determina primero qué políticas de control de acceso son aplicables para dicho usuario y, a continuación, basándose en las políticas de control de acceso aplicables, determina si se permite al usuario realizar la operación solicitada en el recurso en concreto.

¿Qué es un seguimiento de comprobación?

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

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

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

¿Qué es la confidencialidad?

La confidencialidad es el proceso mediante el cual se evita que la información delicada sea descifrada por personas a las que no está destinada dicha información. En el sistema WebSphere Commerce, es necesaria la confidencialidad cuando fluye información confidencial del navegador del usuario al servidor

WebSphere Commerce así como del servidor WebSphere Commerce al navegador del usuario. Tal como se describe en el Capítulo 8, “Habilitación de SSL para producción con IBM HTTP Server” en la página 81, la utilización de SSL (Secure Sockets Layer) proporciona confidencialidad para este escenario.

La confidencialidad es también un requisito importante en el área del gestión de sesiones. Puesto que el protocolo HTTP (Hypertext Transfer Protocol) no tiene estado, se utiliza normalmente un *cookie* para identificar de forma continua el usuario en el servidor WebSphere Commerce. Si se roba este cookie, la cuenta de usuario puede verse comprometida. Esto se conoce normalmente como *robo de sesión*. WebSphere Commerce evita el robo de sesiones utilizando las características exclusivas de las especificaciones de cookie que se describen en el Capítulo 6, “Gestión de sesiones” en la página 67.

Capítulo 2. Autenticación

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

Modelo de autenticación de WebSphere Commerce

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

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

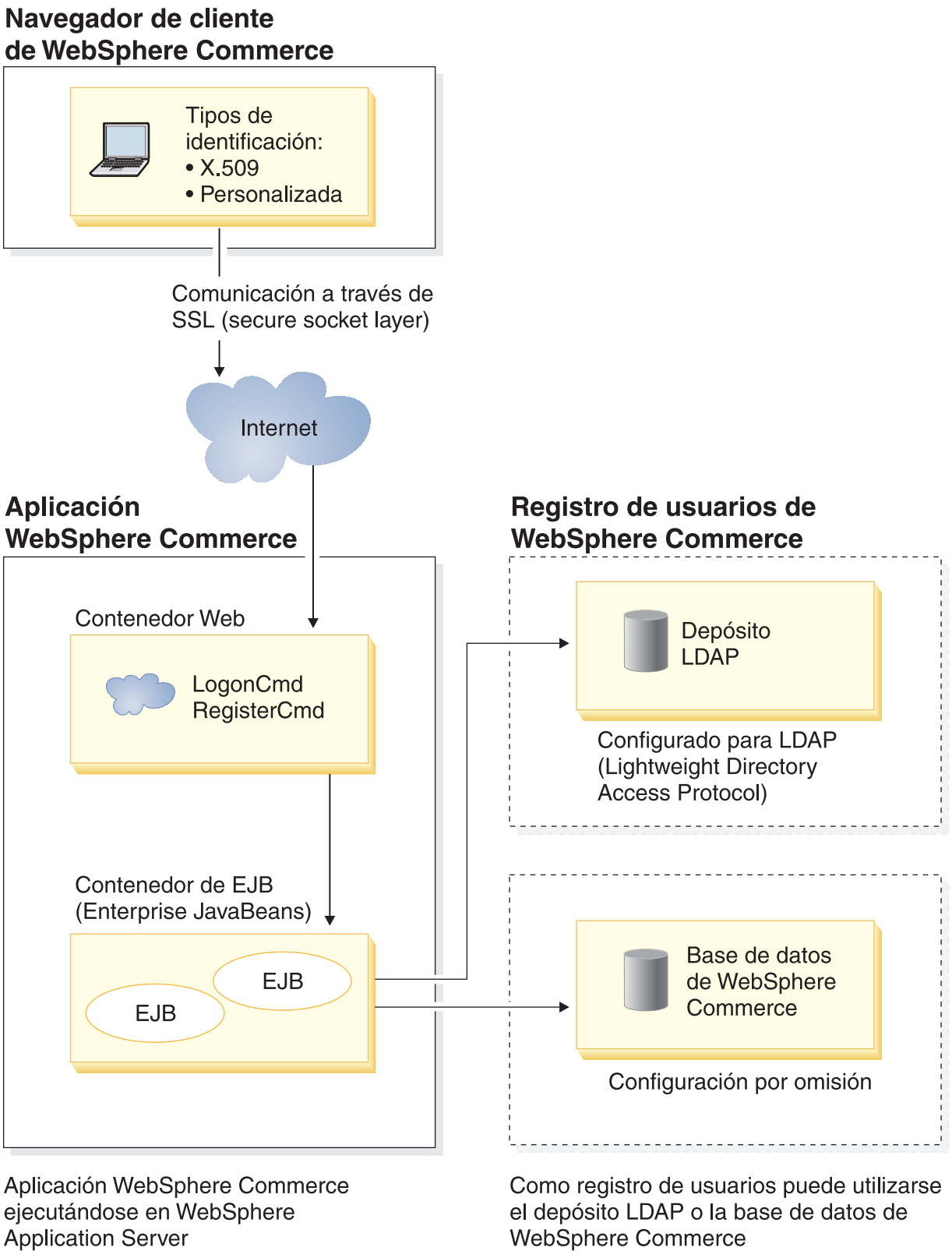


Figura 1. Modelo de seguridad de WebSphere Commerce 5.4

Mecanismos de identificación

Un mecanismo de identificación especifica cómo un servidor identifica y recupera datos de autenticación de un usuario. WebSphere Commerce 5.4 da soporte a los métodos de autenticación o mecanismos de identificación siguientes:

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

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

Mecanismos de autenticación

Un *mecanismo de autenticación* autentica a un usuario verificando sus datos de autenticación con un registro de usuarios asociado. WebSphere Commerce 5.4 emite una señal de autenticación que se asocia a un usuario en cada petición posterior, después del proceso de autenticación. Finaliza cuando el usuario se desconecta o cierra el navegador.

Validación de certificado

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

Enlace LDAP

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

Enlace de base de datos

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

Registro de usuarios

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

WebSphere Commerce 5.4 soporta los registros de usuarios basados en dos dominios de usuarios: registro de usuarios de LDAP y la base de datos de WebSphere Commerce.

WebSphere Commerce 5.4 soporta los siguientes proveedores LDAP:

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

- Windows 2000 Active Directory 2000

Credenciales

El servidor WebSphere Commerce 5.4 soporta mecanismos de autenticación basados en la validación de credenciales, por ejemplo certificados, señales o parejas de ID de usuario y contraseña. Las credenciales se verifican en un registro de usuarios que soporte un esquema de este tipo.

Señal de WebSphere Commerce

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

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

Señal LTPA de WebSphere Application Server

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

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

ID de conexión único

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

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

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

Si desea conocer los pasos a realizar para implementar el ID de conexión único con WebSphere Commerce, consulte el Capítulo 10, “ID de conexión único” en la página 89.

Políticas de autenticación

Una política de autenticación es un conjunto de normas que WebSphere Commerce aplica al proceso de autenticación y a la verificación de los datos de autenticación. WebSphere Commerce 5.4 soporta políticas de cuentas, otras políticas relacionadas con la autenticación y políticas de sesión, tal como se describe en las secciones siguientes.

Políticas de cuentas

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

Política de cuentas

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

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

Para obtener información sobre cómo crear políticas de cuentas, consulte el apartado “Configuración de la política de cuentas” en la página 51.

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

Política de bloqueo de cuentas

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

La política de bloqueo de cuentas impone los elementos siguientes:

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

Para obtener información sobre cómo crear políticas de bloqueo de cuentas, consulte el apartado “Configuración de una política de bloqueo de cuentas” en la página 53.

Política de contraseñas

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

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

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

Para obtener información sobre cómo crear políticas de contraseñas, consulte el apartado "Configuración de una política de contraseñas" en la página 52.

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

Otras políticas relacionadas con la autenticación

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

Invalidación de contraseña

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

Para obtener información sobre cómo utilizar el nodo de Invalidación de contraseña, consulte el apartado "Activación de la invalidación de contraseña" en la página 45.

Mandatos protegidos por contraseña

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

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

Nota: WebSphere Commerce sólo visualizará en la lista de mandatos disponibles los mandatos que están designados como `autenticados` o establecidos con el distintivo `https` en la tabla `URLREG`.

Para obtener información sobre cómo utilizar el nodo de Mandatos protegidos por contraseña, consulte el apartado “Habilitación de mandatos protegidos por contraseña” en la página 46.

Políticas de sesión

En WebSphere Commerce 5.4, las políticas de sesión se incluyen en la política de tiempo de espera de conexión.

Con la política de tiempo de espera de conexión, WebSphere Commerce desconectará a un usuario que esté inactivo durante un extenso periodo de tiempo y le solicitará que vuelva a conectarse al sistema utilizando el nodo de Tiempo de espera de conexión. Esta mejora se invoca mediante el Gestor de configuración de WebSphere Commerce y se describe detalladamente en el apartado “Habilitación del tiempo de espera de conexión” en la página 45.

Capítulo 3. Autorización (Control de acceso)

En WebSphere Commerce la autorización 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.

La autorización o 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 de organizaciones

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.

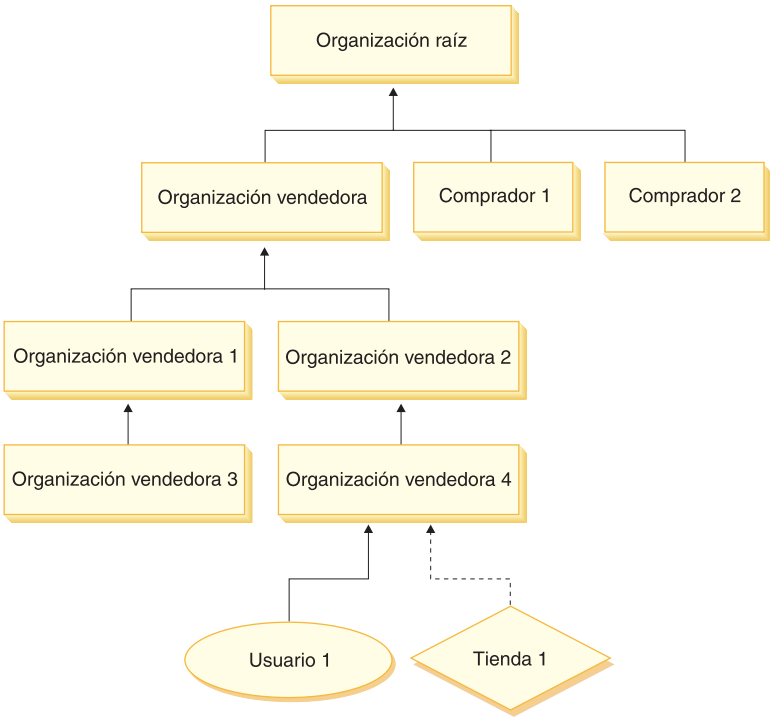


Figura 2. Jerarquía organizativa de un sitio de empresa a empresa

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 18.

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). Generalmente, el Administrador de tienda posee grandes conocimientos de la Web y de los procedimientos comerciales 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 Commerce 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 Commerce 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.

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.

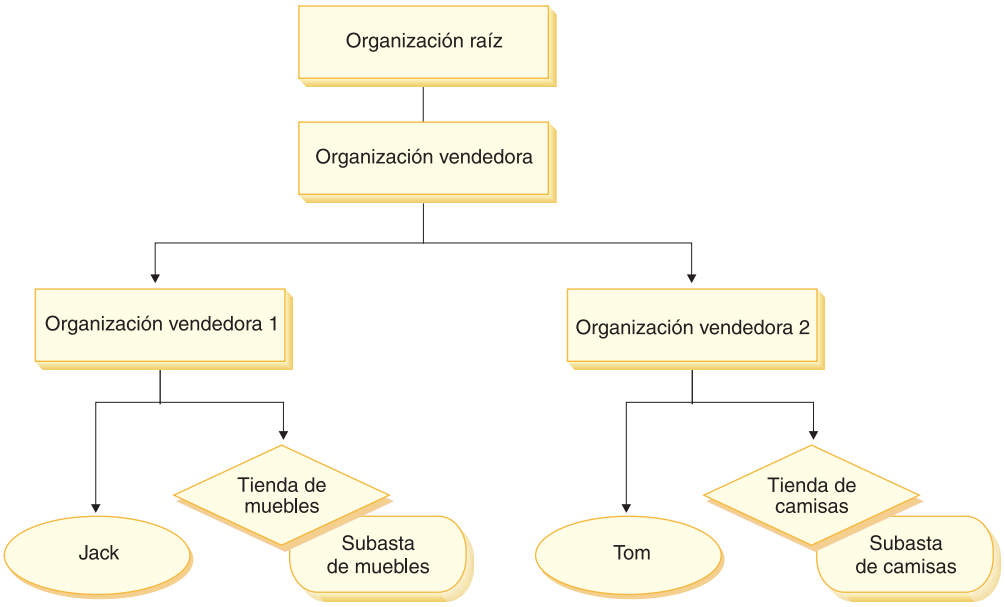
Alteración temporal de las políticas de plantillas: Otra característica de las políticas de plantilla es que se pueden alterar temporalmente para las entidades de organización especificadas. Utilizando el ejemplo anterior, si se añade una onceava organización al sitio de WebSphere, pero esta entidad 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 de 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 30, 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.

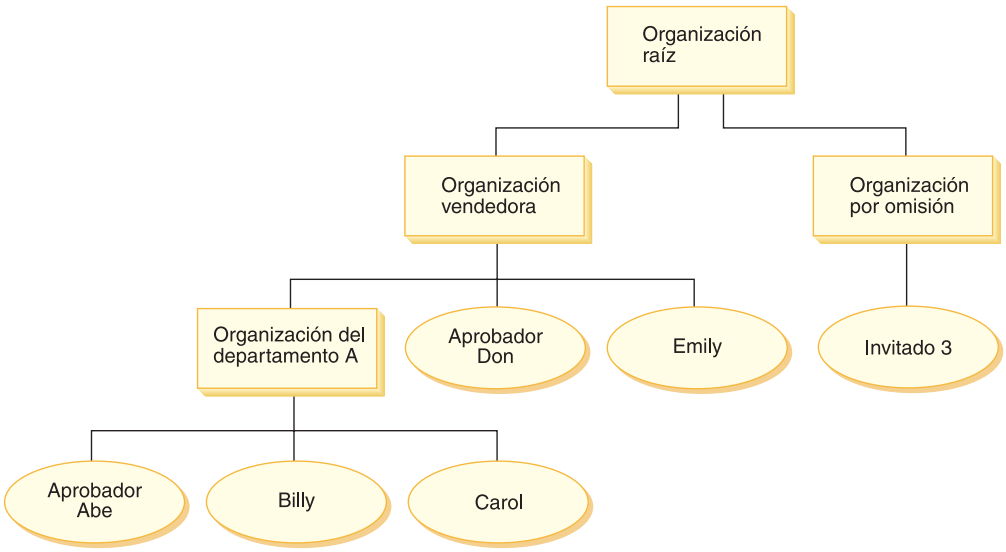
Utilización del control de acceso

Para obtener más información acerca de tareas tales como personalizar las políticas de control de acceso por omisión, personalizar los escenarios y utilizar archivos XML para personalizar las políticas de control de acceso consulte la Guía de control de acceso de WebSphere Commerce.

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 28.

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 34.

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.

Parte 2. Tareas de seguridad del administrador de sitio de WebSphere Commerce

Esta parte describe las tareas de seguridad que normalmente puede realizar el administrador de sitio de WebSphere Commerce.

Capítulo 4. Mejora de la seguridad del sitio

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

- Desconectar un usuario que está inactivo durante un extenso periodo de tiempo y solicitar que vuelva a conectarse al sistema, utilizando el nodo de tiempo de espera de conexión. Para obtener detalles, consulte el apartado "Habilitación del tiempo de espera de conexión" en la página 45.
- Exigir a los usuarios que cambien sus contraseñas cuando se están conectando al sistema por primera vez, utilizando el nodo de Invalidación de contraseña. Para obtener detalles, consulte el apartado "Activación de la invalidación de contraseña" en la página 45.
- Exigir a los usuarios que entren sus contraseñas si están ejecutando peticiones que ejecutan mandatos designados, utilizando el nodo de Mandatos protegidos por contraseña. Para obtener detalles, consulte el apartado "Habilitación de mandatos protegidos por contraseña" en la página 46.
- Actualizar datos cifrados tales como contraseñas e información de tarjeta de crédito así como la clave de comerciante en una base de datos de WebSphere Commerce, utilizando el nodo de Herramienta de actualización de base de datos. Para obtener detalles, consulte el apartado "Actualización de datos cifrados" en la página 47.
- Rechazar cualquier petición de usuario que contenga atributos o caracteres que están designados como no permitidos, utilizando el nodo de protección contra la vulnerabilidad Cross Site Scripting. Para obtener detalles, consulte el apartado "Habilitación de la protección contra la vulnerabilidad Cross Site Scripting" en la página 48.
- Identificar de forma rápida cualquier amenaza para la seguridad de WebSphere Commerce habilitando el registro de accesos. Para obtener detalles, consulte el apartado "Habilitación del registro de accesos" en la página 50.

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

- Configurar una política de cuentas para el sitio a fin de definir las políticas relacionadas con las cuentas que se están usando, utilizando la página Política de cuentas. Para obtener detalles, consulte el apartado "Configuración de la política de cuentas" en la página 51.
- Configurar una política de contraseñas para el sitio a fin de controlar las características de selección de contraseña del usuario utilizando la página Política de contraseñas (sólo si los usuarios están autenticados en la base de datos de WebSphere Commerce). Para obtener detalles, consulte el apartado "Configuración de una política de contraseñas" en la página 52.
- Configurar una política de bloqueo de cuentas para el sitio a fin de reducir las posibilidades de que se ponga en peligro una cuenta de usuario, utilizando la página Política de bloqueo de cuentas (sólo si los usuarios están autenticados en la base de datos de WebSphere Commerce). Para obtener detalles, consulte el apartado "Configuración de una política de bloqueo de cuentas" en la página 53.
- Iniciar un programa de seguridad que comprueba y suprime archivos de WebSphere Commerce temporales que pueden contener riesgos potenciales para

la seguridad utilizando la página Iniciar comprobación de seguridad . Para obtener detalles, consulte el apartado “Inicio de una comprobación de seguridad” en la página 54.

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

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

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

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

Vistas para la seguridad

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

- Tiempo de espera de conexión (consulte el apartado “Tiempo de espera de conexión”)
- Invalidación de contraseña (consulte el apartado “Invalidación de contraseña” en la página 43)
- Mandatos protegidos por contraseña (consulte el apartado “Mandatos protegidos por contraseña” en la página 44)
- Protección contra la vulnerabilidad Cross Site Scripting (consulte el apartado “Protección contra la vulnerabilidad Cross Site Scripting” en la página 44)

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

Tiempo de espera de conexión

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

LoginTimeoutErrorView

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

Tabla 1. Atributos de LoginTimeoutErrorView

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

ReLogonFormView

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

No hay atributos para ReLogonFormView.

Tabla 2. Atributos del formulario de ReLogonFormView

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

Invalidación de contraseña

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

ChangePassword

Esta vista se visualiza si ha caducado la contraseña de un usuario. Debe proporcionar al usuario un formulario para entrar la contraseña actual (caducada) y una contraseña nueva. El botón Someter invoca el mandato ResetPassword. También tiene que haber un botón Cancelar que redirija al usuario a otra página, en la mayoría de los casos, la página de escaparate de la tienda.

Tabla 3. Atributos de ChangePassword

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

Tabla 4. Atributos del formulario de ChangePassword

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

Mandatos protegidos por contraseña

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

PasswordReEnterErrorView

Esta vista se utiliza en los escenarios siguientes:

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

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

Tabla 5. Atributos de PasswordReEnterErrorView

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

PasswordReEnterFormView

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

Tabla 6. Atributos de PasswordReEnterFormView

ECConstants.EC_PASSWORD_REREQUEST_URL	El URL se ejecuta utilizando el botón Someter del formulario.	
ECConstants.EC_PASSWORD_REREQUEST_MSGCODE	Código de mensaje que especifica el mensaje que se muestra al usuario:	
	1	Las contraseñas que se han entrado no coinciden.
	2	No se ha entrado ninguna contraseña.
	3	Se ha entrado una contraseña incorrecta.

ACCIÓN: El URL se pasa como un parámetro denominado:

Tabla 7. Atributos del formulario de PasswordReEnterFormView

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

Protección contra la vulnerabilidad Cross Site Scripting

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

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

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

ProhibCharEncodingErrorView
Es igual que la vista anterior ProhibitedCharacterErrorView.

Habilitación del tiempo de espera de conexión

Nota: Para utilizar la característica de seguridad Tiempo de espera de conexión para una tienda, necesita definir las vistas LoginTimeoutErrorView y ReLogonFormView para la tienda tal como se describe en el apartado "Tiempo de espera de conexión" en la página 42.

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

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

Para habilitar esta característica:

1. Inicie el Gestor de configuración y vaya al nodo de Tiempo de espera de conexión para la instancia del modo siguiente: **WebSphere Commerce >** *nombre_sistpral* **> Lista de instancias >** *nombre_instancia* **> Propiedades de instancia> Tiempo de espera de conexión**
2. Para activar la característica Tiempo de espera de conexión, pulse el recuadro de selección **Habilitar**.
3. Entre el valor de tiempo de espera de conexión, en segundos, en el campo Valor.
4. Para aplicar los cambios en el Gestor de configuración, pulse **Aplicar**.
5. Después de actualizar satisfactoriamente la configuración para la instancia, recibirá un mensaje indicando una actualización satisfactoria.
6. En la Consola de administración de WebSphere Application Server, detenga y, a continuación, reinicie la instancia de WebSphere Commerce Server.

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

Activación de la invalidación de contraseña

Nota: Para utilizar la característica de seguridad Invalidación de contraseña, necesita definir la vista ChangePassword para la tienda tal como se describe en el apartado "Invalidación de contraseña" en la página 43.

Utilice el nodo de Invalidación de contraseña del Gestor de configuración para habilitar o inhabilitar la característica Invalidación de contraseña. Esta característica, cuando está habilitada, requiere que los usuarios de WebSphere Commerce cambien su contraseña si la contraseña del usuario ha caducado. En este caso, se redirige al usuario a una página en la que se le pide que cambie su

contraseña. Los usuarios no podrán acceder a ninguna página segura del sitio hasta que hayan cambiado la contraseña. Para habilitar esta característica:

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

Habilitación de mandatos protegidos por contraseña

Nota: Para utilizar la característica de seguridad Mandatos protegidos por contraseña, necesita definir las vistas PasswordReEnterErrorView y PasswordReEnterFormView para la tienda tal como se describe en el apartado "Mandatos protegidos por contraseña" en la página 44.

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

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

Para habilitar esta característica:

1. Inicie el Gestor de configuración y vaya al nodo Mandatos protegidos por contraseña para la instancia, del modo siguiente: **WebSphere Commerce >** *nombre_sistpral* **> Lista de instancias >** *nombre_instancia* **> Propiedades de instancia > Mandatos protegidos por contraseña**
2. En la pestaña General:
   a. Para habilitar la característica Mandatos protegidos por contraseña, pulse **Habilitar**.
   b. Entre el número de reintentos en el campo Reintentos. (El número de reintentos por omisión es 3.)
3. En la pestaña Avanzada:
   a. Seleccione en la ventana Lista de mandatos protegidos por contraseña un mandato de WebSphere Commerce que desee proteger y pulse **Añadir**. El mandato que ha seleccionado se listará en la ventana de lista de Mandatos protegidos por contraseña actuales.

b. Si desea inhabilitar la protección por contraseña para cualquier mandato de WebSphere Commerce, seleccione el mandato en la ventana de lista de Mandatos protegidos por contraseña actuales y pulse **Eliminar**.

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

Nota: WebSphere Commerce sólo visualizará en la lista de mandatos disponibles los mandatos que están designados como `autenticados` o establecidos con el distintivo `https` en la tabla `URLREG`.

Actualización de datos cifrados

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

1. Inicie el Gestor de configuración y vaya a la entrada de base de datos específica, del modo siguiente: **WebSphere Commerce >** *nombre_sistpral* **> Lista de instancias >** *nombre_instancia* **> Propiedades de instancia > Base de datos >** *nombre_basedatos*
2. Pulse el botón derecho del ratón en *nombre_basedatos* y seleccione **Ejecutar herramienta de actualización de base de datos**
   - Seleccione **Actualizar todas las bases de datos para esta instancia** para migrar los datos cifrados de todas las bases de datos de la instancia seleccionada.

     400 Puesto que iSeries da soporte a la configuración con una sola base de datos, esta opción no se aplica a iSeries.
   - Seleccione **Actualizar la base de datos seleccionada** para migrar los datos cifrados de una base de datos específica seleccionando la base de datos en la lista desplegable (por omisión).
3. Seleccione una acción que desee ejecutar en el recuadro Acciones y rellene la información necesaria en el campo Parámetros:

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

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

Habilitación de la protección contra la vulnerabilidad Cross Site Scripting

Nota: Para utilizar la característica de seguridad de protección contra la vulnerabilidad Cross Site Scripting para una tienda, debe definir las vistas `ProhibitedAttrsErrorView`, `ProhibitedCharacterErrorView` y `ProhibCharEncodingErrorView` para la tienda, tal como se describe en el apartado "Protección contra la vulnerabilidad Cross Site Scripting" en la página 44.

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

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

Para habilitar esta característica:

1. Inicie el Gestor de configuración y vaya al nodo Protección contra la vulnerabilidad Cross Site Scripting para la instancia, del modo siguiente: **WebSphere Commerce >** *nombre_sistpral* **> Lista instancias >** *nombre_instancia* **> Propiedades de instancia > Protección contra la vulnerabilidad Cross Site Scripting**
2. Utilice la pestaña General para activar la característica Protección contra la vulnerabilidad Cross Site Scripting del modo siguiente:
   a. Pulse **Habilitar**.
   b. Para añadir atributos que desea prohibir para los mandatos de WebSphere Commerce, pulse el botón derecho del ratón en la tabla Atributos prohibidos y seleccione **Añadir fila**. Escriba el atributo que desea prohibir. Sólo puede especificar un atributo por fila.

c. Para eliminar atributos de la tabla Atributos prohibidos, resalte en la tabla la línea que contiene el atributo, pulse el botón derecho del ratón en dicha línea y seleccione **Suprimir fila**.
d. Para añadir series que desea prohibir para los mandatos de WebSphere Commerce, pulse el botón derecho del ratón en la tabla Caracteres prohibidos y seleccione **Añadir fila**. Añada la serie que desea prohibir. Sólo puede especificar una serie por fila.
e. Para eliminar caracteres de la tabla Caracteres prohibidos, resalte en la tabla Caracteres prohibidos la línea que contiene el carácter, pulse el botón derecho del ratón en dicha línea y seleccione **Suprimir fila**.

Nota: Las series siguientes están especificadas por omisión en los campos de caracteres prohibidos. Estas series se utilizan muy comúnmente como códigos de script en los ataques Cross Site Scripting.

- `<SCRIPT`
- `&lt;SCRIPT`
- `<%` y `&lt;%`

.

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

   También puede eliminar atributos específicos de un mandato seleccionando el atributo y pulsando **Eliminar**.
4. Para aplicar los cambios en el Gestor de configuración, pulse **Aplicar**.
5. Después de actualizar satisfactoriamente la configuración para la instancia, recibirá un mensaje indicando una actualización satisfactoria.
6. En la Consola de administración de WebSphere Application Server, detenga y, a continuación, reinicie la instancia de WebSphere Commerce Server.

Notas:

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

ejemplo, la serie <%gg hará que falle la conversión porque HEX 'gg' no es una representación de valor hexadecimal válida. En este caso, la serie <%gg producirá una excepción, haciendo que no haya ninguna respuesta a la petición de URL que contiene dicha serie, tanto si la protección contra la vulnerabilidad Cross Site Scripting está habilitada como si no lo está.

Ejemplo: Examine los ejemplos siguientes:

- Series prohibidas: <SCRIPT, <%

  Atributos prohibidos: mycomment, description

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

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

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

Habilitación del registro de accesos

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

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

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

Para habilitar el registro de accesos, realice lo siguiente:

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

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

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

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

   donde:

   - *aa* es un valor entero que especifica el número máximo de entradas que se anotarán en la memoria antes de que se graben las entradas en la base de datos. Generalmente cuanto mayor sea el número, mejor será el rendimiento en lo que respecta al registro de accesos. El valor por omisión es 32.
   - *bbbbb* es `true` o `false`. El valor `true` significa que se anotan cronológicamente todas las peticiones de entrada. El valor `false` significa que sólo se anotan cronológicamente las violaciones de acceso. Para evitar un registro excesivo o innecesario, se recomienda el valor `false`. Utilice `true` sólo cuando sospeche que existen problemas de autenticación o se produce una violación de la seguridad en el sitio. El valor por omisión es `false`.
3. Cuando haya realizado las actualizaciones, guarde el archivo *instancia*.xml para la instancia de WebSphere Commerce.
4. Reinicie WebSphere Application Server.

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

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

Configuración de la política de cuentas

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

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

- Puede suprimir una política de cuentas existente seleccionando la política en la lista y pulsando **Suprimir**.

Para crear una política de cuentas nueva:

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

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

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

Configuración de una política de contraseñas

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

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

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

Para crear una política de contraseñas nueva:

1. Abra la Consola de administración.

2. En el menú desplegable Seguridad de la Consola de administración, pulse **Política de contraseñas**.
3. En la página Política de contraseñas, pulse **Nueva** para crear una nueva política de contraseñas.
4. Entre un nombre para la política de contraseñas en el campo Nombre (por ejemplo `mi_política_contraseñas`)
5. Actualice lo siguiente según sea necesario para modificar cualquiera de los valores respecto al valor por omisión para los compradores:
   - **¿Pueden coincidir el ID de usuario y la contraseña?** Define si el ID de usuario y la contraseña pueden ser idénticos o no. Seleccione `Sí` o `No` en la lista.
   - **Número máximo de tipos de caracteres consecutivos**. Define el número máximo de apariciones de caracteres consecutivos en una contraseña. El valor mínimo es 2 caracteres consecutivos. Por ejemplo, con un valor de 2, un usuario no puede entrar una contraseña como `aaabc`.
   - **Número máximo de apariciones de cualquier carácter**. Define el número máximo de veces que el mismo carácter puede aparecer en una contraseña. El valor mínimo es 1 instancia de un carácter. Por ejemplo, con un valor de 2, un usuario no puede entrar una contraseña como `abcaabc`.
   - **Duración máxima de la contraseña.** Define el periodo máximo de tiempo, en días, durante el cual puede existir una contraseña. El valor mínimo es 1 día. Una vez transcurrido este periodo de tiempo, se solicita al usuario que cambie la contraseña.
   - **Número mínimo de caracteres alfabéticos**. Define el número mínimo de caracteres alfabéticos que se necesitan en una contraseña. El valor mínimo es 0 caracteres alfabéticos.
   - **Número mínimo de caracteres numéricos**. Define el número mínimo de caracteres numéricos que se necesitan en una contraseña. El valor mínimo es 0 caracteres numéricos.
   - **Longitud mínima de la contraseña**. Define la longitud más pequeña de una contraseña, en caracteres. El valor mínimo es 1 carácter.
   - **¿Se puede volver a utilizar la contraseña?** Define si la contraseña anterior de un usuario se puede volver a utilizar. Seleccione `sí` o `no` en la lista.
6. Pulse **Aceptar**.

Notas:

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

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

Configuración de una política de bloqueo de cuentas

La página Política de bloqueo de cuentas de la Consola de administración de WebSphere Commerce le permite configurar una política de bloqueo de cuentas para diferentes roles de usuario en WebSphere Commerce. Esta página lista todas las políticas de bloqueo de cuentas existentes, incluidas las políticas predefinidas que proporciona WebSphere Commerce por omisión. Si se inician acciones

malintencionadas contra una cuenta de usuario, la política de bloqueo de cuentas inhabilita dicha cuenta a fin de reducir las posibilidades de que las acciones la pongan en peligro.

Una política de bloqueo de cuentas impone los elementos siguientes:

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

Para establecer la política de bloqueo de cuentas:

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

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

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

Notas:

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

Inicio de una comprobación de seguridad

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

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

Para invocar el programa de comprobación de seguridad:

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

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

NT *unidad*:\WebSphere\Commerce\instances*nombre_instancia*\log

2000 *unidad*:\Archivos de programa\WebSphere\Commerce\instances*nombre_instancia*\log

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

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

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

Windows En las plataformas que no son Windows, WebSphere Commerce establece automáticamente los permisos de archivo para que los usuarios no autorizados no puedan acceder a archivos confidenciales. En las plataformas Windows, necesitará establecer los permisos manualmente del modo siguiente. Este procedimiento asegura que sólo el grupo de Administradores tenga el derecho de lectura/grabación/ejecución (`read/write/execute`) en los archivos confidenciales:

1. En Windows Explorer, pulse el botón derecho del ratón en la carpeta *unidad*:\WebSphere.
2. Pulse **Propiedades** y **Seguridad**. Por omisión, el grupo "Todos" tiene el permiso **all** para esta carpeta.
3. Pulse **Agregar**.
4. Se visualiza una ventana (Seleccionar usuarios, equipos...). En esta ventana, seleccione el grupo **Administradores**.

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

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

Campo Cifrado PDI del Gestor de configuración

Al configurar la instancia de WebSphere Commerce, se recomienda seleccionar el recuadro Cifrado PDI, lo cual especifica que debe cifrarse la información de las tablas `ORDPAYINFO` y `ORDPAYMTHD`. Cuando se selecciona el recuadro, la información de pago se almacena en la base de datos de WebSphere Commerce en formato cifrado.

Capítulo 5. Habilitación de la seguridad de WebSphere Application Server

Este capítulo describe cómo habilitar la seguridad para WebSphere Application Server. Al habilitar la seguridad de WebSphere Application Server, se evita que todos los componentes Enterprise JavaBean se expongan a la invocación remota por parte de cualquier usuario.

Nota: Windows AIX Solaris Linux Cuando se habilita la seguridad de WebSphere Application Server, se recomienda encarecidamente que la máquina satisfaga los requisitos siguientes:

- Un mínimo de memoria de 1 GB.
- Un mínimo de tamaño de almacenamiento dinámico de 384 MB, para la aplicación WebSphere Commerce.

Antes de empezar

Antes de empezar a habilitar la seguridad, necesitará conocer cómo valida los ID de usuario el sistema WebSphere Application Server en el que está habilitando la seguridad. WebSphere Application Server puede utilizar el registro de usuarios de LDAP o del sistema operativo como registro de usuarios de WebSphere Application Server.

Windows AIX Solaris Linux Para obtener información sobre los eFixes más recientes que se necesitan para ejecutar la seguridad de WebSphere Application Server, consulte el documento README de WebSphere Commerce 5.4 más reciente que esté disponible en el sitio Web de WebSphere Commerce, en:

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

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

Habilitación de la seguridad con un registro de usuarios de LDAP

Windows Para habilitar la seguridad de WebSphere Application Server cuando se está utilizando LDAP como registro de usuarios de WebSphere Application Server, conéctese al sistema como usuario con autorización administrativa y realice los pasos siguientes.

400 Para habilitar la seguridad de WebSphere Application Server cuando se está utilizando LDAP como registro de usuarios de WebSphere Application Server, conéctese al sistema y realice los pasos siguientes.

AIX Solaris Linux Para habilitar la seguridad de WebSphere Application Server cuando se está utilizando LDAP como registro de usuarios de WebSphere Application Server, conéctese al sistema como `wasuser` y realice los pasos siguientes.

1. Inicie el Servidor de administración de WebSphere Application Server y abra la Consola del administrador de WebSphere Application Server.

2. En la Consola, modifique los valores de seguridad globales como se indica a continuación:
   a. En el menú Consola, seleccione **Centro de seguridad**.
   b. En la pestaña General, seleccione **Habilitar seguridad**.
   c. En la pestaña **Autentificación**, seleccione Lightweight Third Party Authentication (LTPA). Rellene los valores de LTPA y elimine la selección del recuadro **Habilitar inicio de sesión único** si no desea utilizar esta función. Rellene la pestaña **Valores de LDAP** como se indica a continuación, en función del tipo de servidor de directorios que esté utilizando:

Tabla 8. Usuarios de SecureWay

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de servidor de seguridad	ID de usuario	*ID_usuario*	• No debe ser el administrador de LDAP. • No utilice un usuario que se haya especificado como cn=xxx. • Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de servidor de seguridad	Contraseña de usuario	*contraseña*	
Tipo de directorio	Tipo de servidor LDAP	SecureWay	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda	o=ibm,c=us	
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda		Este campo no es necesario
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace		Este campo no es necesario

Windows

Tabla 9. Usuarios de Netscape

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de servidor de seguridad	ID de usuario	*ID_usuario*	• No debe ser el administrador de LDAP. • No utilice un usuario que se haya especificado como cn=xxx. • Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de servidor de seguridad	Contraseña de usuario	*contraseña*	
Tipo de directorio	Tipo de servidor LDAP	Netscape	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda	o=ibm	
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda		Este campo no es necesario
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace		Este campo no es necesario

Windows

Tabla 10. Usuarios de Domino

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de servidor de seguridad	Nombre abreviado/ID de usuario	*ID_usuario*	Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de servidor de seguridad	Contraseña de usuario	*contraseña*	
Tipo de directorio	Tipo de servidor LDAP	Domino 5.0	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda		Este campo no es necesario
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda		Este campo no es necesario
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace		Este campo no es necesario

Windows

Tabla 11. Usuarios de Active Directory

Nombre de campo	Definición	Valores de ejemplo	Notas
ID de servidor de seguridad	Nombre de cuenta sAM	*ID_usuario*	• Nombre de conexión de usuario de cualquier usuario corriente. • No utilice un usuario que se haya especificado como cn=xxx. • Asegúrese de que la clase de objeto de este usuario sea compatible con la clase de objeto especificada en el campo Filtro de usuarios de la ventana de Propiedades avanzadas de LDAP.
Contraseña de servidor de seguridad	Contraseña de usuario	*contraseña*	
Tipo de directorio	Tipo de servidor LDAP	Active Directory	
Sistema principal	Nombre de sistema principal del servidor LDAP	*sistpral.dominio.com*	
Puerto	Puerto que está utilizando el servidor LDAP		Este campo no es necesario
Nombre distinguido básico	Nombre distinguido bajo el que se produce la búsqueda	CN=users, DC=domain1, DC=domain2, DC=com	
Nombre distinguido de enlace	Nombre distinguido para enlazar al directorio al realizar la búsqueda	CN=*ID_usuario*, CN=users, DC=domain1, DC=domain2, DC=com	El valor de *ID_usuario* es el Nombre de visualización. Este no es necesariamente igual al Nombre de conexión de usuario.
Contraseña de enlace	Contraseña para el Nombre distinguido de enlace	*contraseña_enlace*	Debe ser la misma que la Contraseña de servidor de seguridad.

d. Windows 400 Reinicie el servidor de administración de WebSphere Application Server y, a continuación, vuelva a abrir la Consola de administración de WebSphere Application Server.

e. En la pestaña **Correlación de roles**, seleccione el servidor de aplicaciones WCS y pulse el botón **Editar correlaciones...**.
   1) Seleccione el Rol de seguridad de WC y pulse el botón **Seleccionar...**.
   2) Marque el recuadro de selección Seleccionar usuarios/grupos y añada el ID de usuario que se ha entrado en el paso 2c en la página 58.

f. Pulse **Finalizar**.

3. Cierre la consola de administración y detenga y reinicie el Servidor de administración de WebSphere Application Server. A partir de ahora, cuando abra la Consola de administración de WebSphere Application Server, se le solicitará el ID y la contraseña del Servidor de seguridad.
4. Abra el Gestor de configuración de WebSphere Commerce y seleccione **Instancias** > *nombre_instancia* > **Propiedades de instancia** > **Seguridad** y pulse el recuadro de selección **Habilitar**. Se le solicitará que entre el nombre de usuario y la contraseña que ha entrado en el paso 2c en la página 58. Pulse **Aplicar** y, a continuación, salga del Gestor de configuración.
5. Detenga y reinicie el servidor de administración de WebSphere Application Server.

Habilitación de la seguridad con un registro de usuarios del sistema operativo

Windows 400 Para habilitar la seguridad de WebSphere Application Server cuando se está utilizando la validación de usuarios del sistema operativo como registro de usuarios de WebSphere Application Server, conéctese como usuario con autorización administrativa y realice los pasos siguientes.

AIX Solaris Linux Para utilizar el sistema operativo como un registro de usuario, debe ejecutar WebSphere Application Server como root. Ejecute WebSphere Application Server como root y realice los pasos siguientes.

1. AIX Solaris Linux Conéctese como root.
2. AIX Solaris Linux Inicie WebSphere Application Server e inicie la Consola de administración de WebSphere Application Server mientras está conectado como root:

   ```
   export DISPLAY=nombre_sistpral_totalmente_calificado:0.0
   cd INICIO_WAS/bin
   ./startupServer.sh &
   ./adminclient.sh nombre_sistpral_WAS_remoto puerto
   ```

   donde *nombre_sistpral_totalmente_calificado* es el nombre del sistema que utiliza para acceder a la Consola de administración de WebSphere Application Server, *nombre_sistpral_WAS_remoto* es el nombre de sistema principal totalmente calificado de WebSphere Application Server y puerto es el puerto a través del cual accede a WebSphere Application Server (el puerto por omisión es 2222).
3. En la Consola de administración de WebSphere Application Server, modifique los valores de seguridad globales como se indica a continuación:
   a. En el menú Consola, seleccione **Centro de seguridad**.
   b. En la pestaña General, seleccione el recuadro de selección **Habilitar seguridad**.
4. Seleccione la pestaña **Autentificación** y seleccione el botón de selección **Sistema operativo local**.
5. Entre el ID de servidor de seguridad en el campo **ID de servidor de seguridad**. Entre el nombre de usuario como se indica a continuación:

Nombre de campo	Valores de ejemplo	Notas
ID de usuario	*ID_usuario*	Windows ID de usuario con privilegios administrativos de sistema operativo con el que se ha conectado. Si la máquina pertenece a un dominio, utilice el ID de usuario totalmente calificado. Por ejemplo: DominioXYZ\id_usuario. Asegúrese de que esta cuenta exista en el servidor de dominios y de que sea miembro del grupo del Administrador. AIX Solaris Linux ID de usuario que sea root o que tenga autorización de root. 400 El id de usuario de iSeries debe tener autorización de `*SECOFR`.
Contraseña de servidor de seguridad	*contraseña*	Es la contraseña que pertenece al usuario con privilegios administrativos de sistema operativo con el que se ha conectado.

6. Windows 400 Reinicie el servidor de administración de WebSphere Application Server y, a continuación, vuelva a abrir la Consola de administración de WebSphere Application Server.
7. En la pestaña **Correlación de roles**, seleccione WC Enterprise Application y pulse el botón **Editar correlaciones...**.
   a. Seleccione el Rol de seguridad de WC y pulse el botón **Seleccionar...**.
   b. Seleccione el recuadro de selección Seleccionar usuarios/grupos, entre el ID de usuario que se ha utilizado en el paso 5 en la página 62 en el campo Buscar y pulse **Buscar**. Seleccione ese usuario en la lista Usuarios/Grupos disponibles y pulse **Añadir** para añadirlo a la lista Usuarios/Grupos seleccionados. A continuación, pulse **Aceptar** en cada panel hasta que salga del Centro de seguridad.
8. Abra el Gestor de configuración de WebSphere Commerce y seleccione **Lista de instancias** → *nombre_instancia* → **Propiedades de instancia**→ **Seguridad** y seleccione el recuadro de selección **Habilitar seguridad**. Seleccione **Registro de usuarios del sistema operativo** para la modalidad de autenticación y para entrar el nombre de usuario y la contraseña que ha entrado en el paso 5 en la página 62. Pulse **Aplicar** y, a continuación, salga del Gestor de configuración.
9. Detenga y reinicie el servidor de administración de WebSphere Application Server. A partir de ahora, cuando abra la Consola de administración de WebSphere Application Server, se le solicitará el ID y la contraseña del Servidor de seguridad .

Inhabilitación de la seguridad de EJB de WebSphere Commerce

WebSphere Commerce Business Edition le permite inhabilitar la seguridad de EJB. Para inhabilitar la seguridad de EJB de WebSphere Commerce, realice lo siguiente:

1. Inicie la Consola de administración de WebSphere Application Server.
2. Pulse **Consola → Centro de seguridad...** y deseleccione el recuadro de selección **Habilitar seguridad** de la pestaña **General**.
3. Abra el Gestor de configuración de WebSphere Commerce y seleccione **Lista de instancias → *nombre_instancia* → Propiedades de instancia→ Seguridad** y elimine la selección del recuadro **Habilitar seguridad**.
4. Salga de la Consola de administración de WebSphere Application Server.
5. Detenga y reinicie el servidor de administración de WebSphere Application Server.

Opciones de despliegue de seguridad de WebSphere Commerce

WebSphere Commerce soporta diversas configuraciones de despliegue de seguridad. La tabla siguiente ilustra las opciones de despliegue de seguridad disponibles.

Tabla 12. Escenarios de seguridad de una sola máquina

La seguridad de WebSphere Application Server está habilitada.	• Utilice el sistema operativo como registro de WebSphere Application Server. • Utilice la base de datos como registro de WebSphere Commerce.
	• Utilice LDAP como registro de WebSphere Application Server. • Utilice LDAP como registro de WebSphere Commerce.
	• Utilice LDAP como registro de WebSphere Application Server.
La seguridad de WebSphere Application Server está inhabilitada y el sitio de WebSphere Commerce está ubicado detrás de un cortafuegos.	• No se necesita un registro de WebSphere Application Server. • Utilice la base de datos como registro de WebSphere Commerce.
	• No se necesita un registro de WebSphere Application Server. • Utilice LDAP como registro de WebSphere Commerce.

Tabla 13. Escenarios de seguridad de varias máquinas

La seguridad de WebSphere Application Server está habilitada. LDAP se despliega siempre.	• Utilice LDAP como registro de WebSphere Application Server. • Utilice LDAP como registro de WebSphere Commerce.
	• Utilice LDAP como registro de WebSphere Application Server. • Utilice una base de datos como registro de WebSphere Commerce. • Necesitará configurar LDAP y poner una entrada administrativa en el registro de LDAP.
La seguridad de WebSphere Application Server está inhabilitada y el sitio de WebSphere Commerce está ubicado detrás de un cortafuegos.	• Utilice una base de datos como registro de WebSphere Commerce. • No se necesita un registro de WebSphere Application Server. • No se soporta el inicio de sesión único.
	• Utilice LDAP como registro de WebSphere Application Server. • No se necesita un registro de WebSphere Application Server.

Nota: Si el sitio de WebSphere Commerce funciona detrás de un cortafuegos, puede inhabilitar la seguridad de WebSphere Application Server. Sólo deberá inhabilitar la seguridad de WebSphere Application Server si está seguro de que no se están ejecutando aplicaciones delictivas detrás del cortafuegos.

Capítulo 6. Gestión de sesiones

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

WebSphere Commerce soporta dos tipos de gestión de sesiones: basada en cookies y de reescritura de URL. El administrador puede elegir dar soporte sólo a la gestión de sesiones basada en cookies o a la gestión de sesiones basada en cookies y de reescritura de URL. Si WebSphere Commerce sólo soporta la gestión de sesiones basada en cookies, los navegadores de los compradores deben poder aceptar cookies. Si se seleccionan la gestión de sesiones basada en cookies y de reescritura de URL, WebSphere Commerce intentará primero utilizar cookies para gestionar las sesiones; si el navegador del comprador está establecido para no aceptar cookies, entonces se utilizará la reescritura de URL.

Gestión de sesiones basada en cookies

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

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

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

- Cookie de sesión no seguro

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

  – Un cookie de sesión de WebSphere Application Server se basa en el estándar de sesión HTTP de servlet. Los cookies de WebSphere Application Server permanecen en la memoria o en la base de datos en un despliegue de varios

nodos. Para obtener más información, busque ″session management″ en el InfoCenter de WebSphere Application Server disponible en `http://www.ibm.com/software/webservers/appserv/infocenter.html`.

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

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

- Cookie de autenticación seguro

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

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

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

- El usuario se ha conectado desde otra ubicación con el mismo ID de conexión.
- El cookie ha quedado corrupto y/o se ha manipulado indebidamente.
- Si la aceptación de cookie está establecida en ″true″ (verdadera) y el navegador del usuario no soporta cookies.

Utilización de cookies para la gestión de sesiones

Para utilizar cookies en WebSphere Commerce, haga lo siguiente:

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

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

     Seleccione si desea que sea WebSphere Commerce o WebSphere Application Server quien gestione los cookies. El valor por omisión es WebSphere Commerce.

     – Un cookie de sesión de WebSphere Application Server se basa en el estándar de sesión HTTP de servlet. Los cookies de WebSphere Application Server permanecen en la memoria o en la base de datos en un despliegue de varios nodos. Para obtener más información, busque ″session management″ en el InfoCenter de WebSphere Application Server disponible en `http://www.ibm.com/software/webservers/appserv/infocenter.html`.

     – Un cookie de sesión de WebSphere Commerce es interno a WebSphere Commerce y no permanece en la base de datos.
4. Pulse la pestaña **Avanzada**. Seleccione los valores de sesión apropiados.

- Vía de acceso de cookies

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

  Este campo no se debe modificar. El valor por omisión es que un cookie caduque cuando se cierra el navegador.
- Dominio del cookie

  Generalmente este campo no se debe modificar. Especifica un patrón de restricción de dominio. Un dominio especifica los servidores que deben ver un cookie. Por omisión, el cookie sólo se devuelve al WebSphere Commerce Server que lo ha emitido. Por omisión, los cookies sólo se devuelven al sistema principal que los ha guardado. La especificación de un patrón de nombre de dominio prevalece sobre esto. El patrón debe empezar con un punto y debe contener dos puntos como mínimo. Un patrón sólo coincide con una entrada más allá del punto inicial. Por ejemplo ".ibm.com" es válido y coincide con a.ibm.com y con b.ibm.com pero no con www.a.ibm.com. Para obtener detalles sobre los patrones de dominio, consulte el RFC 2109 y la Especificación de cookie de Netscape.

5. Pulse **Aplicar**.
6. Cierre el Gestor de configuración.
7. En la Consola de administración de WebSphere Application Server, detenga y, a continuación, vuelva a iniciar la instancia.

Reescritura de URL

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

Nota: La reescritura de URL y el almacenamiento en antememoria de WebSphere Commerce no pueden actuar conjuntamente. Con la reescritura de URL activada, debe inhabilitar el componente de almacenamiento en antememoria de WebSphere Commerce.

Utilización de gestión de sesiones de reescritura de URL

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

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

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

   Gestor de sesiones de cookies. Seleccione WebSphere Application Server.
4. Pulse **Aplicar**.
5. Cierre el Gestor de configuración.

6. En la Consola de administración de WebSphere Application Server, detenga y, a continuación, vuelva a iniciar la instancia.

Escritura de plantillas de JSP para la reescritura de URL

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

Escritura de enlaces

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

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

se reescribe como

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

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

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

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

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

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

sustitúyala por:

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

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

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

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

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

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

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

Parte 3. Tareas de seguridad del administrador del sistema

Esta parte describe las tareas de seguridad que normalmente puede realizar un administrador del sistema en el sitio, no necesariamente el administrador de sitio de WebSphere Commerce.

Capítulo 7. Establecimiento y cambio de contraseñas

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

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

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

Windows **ID de usuario de Windows**

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

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

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

Importante

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

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

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

Perfiles de usuario de iSeries 400

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

- Un perfil de usuario que se crea y utiliza para instalar WebSphere Commerce y acceder al Gestor de configuración. Para instalar y configurar WebSphere Commerce, deberá utilizar un perfil de usuario de iSeries de USRCLS(*SECOFR) o utilizar el perfil de usuario QSECOFR. Si necesita crear un perfil de usuario, consulte la publicación *WebSphere Commerce 5.4, Guía de instalación* para iSeries.
- Un perfil de usuario creado por el Gestor de configuración cuando se crea una instancia de WebSphere Commerce. Este perfil de usuario se conoce también como "perfil de usuario de instancia". El Gestor de configuración crea un perfil de usuario de USRCLS(*USER) cada vez que se crea una instancia de WebSphere Commerce. Si necesita crear un perfil de usuario, consulte la publicación *WebSphere Commerce 5.4, Guía de instalación* para iSeries.

ID de usuario del Gestor de configuración

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

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

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

ID de usuario de IBM HTTP Server Windows AIX Solaris Linux

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

`http://`*`nombre_sistpral`*

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

Administrador de instancias de WebSphere Commerce

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

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

  `https://`*`nombre_sistpral`*`:8000/accelerator`

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

  `https://nombre_sistpral:8000/adminconsole`
- Servicios de tienda. Puede acceder a la página Servicios de tienda abriendo el navegador Web y escribiendo la dirección Web siguiente:

  `https://nombre_sistpral:8000/storeservices`

El ID de usuario por omisión del Administrador de instancias es `wcsadmin` y la contraseña por omisión es `wcsadmin`.

Nota: El ID de usuario `wcsadmin` no debe eliminarse nunca y debe tener siempre autorización de administrador de instancias.

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

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

Administrador de Payment Manager

Cuando se instala Payment Manager, se asigna automáticamente al ID de administrador de WebSphere Commerce, `wcsadmin`, el rol de Administrador de Payment Manager. Siga las instrucciones de la publicación *WebSphere Commerce 5.4, Guía de instalación* para conmutar la Clase de dominio de Payment Manager a WCSRealm si dicha acción aún no se ha realizado.

El rol de Administrador de Payment Manager habilita un ID de usuario para controlar y administrar Payment Manager.

Notas: 400

- No suprima el ID de usuario de conexión `wcsadmin` ni le cambie el nombre, y no cambie el rol preasignado de Payment Manager de `wcsadmin` porque las funciones de WebSphere Commerce relacionadas con la integración de Payment Manager no funcionarán.
- Si asigna un rol de Payment Manager a un administrador de WebSphere Commerce y posteriormente desea suprimir el ID de usuario de conexión de este administrador o cambiar su nombre, deberá eliminar el rol de Payment Manager de administrador antes de suprimir el ID de usuario o de cambiarle el nombre.

Importante

Payment Manager ha preasignado el rol de Administrador de Payment Manager a otros dos ID de administración:

- `ncadmin`
- `admin`

Para evitar que un usuario obtenga de forma inadvertida este rol de Administrador de Payment Manager, puede:

1. Crear los ID de administración anteriores en WebSphere Commerce utilizando la Consola de administración de WebSphere Commerce.
2. En la interfaz de usuario de Payment Manager, seleccionar **Usuarios**.
3. Eliminar el rol de Administrador de Payment Manager de estos dos ID de administración.

También deberá conocer la Contraseña de instancia de Payment Manager, que es necesaria para iniciar, detener o suprimir una instancia de Payment Manager. También es necesario añadir casetes a una instancia de Payment Manager. Si el Gestor de configuración de WebSphere Commerce crea una instancia de Payment Manager, la contraseña de esa instancia será la misma que la contraseña de conexión de la instancia de WebSphere Commerce, que también se denomina contraseña del perfil de usuario de la instancia. Si se crea una instancia de Payment Manager desde una sesión de iSeries utilizando el mandato **CRTPYMMGR** o desde la página de tareas de iSeries, se le solicitará que proporcione la contraseña.

Cómo cambiar la contraseña del Gestor de configuración

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

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

```
config_env
java com.ibm.commerce.config.server.PasswordChecker -action [tipo de acción]
   -pwfile [archivo de contraseñas] -userid [ID de usuario]
   -password [contraseña id de usuario] [-newpassword [nueva contr. id de usuario]]
```

donde los tipos de acción son `Add`, `Check`, `Delete` o `Modify`. Los parámetros se explican a continuación:

pwfile
Vía de acceso al archivo donde se almacenará la contraseña. La vía de acceso por omisión es el subdirectorio `bin` bajo la vía de acceso de instalación de WebSphere Commerce. Este parámetro siempre es necesario.

userid
Entre el ID de usuario que desea añadir, comprobar, suprimir o modificar. Este parámetro siempre es necesario.

password
Entre la contraseña que desea crear, comprobar, suprimir o modificar. Este parámetro debe utilizarse conjuntamente con el parámetro `userid`. Este parámetro siempre es necesario.

newpassword
Utilice este parámetro para cambiar la contraseña para un ID de usuario determinado. Este parámetro debe utilizarse conjuntamente con los parámetros `userid` y `password`. Este parámetro es necesario cuando se especifica el tipo de acción `Modify`.

Establecimiento de la contraseña de administrador de IBM HTTP Server

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

1. Vaya al directorio de instalación de IBM HTTP Server de la máquina.
2. Escriba el mandato siguiente:

   Windows `htpasswd -b conf\admin.passwd` *`usuario contraseña`*

   AIX Solaris Linux `htpasswd -b conf/admin.passwd` *`usuario contraseña`* donde *usuario* y *contraseña* son el ID de usuario y la contraseña que desea que tengan autorización administrativa para IBM HTTP Server.

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

Cómo cambiar la contraseña del archivo de claves SSL

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

1. Windows Pulse el menú **Inicio** → **Programas** → **IBM HTTP Server** → **Programa de utilidad de gestión de claves**.
2. En el menú **Archivo de base de datos de claves**, seleccione **Abrir**.
3. Vaya al subdirectorio `ssl` bajo la vía de acceso de instalación de IBM HTTP Server de la máquina. El archivo de claves (que tiene la extensión de archivo `.kdb`) debería estar en esta carpeta. Si no está, cree un archivo de claves nuevo siguiendo las instrucciones descritas en el Capítulo 8, "Habilitación de SSL para producción con IBM HTTP Server" en la página 81.
4. En el menú **Archivo de base de datos de claves**, seleccione **Cambiar contraseña**. Aparecerá la ventana Cambiar contraseña.
5. Entre la contraseña nueva y habilite **Ocultar la contraseña para un archivo**.
6. Pulse **Aceptar**. La contraseña se ha cambiado.

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

Generación de contraseñas cifradas de WebSphere Commerce

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

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

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

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

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

400 En iSeries, para cambiar la contraseña cifrada de los compradores, utilice el mandato `CHGWCSPWD`. Consulte la ayuda en línea, pulsando F1, para obtener detalles sobre la ejecución de este mandato.

Generación de contraseñas cifradas de Payment Manager

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

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

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

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

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

400 En iSeries, para generar contraseñas cifradas para Payment Manager, utilice el mandato `CRTWCSPMPW`. Consulte la ayuda en línea, pulsando F1, para obtener detalles sobre la ejecución de este mandato.

Capítulo 8. Habilitación de SSL para producción con IBM HTTP Server

400 Esta sección no se aplica a la plataforma iSeries. Para obtener información sobre iSeries, consulte el apartado “Habilitación de SSL en IBM HTTP Server (iSeries)” en la página 85.

Después de crear la instancia de WebSphere Commerce con IBM HTTP Server, SSL está habilitado para realizar pruebas. Antes de abrir el sitio a los compradores, deberá habilitar SSL para producción siguiendo los pasos de este capítulo.

Acerca de la seguridad

IBM HTTP Server proporciona un entorno seguro para las transacciones de negocio utilizando la tecnología de cifrado. El cifrado es la codificación del intercambio de información en Internet para que ésta no se pueda leer hasta que el receptor las descifre. El remitente utiliza un patrón o clave de algoritmo para codificar (cifrar) una transacción y el receptor utiliza una clave de descifrado. Estas claves las utiliza el protocolo SSL (Secure Sockets Layer).

El servidor Web utiliza un proceso de autenticación para verificar la identidad de la persona con la que se están realizando negocios (es decir, para asegurarse de que dicha persona es quien afirma ser). Esto implica la obtención de un certificado firmado por un tercero fiable denominado autoridad de certificación (CA). Para los usuarios de IBM HTTP Server, la CA puede ser Equifax® o VeriSign® Inc. También hay otras CA disponibles.

Para crear un archivo de claves de producción, realice los pasos siguientes:

1. Cree un archivo de claves de seguridad para producción.
2. Solicite un certificado seguro a una autoridad de certificación.
3. Establezca el archivo de claves de producción como archivo de claves actual.
4. Reciba el certificado y pruebe el archivo de claves de producción.

Estos pasos se describen detalladamente a continuación.

Notas:

1. Si ya está utilizando un archivo de claves de producción firmado por una autoridad de certificación, es posible que pueda saltarse estos pasos. Para determinarlo, lea este capítulo.
2. Mientras realice estos pasos, puede que el navegador muestre mensajes de seguridad. Examine cuidadosamente la información de cada mensaje y decida cómo debe continuar.

Creación de un archivo de claves de seguridad para producción

Para crear un archivo de claves de seguridad para producción, realice lo siguiente en la máquina servidor web:

1. Detenga IBM HTTP Server.
2. Cambie el directorio por el subdirectorio `conf` bajo el subdirectorio de instalación de IBM HTTP Server de la máquina.
3. Cree una copia de seguridad de `httpd.conf`.

4. Abra `httpd.conf` en un editor de texto.
5. Asegúrese de que se ha eliminado el signo de comentario en las líneas siguientes para el puerto 443:
   - Windows

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

   - AIX Solaris Linux

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

     donde *archivoclaves* es uno de los siguientes:

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

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

     Linux `/opt/IBMHTTPServer/ssl/keyfile.kdb`
6. Asegúrese de que se ha eliminado el signo de comentario en las líneas siguientes para el puerto 8000:
   a. `#Listen 8000`
   b. `#<VirtualHost sistpral.algún_dominio.com:8000>`. En esta línea también debe sustituir el nombre de sistema principal totalmente calificado.
   c. `#SSLEnable`
   d. `#</VirtualHost>`

   Nota: Se recomienda que el software de cortafuegos bloquee el acceso externo al puerto que ha configurado para las Herramientas de WebSphere Commerce (puerto 8000 por omisión). Consulte la documentación para el software de cortafuegos que esté utilizando en el sitio para obtener información sobre cómo realizar dicha tarea.
7. Guarde los cambios.
8. Para asegurarse de que el archivo `httpd.conf` no contiene errores de sintaxis, vaya al subdirectorio `bin` bajo el directorio de instalación de IBM HTTP Server de la máquina y ejecute el mandato siguiente:

   AIX Solaris Linux `./apachectl configtest`

   Windows `apachectl configtest`
9. Inicie IBM HTTP Server.

Solicitud de un certificado seguro a una autoridad de certificación

Para validar el archivo de claves de seguridad que acaba de crear en el paso anterior, necesita un certificado de una autoridad de certificación (CA), por ejemplo Equifax o VeriSign. El certificado contiene la clave pública del servidor, el Nombre distinguido asociado al certificado del servidor y el número de serie y la fecha de caducidad del certificado.

Si desea utilizar una CA diferente, póngase en contacto con ella directamente para obtener información sobre el procedimiento que debe seguir.

Usuarios de Equifax

Para solicitar un certificado de servidor seguro a Equifax, consulte la dirección Web siguiente y siga las instrucciones que se proporcionan:

`http://www.equifax.com`

Deberá recibir de Equifax el certificado de servidor de seguridad por correo electrónico en un periodo de 2 a 4 días laborables.

Usuarios de VeriSign

Para solicitar un certificado de servidor seguro a VeriSign, consulte el URL siguiente y siga las instrucciones que se proporcionan:

`http://www.verisign.com`

AIX Aunque esté utilizando los procedimientos para IBM HTTP Server, siga el enlace para **Internet Connection Secure Server** (ICSS). Siga las instrucciones que se proporcionan. Cuando reciba el certificado, cree el archivo de claves de producción tal como se describe en el apartado anterior, si aún no lo ha creado.

Solaris Aunque esté utilizando los procedimientos para IBM HTTP Server, siga el enlace para **Internet Connection Secure Server** (ICSS). La página que aparece a continuación indica que los procedimientos se aplican a las plataformas OS/2 y AIX. Estas instrucciones también se aplican para el software Solaris.

Siga las instrucciones que se proporcionan. Una vez que haya sometido la petición, el certificado deberá llegar en un periodo de tiempo de tres a cinco días laborables. Cuando lo reciba, cree el archivo de claves de producción tal como se describe en el apartado anterior, si aún no lo ha creado.

Cómo recibir el archivo de claves de producción y establecerlo como archivo de claves actual

Cuando llegue el certificado de la CA, tendrá que hacer que el servidor Web utilice el archivo de claves de producción. Realice los pasos siguientes:

1. Copie los archivos *nombrecertificado*`.kdb`, *nombrecertificado*`.rdb` y *nombrecertificado*`.sth` que ha recibido de la autoridad de certificación en el subdirectorio `ssl` bajo la vía de acceso de instalación de IBM HTTP Server de la máquina, donde *nombrecertificado* es el nombre de certificado que ha proporcionado con la petición de certificado.
2. Abra el Programa de utilidad de gestión de claves.
3. Abra el archivo *nombrecertificado*`.kdb` y entre la contraseña cuando se le solicite.
4. Seleccione **Certificados personales** y pulse **Recibir**.

5. Pulse **Examinar**.
6. Seleccione la carpeta donde ha almacenado los archivos que ha recibido de la autoridad de certificación. Seleccione el archivo *nombrecertificado*.txt y pulse **Aceptar**.
7. El recuadro de lista **Certificados personales** debe listar ahora el certificado *nombrecertificado* de Verisign o el certificado *nombrecertificado* de Equifax.
8. Salga del Programa de utilidad de gestión de claves.
9. Cambie de directorio y vaya al subdirectorio conf bajo la vía de acceso de instalación de IBM HTTP Server de la máquina.
10. Cree una copia de seguridad de httpd.conf.
11. Abra httpd.conf en un editor de texto.
12. Asegúrese de que las líneas listadas en el paso 5 en la página 82 no estén comentadas.
13. Busque la directiva Keyfile "*nombre de vía de acceso de archivo de claves*" y cambie el nombre de vía de acceso para que apunte al archivo creado en los pasos anteriores.
14. Detenga y reinicie IBM HTTP Server.

Prueba del archivo de claves de producción

Para probar la clave de producción, realice lo siguiente:

1. Vaya al URL siguiente con el navegador:
   https://*nombre_sistpral*

   Notas:

   a. Si ha personalizado el servidor Web, puede que necesite escribir el nombre de la página frontal del servidor Web después del nombre de sistema principal.
   b. Asegúrese de escribir https, *no* http.

   Si la clave está definida correctamente, verá varios mensajes acerca del nuevo certificado.
2. Si desea aceptar este certificado, en el panel **Nuevo certificado de sitio** seleccione el botón de selección **Aceptar este certificado para siempre (hasta que caduque)**.
3. Desde el navegador Web, restaure los valores de servidor de antememoria y proxy (o socks) a sus estados originales.

SSL ya está habilitado en el servidor.

Consideraciones sobre SSL para Payment Manager

Por omisión, la comunicación entre WebSphere Commerce y Payment Manager se efectúa a través de SSL. Sin embargo, si inicia directamente la interfaz de usuario de Payment Manager de la manera siguiente:

http://*nombre_sistpral*/webapp/Paymentmanager/

está llamando a Payment Manager utilizando una comunicación no SSL. Para asegurarse de que la comunicación es a través de SSL, debe utilizar

https://*nombre_sistpral*/webapp/Paymentmanager/

o cambiar el nombre del archivo `indexSSL.html` por `index.html` en el siguiente directorio:

- Windows *INICIO_WAS*`\installedApps\IBM_PaymentManager.ear\PaymentManager.war`
- AIX Solaris

  Linux *INICIO_WAS*`/installedApps/IBM_PaymentManager.ear/PaymentManager.war`

De esta manera, puede seguir utilizando el directorio **http://***nombre_sistpral*`/webapp/Paymentmanager/` y el archivo `index.html` redenominado le redirigirá a `https` (SSL).

Habilitación de SSL en IBM HTTP Server (iSeries)

400 Esta sección se aplica a la plataforma iSeries.

SSL es un protocolo de seguridad. SSL asegura que los datos transferidos entre un cliente y un servidor permanezcan privados. Permite que el cliente autentique la identidad del servidor y que el servidor autentique la identidad del cliente.

Los certificados digitales son documentos electrónicos que autentican los servidores y clientes involucrados en las transacciones seguras por Internet. El emisor de certificados digitales se denomina Autoridad de certificación (CA). El sistema iSeries puede efectuar el rol de una CA en un entorno de Intranet emitiendo certificados de servidor y de cliente, y funcionar como un servidor autenticado con certificados de servidor emitidos por una CA de iSeries o una CA de Internet como VeriSign®. Como servidor Web, también se puede configurar IBM HTTP Server para iSeries para que solicite certificados de cliente para autenticar los clientes habilitados SSL.

Para obtener información detallada sobre cómo habilitar SSL en IBM HTTP Server para iSeries, consulte la siguiente dirección Web:

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

En concreto, consulte la sección **Hints and Tips**.

Utilización de SSL con Payment Manager

Si crea la tienda con certificados del sistema después de crear la instancia de WebSphere Commerce, debe otorgar acceso a la tienda, tanto a la instancia de Payment Manager como a la instancia de WebSphere Commerce. Por ejemplo, los mandatos siguientes otorgan, a la instancia de Payment Manager, el acceso necesario en un sistema V5R1:

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

y los mandatos siguientes otorgan, a WebSphere Commerce, el acceso necesario en un sistema V5R1:

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

Si elige utilizar una instancia de Payment Manager remota, debe configurar la instancia de WebSphere Commerce y la instancia de Payment Manager para que acepten la autoridad de certificación remota que emite el certificado digital. Para establecer una relación de confianza entre dos aplicaciones remotas, consulte el siguiente procedimiento general:

1. En la máquina de WebSphere Commerce, utilice el gestor de certificados digitales para exportar la autoridad de certificación del servidor.

2. Transfiera el archivo de certificados a la máquina de Payment Manager.
3. En la máquina de Payment Manager, utilice el gestor de certificados digitales para importar la autoridad de certificación del servidor WebSphere Commerce.
4. Configure el servidor de aplicaciones de Payment Manager para que acepte la autoridad de certificación del servidor WebSphere Commerce importado.
5. En la máquina de Payment Manager, utilice el gestor de certificados digitales para exportar la autoridad de certificación del servidor.
6. Transfiera el archivo de certificados a la máquina de WebSphere Commerce.
7. En la máquina de WebSphere Commerce, utilice el gestor de certificados digitales para importar la autoridad de certificación del servidor de Payment Manager.
8. Configure el servidor de aplicaciones de WebSphere Commerce para que acepte la autoridad de certificación del servidor de Payment Manager importado.

Para obtener información detallada, consulte la sección **Hints and Tips** en la dirección Web siguiente:

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

Capítulo 9. Habilitación de SSL para IBM SecureWay Directory Server (LDAP)

A continuación se indican los pasos necesarios para configurar la seguridad SSL para IBM SecureWay Directory Server y WebSphere Commerce.

Configuración de SecureWay

Para configurar IBM SecureWay Directory Server:

1. Instale IBM SecureWay Directory Server siguiendo las instrucciones de instalación de SecureWay Directory Server. Asegúrese de instalar el componente GSKit.
2. Cuando la instalación se haya completado, invoque el Gestor de claves de IBM (*unidad*:\Archivos de programa\IBM\GSK4\bin\gsk4ikm.exe en Windows).
3. Cree un archivo de base de datos de claves CMS nuevo. Asegúrese de que **ocultar la contraseña para un archivo** esté seleccionado (por ejemplo ldap_key.kdb)
4. Cree un certificado autofirmado.
5. Extraiga el certificado como tipo datos ASCII codificados con Base64.
6. Cree una clase de base de datos de claves SSLight nueva (por ejemplo, keyring.class).
7. En la sección **Certificados Singer**, añada el archivo de certificado creado en el paso 5.
8. Abra un navegador en la dirección siguiente: http://nombresistpral/ldap
9. Pulse **Seguridad —> SSL —> Valores** y realice los cambios siguientes:
   - Estado de SSL: SSL activo o SSL sólo
   - Método de autenticación: Autenticación de servidor
   - Puerto seguro: 636
   - Vía de acceso y nombre de archivo de base de datos de claves:

     AIX Solaris Linux /Keys/ldap_key.kdb

     Windows *unidad*:\Keys\ldap_key.kdb
   - Etiqueta de clave: *su_etiqueta* (La etiqueta del certificado)
10. Pulse **Actualizar** y reinicie SecureWay.

WebSphere Commerce

Si desea configurar WebSphere Commerce para que funcione con SecureWay Directory Server, deberá modificar el archivo *instancia*.xml:

```
java.naming.security.ssl.keyring = keyring
'keyring' es el nombre de la clase de base de datos de claves SSLight (keyring.class)
Este archivo de clase debe ponerse en la vía de acceso de clases en WAS.

java.naming.security.ssl.authentication = ibm
'ibm' es la contraseña especificada al crear la clase de base de datos de claves SSLight.

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

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

Reinicie WebSphere Commerce.

Capítulo 10. ID de conexión único

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

Prerrequisitos

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

- Tiene que estar instalado y configurado un servidor LDAP existente. Para configurar un servidor LDAP, consulte la publicación *IBM WebSphere Commerce Versión 5.4, Guía de software adicional*.
- WebSphere Commerce tiene que estar instalado y configurado para utilizar LDAP.
- La seguridad de WebSphere Application Server tiene que estar habilitada. Para habilitar la seguridad de WebSphere Application Server, consulte el Capítulo 5, "Habilitación de la seguridad de WebSphere Application Server" en la página 57.

Habilitación del ID de conexión único

Limitaciones

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

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

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

1. Habilite el ID de conexión único en WebSphere Application Server. Para obtener más información, busque "single sign-on" (ID de conexión único) en el InfoCenter de WebSphere Application Server disponible en:

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

   Seleccione **Single Sign-On: WebSphere Application Server** y complete las secciones siguientes:

   - **Configuring SSO for WebSphere Application Server**.
     - **Modify WebSphere Application Server security settings**.

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

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

2. En la máquina de WebSphere Commerce, inicie el Gestor de configuración de WebSphere Commerce.
3. Para configurar el nodo **Subsistema de miembros**, realice lo siguiente:
   a. Expanda **WebSphere Commerce** → *nombre_sistpral* → **Lista de instancias** → *nombre_instancia* → **Propiedades de instancia** → **Subsistema de miembros**.
   b. En el menú desplegable **Modalidad de autenticación**, seleccione **LDAP**.
   c. Habilite el recuadro de selección **ID de conexión único**.
   d. En el campo **Sistema principal**, entre el nombre de sistema principal totalmente calificado del servidor LDAP.
   e. Entre el nombre distinguido del administrador en el campo **Nombre distinguido del administrador**. Este deberá ser el mismo nombre que se ha utilizado en el servidor LDAP.
   f. En el campo **Contraseña del administrador**, entre la contraseña del administrador. Esta deberá ser la misma contraseña que se ha utilizado en el servidor LDAP. Confirme la contraseña en el campo **Confirmar contraseña**.
   g. Rellene cada uno de los campos restantes.
   h. Pulse **Aplicar** y, a continuación, pulse **Aceptar**.
4. Reinicie WebSphere Application Server.

Parte 4. Tareas de seguridad del desarrollador de WebSphere Commerce

Esta parte describe las tareas de seguridad que están relacionadas con la programación de WebSphere Commerce. Estas tareas las realizan normalmente los programadores de WebSphere Commerce.

Capítulo 11. Control de acceso

¿Qué es el control de acceso?

El modelo de control de acceso de una aplicación WebSphere Commerce tiene tres conceptos principales: usuarios, acciones y recursos. Los usuarios son las personas que utilizan el sistema. Los recursos son las entidades que se mantienen en la aplicación o mantenidas por la aplicación. Por ejemplo, los recursos pueden ser productos, documentos o pedidos. Los perfiles de usuario que representan a las personas son también recursos. Las acciones son las actividades que pueden realizar los usuarios en los recursos. El control de acceso es el componente de la aplicación e-commerce que determina si un usuario determinado puede realizar una acción concreta en un recurso en particular.

En una aplicación de WebSphere Commerce, existen dos niveles principales de control de acceso. El primer nivel de control de acceso lo realiza WebSphere Application Server. En este sentido, WebSphere Commerce utiliza WebSphere Application Server para proteger los servlets y los beans enterprise. El segundo nivel de control de acceso es el sistema de control de acceso detallado de WebSphere Commerce.

La infraestructura de control de acceso de WebSphere Commerce utiliza políticas de control de acceso para determinar si a un usuario determinado se le permite realizar una acción concreta en un recurso en particular. Esta infraestructura de control de acceso proporciona control de acceso detallado. Funciona conjuntamente con el control de acceso proporcionado por WebSphere Application Server, pero no lo sustituye.

Visión general de la protección de recursos en WebSphere Application Server

Los siguientes recursos de WebSphere Commerce están protegidos bajo el control de acceso realizado por WebSphere Application Server:

- Beans de entidad
  Estos beans crean modelos de objetos en una aplicación e-commerce. Se trata de objetos distribuidos a los que pueden acceder clientes remotos.
- Plantillas JSP
  WebSphere Commerce utiliza plantillas JSP para las páginas de visualización. Cada plantilla JSP puede contener uno o más beans de datos que recuperan datos de los beans de entidad. Los clientes pueden solicitar páginas JSP escribiendo una petición de URL.
- Mandatos de controlador y vista
  Los clientes pueden solicitar mandatos de controlador y vista escribiendo peticiones de URL. Además, una página de visualización puede contener un enlace a otra página utilizando el nombre de archivo JSP o el nombre de vista, tal como está registrado en la tabla VIEWREG.

WebSphere Commerce Server se configura normalmente para utilizar las vías de acceso Web siguientes:

- `/webapp/wcs/stores/servlet/*`
  Se utiliza para peticiones al servlet de peticiones.

- `/webapp/wcs/stores/*.jsp`
  Se utiliza para peticiones al servlet JSP.

El diagrama siguiente muestra la ruta que potencialmente pueden seguir las peticiones para acceder a los recursos de WebSphere Commerce, para la configuración de vías de acceso Web anterior.

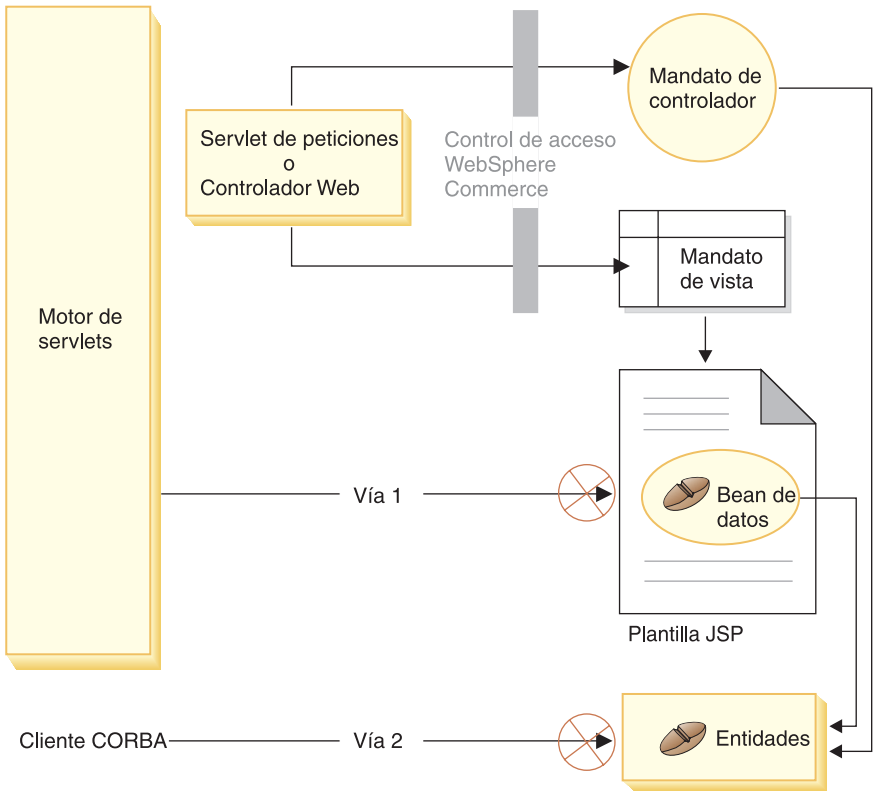


Figura 3.

Todas las peticiones legítimas deben dirigirse al servlet de peticiones, el cual, a continuación, las dirige al controlador Web. El controlador Web implementa el control de acceso para los mandatos de controlador y las vistas. No obstante, las vías de acceso Web hacen que sea posible que usuarios malintencionados accedan directamente a las plantillas JSP (vía 1) y a los beans de entidad (vía 2). Para evitar estas intrusiones malintencionadas, deben rechazarse en la ejecución.

El acceso directo a las plantillas JSP y los beans de entidad puede evitarse utilizando una de las propuestas siguientes:

Seguridad de WebSphere Application Server
WebSphere Application Server proporciona una característica de seguridad. Si se utiliza esta característica, todos los métodos de bean enterprise y las plantillas JSP se configuran para que sólo los invoque la Identidad de sistema. Para acceder a estos recursos de WebSphere Commerce, una petición de URL debe direccionarse al servlet de peticiones que establece la Identidad del sistema en la hebra actual, antes de pasarla al controlador Web. Entonces el controlador Web asegura que la persona que realiza la llamada tenga la autorización necesaria antes de pasar la petición a la vista o al mandato de controlador correspondiente. El componente de seguridad

de WebSphere Application Server rechaza cualquier intento de acceso directo a las plantillas JSP y a los beans de entidad (es decir, sin utilizar el controlador Web).

Para obtener información sobre cómo configurar WebSphere Application Server para proteger los recursos de WebSphere Commerce, consulte la publicación *WebSphere Commerce, Guía de instalación*. Para obtener información sobre la seguridad en WebSphere Application Server, consulte el tema que trata sobre la Administración del sistema en la documentación de WebSphere Application Server.

Para obtener información sobre cómo configurar la seguridad de WebSphere Application Server para los métodos de los beans enterprise personalizados, consulte las secciones "Ensamblaje de beans enterprise nuevos en una aplicación de empresa" y "Ensamblaje de beans enterprise modificados en una aplicación de empresa" de la publicación *WebSphere Commerce 5.4, Guía del programador*.

Protección mediante cortafuegos

Cuando WebSphere Commerce Server se ejecuta detrás de un cortafuegos, los clientes de Internet no pueden acceder directamente a los beans de entidad. Si se utiliza este método, el bean de datos que está incluido en la página proporciona protección para las plantillas JSP. El gestor de beans de datos activa el bean de datos. El gestor de beans de datos detecta si la plantilla JSP ha sido reenviada por un mandato de vista. Si no ha sido reenviada por un mandato de vista, se emite una excepción y se rechaza la petición de la plantilla JSP.

Introducción a las políticas de control de acceso de WebSphere Commerce

El modelo de control de acceso de WebSphere Commerce se basa en la imposición de las políticas de control de acceso. Las políticas de control de acceso permiten exteriorizar las normas de control de acceso respecto al código de la lógica de negocio, eliminando de este modo la necesidad de codificar sentencias de control de acceso en el código. Por ejemplo, no es necesario incluir código similar al siguiente:

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

Las políticas de control de acceso las impone el gestor de políticas de control de acceso. En general, cuando un usuario intenta acceder a un recurso protegido, el gestor de políticas de control de acceso determina primero qué políticas de control de acceso son aplicables para dicho recurso protegido y, a continuación, basándose en las políticas de control de acceso aplicables, determina si se permite al usuario acceder a los recursos solicitados.

Una política de control de acceso es una política con cuatro elementos que se almacena en la tabla ACPOLICY. Cada política de control de acceso tiene el formato siguiente:

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

Estos elementos de la política de control de acceso de cuatro secciones especifican que a un usuario que pertenece a un grupo de acceso específico se le permite realizar acciones del grupo de acciones especificado, en los recursos que pertenecen al grupo de recursos especificado, a condición de que el usuario satisfaga las condiciones especificadas en la relación o grupo de relaciones, respecto al recurso

en cuestión. Por ejemplo, [AllUsers, UpdateDoc, doc, creator] especifica que todos los usuarios pueden actualizar un documento, si son los creadores del documento.

El grupo de usuarios es un tipo específico de grupo de miembros que se define en la tabla de base de datos MBRGRP. Un grupo de usuarios debe estar asociado con un tipo de grupo de miembros de -2. El valor -2 representa un grupo de acceso que está definido en la tabla MBRGRPTYPE. La asociación entre el grupo de usuarios y el tipo de grupo de miembros se almacena en la tabla MBRGRPUSG.

La pertenencia de un usuario, como miembro, a un grupo de acceso determinado puede expresarse de forma explícita o implícita. Se produce una especificación explícita si la tabla MBRGRPMBR indica que el usuario pertenece a un grupo de miembros determinado. Una especificación implícita se produce si el usuario satisface una condición (por ejemplo, todos los usuarios que desempeñan un rol de Jefe de producto) que está expresada en la tabla MBRGRPCOND. También pueden haber condiciones combinadas (por ejemplo, todos los usuarios que desempeñan el rol de Jefe de producto y que han desempeñado el rol durante un mínimo de 6 meses) o exclusiones explícitas.

La mayoría de las condiciones para incluir a un usuario en un grupo de usuarios se basan en la ejecución de un rol determinado por parte del usuario. Por ejemplo, puede haber una política de control de acceso que permita a todos los usuarios que desempeñan el rol de Jefe de producto realizar operaciones de gestión de catálogo. En este caso, cualquier usuario al que se haya asignado el rol de Jefe de producto en la tabla MBRROLE estará incluido implícitamente en el grupo de usuarios.

Para obtener más detalles sobre el subsistema de grupos de miembros, consulte la ayuda en línea de WebSphere Commerce.

El elemento Grupo de acciones procede de la tabla ACACTGRP. Un grupo de acciones hace referencia a un grupo de acciones especificado explícitamente. El listado de acciones se almacena en la tabla ACACTION y la relación de cada acción con su grupo (o grupos) de acciones se almacena en la tabla ACACTACTGP. El grupo de acciones ″OrderWriteCommands″ es un ejemplo de grupo de acciones. Este grupo de acciones incluye las acciones siguientes que se utilizan para actualizar pedidos:

- com.ibm.commerce.order.commands.OrderDeleteCmd
- com.ibm.commerce.order.commands.OrderCancelCmd
- com.ibm.commerce.order.commands.OrderProfileUpateCmd
- com.ibm.commerce.order.commands.OrderUnlockCmd
- com.ibm.commerce.order.commands.OrderScheduleCmd
- com.ibm.commerce.order.commands.ScheduledOrderCancelCmd
- com.ibm.commerce.order.commands.ScheduledOrderProcessCmd
- com.ibm.commerce.order.commands.OrderItemAddCmd
- com.ibm.commerce.order.commands.OrderItemDeleteCmd
- com.ibm.commerce.order.commands.OrderItemUpdateCmd
- com.ibm.commerce.order.commands.PayResetPMCmd

Un grupo de recursos es un mecanismo para agrupar determinados tipos de recursos. La calidad de miembro de un recurso en un grupo de recursos puede especificarse de una de estas dos formas:

- Utilizando la columna de condiciones de la tabla ACRESGRP

- Utilizando la tabla ACRESGPRES

En la mayoría de los casos, es suficiente utilizar la tabla ACRESGPRES para asociar recursos con grupos de recursos. Si se utiliza este método, los recursos se definen en la tabla ACRESCGRY utilizando el nombre de clase Java. Entonces estos recursos se asocian con los grupos de recursos apropiados (tabla ACRESGRP) utilizando la tabla de asociación ACRESGPRES. En los casos en que el nombre de clase Java solo no es suficiente para definir los miembros de un grupo de recursos (por ejemplo, si necesita restringir adicionalmente los objetos de esta clase basándose en un atributo del recurso), el grupo de recursos puede definirse por completo utilizando la columna de condiciones de la tabla ACRESGRP. Tenga en cuenta que para realizar esta agrupación de recursos basándose en un atributo, el recurso también debe implementar la interfaz Groupable.

El diagrama siguiente muestra un ejemplo de especificación de agrupación de recursos. En este ejemplo, el grupo de recursos `10023` incluye todos los recursos que están asociados a él en la tabla ACRESGPRES. El grupo de recursos `10070` se define utilizando la columna del campo de condiciones de la tabla ACRESGRP. Este grupo de recursos incluye instancias de la interfaz remota Order, que también tienen el estado = `"Z"` (que especifica una lista de solicitudes compartida).

Nota: Para obtener detalles acerca de la información de XML para la columna Conditions de la tabla ACRESGRP, consulte la publicación *WebSphere Commerce, Guía de control de acceso*.

ACRESGRP

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

ACRESGRPES

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

ACRESCGRY

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

Figura 4.

La columna MEMBER_ID de las tablas ACACTGRP, ACRESGRP y ACRELGRP debe tener un valor de `-2001` (Organización raíz).

La política de control de acceso puede incluir opcionalmente un elemento Relación o Grupo de relaciones como cuarto elemento.

Si la política de control de acceso utiliza un elemento Relación, éste procede de la tabla ACRELATION. Si, por otra parte, incluye un elemento Grupo de relaciones, éste procede de la tabla ACRELGRP. Tenga en cuenta que no es necesario incluir ninguno de los dos, pero si incluye uno, no puede incluir el otro. Una especificación de Grupo de relaciones de la tabla ACRELGRP tiene prioridad sobre la información de Relación de la tabla ACRELATION.

La tabla ACRELATION especifica los tipos de relaciones que existen entre los usuarios y los recursos. Los tipos de relaciones incluyen, por ejemplo, creador,

emisor y propietario. Utilizar el elemento de relación para asegurarse de que el creador de un pedido puede actualizar siempre el pedido es un ejemplo de utilización de dicho elemento.

La tabla ACRELGRP especifica los tipos de grupos de relaciones que se pueden asociar con recursos determinados. Un grupo de relaciones es una agrupación de una o más cadenas de relaciones. Una cadena de relaciones es una serie de una o más relaciones. Especificar que un usuario debe ser el creador del recurso y también debe pertenecer a la entidad de organización compradora a la que se hace referencia en el recurso es un ejemplo de grupo de relaciones.

La especificación de grupo de relaciones (o relación) es una parte opcional de la política de control de acceso. Se utiliza normalmente si se han creado mandatos propios y estos mandatos no están restringidos a determinados roles. En estos casos, puede que desee imponer una relación entre el usuario y el recurso. Normalmente, si los mandatos deben restringirse a determinados roles, esto se lleva a cabo mediante el elemento Grupo de usuarios de la política de control de acceso en lugar de realizarse utilizando el elemento Relación.

Otro concepto importante relacionado con las políticas de control de acceso es el concepto de *propietario* de política de control de acceso. Un propietario de política de control de acceso es la entidad de organización que es propietaria de la política de control de acceso. Es importante conocer el propietario de una política de control de acceso porque ésta sólo se puede aplicar a recursos que son propiedad del propietario de política de control de acceso.

Para cada recurso en cuestión, el gestor de políticas de control de acceso aplica las políticas de control de acceso que son propiedad de la entidad de organización propietaria o de las entidades de organización predecesoras en la jerarquía de miembros, hasta que se encuentra una política que otorga el permiso o hasta que se han comprobado todas las políticas y ninguna otorga el permiso.

Examine el diagrama siguiente que muestra una jerarquía de miembros.

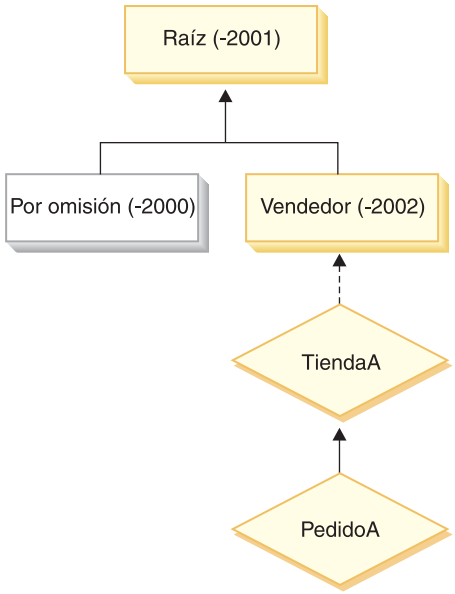


Figura 5.

Para el recurso “PedidoA”, se puede aplicar cualquier política de control de acceso que sea propiedad de la organización Raíz o de Vendedor. Si el gestor de políticas de control de acceso encuentra una política que es propiedad de una de estas organizaciones que otorga el permiso de usuario (basándose en los cuatro elementos de la política de control de acceso), detiene inmediatamente la búsqueda en las políticas de control de acceso. Sin embargo, si no encuentra ninguna política de control de acceso que sea propiedad de esas organizaciones que otorgan el permiso de usuario para realizar la acción en los recursos protegidos, se rechaza el acceso.

Grupos de relaciones

Un grupo de relaciones le permite especificar varias relaciones. Una relación puede ser directamente entre un usuario y el recurso en cuestión o puede ser una cadena de relaciones que relacionan indirectamente el usuario con el recurso.

Nota: En las secciones siguientes relacionadas con los grupos de relaciones, es importante recordar que las únicas organizaciones disponibles en WebSphere Commerce Professional Edition son la Organización raíz, la Organización por omisión y la Organización de vendedor. Los ejemplos que hacen referencia a otras organizaciones sólo se aplican a WebSphere Commerce Business Edition.

Comparación de las relaciones con los grupos de relaciones: Las políticas de control de acceso pueden especificar que un usuario deba satisfacer una relación determinada respecto al recurso al que se está accediendo o pueden especificar que un usuario deba satisfacer las condiciones especificadas en un grupo de relaciones.

En la mayoría de los casos, la especificación de una relación debe satisfacer los requisitos de control de acceso de la aplicación. Sin embargo, si la política es tal que se debe especificar una relación que no es directamente entre el usuario y el recurso, sino que se trata de una serie de relaciones entre el usuario y el recurso, debe utilizar un grupo de relaciones.

Por ejemplo, si debe especificar una asociación entre un usuario y una organización compradora donde la relación requiere que un usuario desempeñe un rol determinado para dicha organización o que el usuario sea miembro de la organización compradora, deberá utilizar un grupo de relaciones y una cadena de relaciones.

Si simplemente necesita imponer una asociación directa entre el usuario y el recurso en cuestión, puede utilizar una relación simple. Por ejemplo, este será el caso si necesita imponer que el usuario sea el creador del recurso.

Si combina varias relaciones simples, por ejemplo, el usuario debe ser el creador *o* el emisor, esto se convertirá en una cadena de relaciones y deberá utilizar un grupo de relaciones. Esta combinación de relaciones simples puede producirse cuando se utiliza WebSphere Commerce Professional Edition o WebSphere Commerce Business Edition.

Información general sobre los grupos de relaciones: Una cadena de relaciones es una serie de una o más relaciones. La longitud de una cadena de relaciones la determina el número de relaciones que contiene. Esto puede determinarse examinando el número de elementos `<parameter name="unNombre" value="unValor" />` en la representación XML de la cadena de relaciones.

El método fulfills() del recurso sólo debe manejar el último elemento <parameter name="Relationship" value="aValue" />. Los restantes los maneja internamente el gestor de políticas de control de acceso.

Cuando una cadena de relaciones tiene una longitud de 2, el primer elemento <parameter name="unNombre" value="unValor" es entre un usuario y una entidad de organización. El último elemento <parameter name="unNombre" value="unValor" es entre una entidad de organización y el recurso.

Si necesita definir grupos de relaciones, deberá realizar dicha acción definiendo la información de grupo de relaciones en un archivo XML. Puede modificar el archivo defaultAccessControlPolicies.xml o crear un archivo XML propio. Para obtener más información sobre cómo crear esta información basada en XML, consulte la publicación *WebSphere Commerce, Guía de control de acceso*.

Las secciones siguientes muestran ejemplos de diferentes tipos de grupos de relaciones.

Grupos de relaciones compuestos por una sola cadena de relaciones: Business Como parte de una política de control de acceso, puede que necesite forzar que un usuario pertenezca a la entidad de organización que es la Entidad de organización compradora del recurso. Para ello es necesario crear un grupo de relaciones que se componga de una cadena de relaciones que tenga una longitud de dos. Se dice que la cadena de relaciones es de longitud ″dos″ porque consta de dos relaciones independientes. La primera relación es entre el usuario y la entidad de organización padre. En dicha relación, el usuario es el ″hijo″. Para la segunda relación, el gestor de políticas de control de acceso comprueba si la entidad de organización padre satisface la relación de BuyingOrganizationalEntity (Entidad de organización compradora) con el recurso. En otras palabras, devuelve ″true″ (verdadero) si es la entidad de organización compradora del recurso.

El siguiente fragmento de XML se ha tomado del archivo defaultAccessControlPolicies.xml y muestra cómo definir este tipo de grupo de relaciones:

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

Business Otro ejemplo sería forzar que el usuario tuviera el rol de Representante de cuentas para la entidad de organización que es la entidad de organización compradora del recurso en cuestión. De nuevo, se utiliza un grupo de relaciones que está compuesto por una cadena de relaciones de longitud dos. La primera parte de la cadena buscará todas las entidades de organización para las que el usuario tiene el rol de Representante de cuentas. Entonces para este conjunto de entidades de organización, el gestor de políticas de control de acceso comprueba si al menos una de ellas satisface la relación BuyingOrganizationalEntity con el recurso. En otras palabras, devuelve ″true″ (verdadero) si una de ellas es la entidad de organización compradora del recurso.

El siguiente fragmento de XML se ha tomado del archivo `defaultAccessControlPolicies.xml` y muestra cómo definir este tipo de grupo de relaciones:

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

Grupos de relaciones compuestos por varias cadenas de relaciones: Es posible componer un grupo de relaciones para que contenga varias cadenas de relaciones. Cuando realice dicha tarea, deberá especificar si el usuario debe satisfacer todas las cadenas de relaciones, lo que significa que se trata de un escenario *AND* (Y), o si el usuario debe satisfacer al menos una de las cadenas de relaciones, lo que significa que es un escenario *OR* (O).

Business Para mostrar este tipo de relación, se utiliza el fragmento siguiente de XML para forzar que el usuario sea el creador del recurso y que el usuario pertenezca también a la Entidad de organización compradora (BuyingOrganizationalEntity) especificada en el recurso. La primera cadena, que especifica que el usuario debe ser el creador del recurso es de longitud uno. La segunda cadena que especifica que el usuario debe pertenecer a la entidad de organización de compradora (BuyingOrganizationalEntity) especificada en el recurso es de longitud dos.

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

Si, en lugar del escenario *AND*, necesita que el usuario satisfaga una de las dos cadenas de relaciones, el código `<andListCondition>` debe cambiarse por el código `<orListCondition>`.

Professional Business Para mostrar un grupo de relaciones que puede utilizarse en WebSphere Commerce Professional Edition (así como en WebSphere Commerce Business Edition), examine un grupo de relaciones que se utiliza para imponer que el usuario sea el creador o el emisor del recurso. Esto se muestra en el fragmento XML siguiente.

```
<RelationGroup Name="Creator_Or_Submitter"
     OwnerID="RootOrganization">
   <RelationCondition><![CDATA [
```

```
   <profile>
      <orListCondition>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="creator"/>
         </openCondition>
         <openCondition name="RELATIONSHIP_CHAIN">
            <parameter name="RELATIONSHIP"value="submitter"/>
         </openCondition>
      </orListCondition>
   </profile>
   ]]></RelationCondition>
</RelationGroup>
```

Tipos de control de acceso

Existen dos tipos de control de acceso y ambos se basan en políticas: control de acceso a nivel de mandatos y control de acceso a nivel de recursos.

El control de acceso a nivel de mandatos (también conocido como “basado en rol”) utiliza un amplio tipo de política. Puede especificar que todos los usuarios de un rol determinado puedan ejecutar determinados tipos de mandatos. Por ejemplo, puede especificar que los usuarios con el rol de Representante de cuentas puedan ejecutar cualquier mandato del grupo de recursos AccountRepresentativesCmdResourceGroup. O, tal como se muestra en el diagrama siguiente, otra política de ejemplo consiste en especificar que todos los administradores de tienda puedan realizar cualquier acción especificada en el grupo ExecuteCommandAction en cualquier recurso especificado por StoreAdminCmdResourceGrp.

Nota: La información XML para la columna Conditions de la tabla MBRGRPCOND se genera al utilizar la Consola de administración para configurar los grupos de acceso. Si desea obtener información sobre cómo utilizar la Consola de administración para configurar grupos de acceso, consulte la ayuda en línea de WebSphere Commerce.

ACPOLICY

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

MBRGRP

MbrGrp_Id	MbrGrpName
-8	StoreAdministrators

MBRGRPCOND

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

ACACTGRP

AcActGrp_Id	GroupName
10052	ExecuteCommandActionGroup

ACRESGRP

AcResGrp_Id	GrpName
10018	StoreAdminCmdResourceGroup

Figura 6.

Una política de control de acceso a nivel de mandatos tiene siempre `ExecuteCommandActionGroup` como grupo de acciones para los mandatos de controlador. Para las vistas, el grupo de recursos es siempre `ViewCommandResourceGroup`.

Todos los mandatos de controlador deben estar protegidos por el control de acceso a nivel de mandatos. Además, cualquier vista que pueda llamarse directamente o que pueda iniciarse mediante un redireccionamiento desde otro mandato (en lugar de iniciarse mediante el reenvío a la vista) debe estar protegida por el control de acceso a nivel de mandatos.

El control de acceso a nivel de mandatos no tiene en cuenta el recurso en el que actuaría el mandato. Simplemente determina si a un usuario se le permite ejecutar el mandato en particular. Si se permite al usuario ejecutar el mandato, se puede aplicar una política de control de acceso a nivel de recursos subsiguiente para determinar si el usuario puede acceder al recurso en cuestión.

Examine una situación en la que un administrador de tienda intenta realizar una tarea administrativa. El primer nivel de comprobación de control de acceso será determinar si a este usuario se le permite ejecutar el mandato de administración de tienda en particular. Una vez que se ha determinado que efectivamente al usuario

se le permite efectuar dicha acción (porque a los administradores de tienda se les permite ejecutar mandatos del grupo storeAdminCmds), se puede invocar una política de control de acceso a nivel de recursos. Puede que esta política determine que a los administradores de tienda sólo se les permite realizar tareas administrativas para las tiendas que son propiedad de la organización de la cual el usuario es un administrador de tienda.

En resumen, en el control de acceso a nivel de mandatos, el "recurso" es el propio mandato y la "acción" consiste simplemente en ejecutar el mandato (en otras palabras, crear una instancia del objeto de mandato). La comprobación de control de acceso determina si se permite al usuario ejecutar el mandato. En cambio, en el control de acceso a nivel de recursos, el "recurso" es cualquier recurso protegido al que accede el mandato o bean y la "acción" es el mandato propiamente dicho.

Interacciones de control de acceso

Este apartado presenta el diagrama de interacciones que muestra cómo funciona el control de acceso en la infraestructura de políticas de control de acceso de WebSphere Commerce.

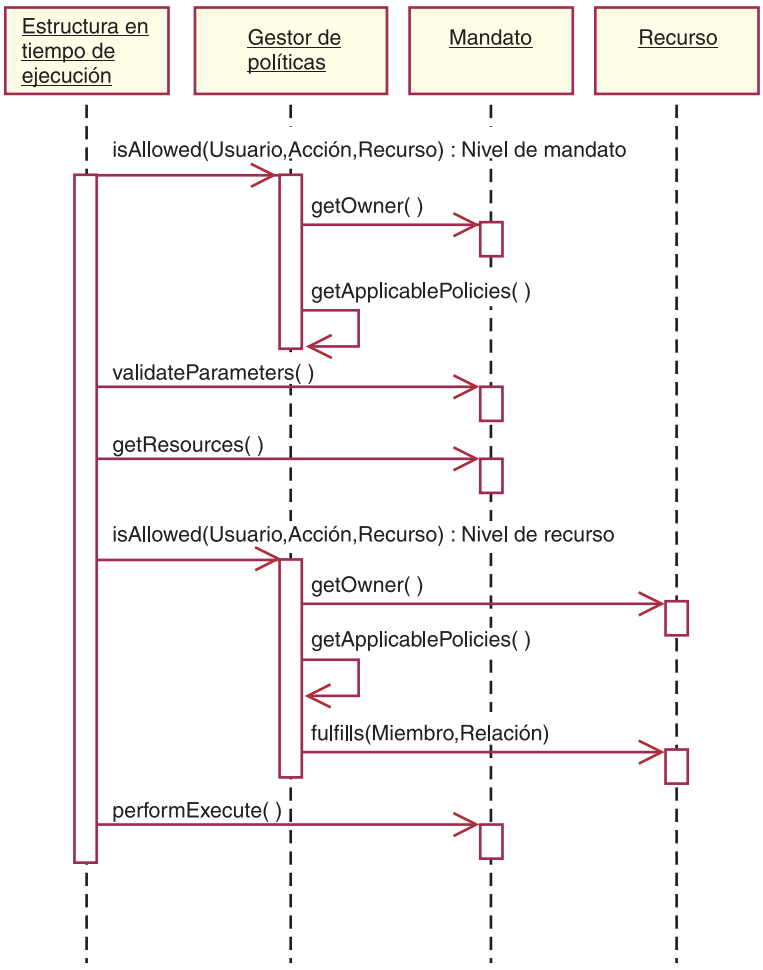


Figura 7.

El diagrama anterior muestra acciones realizadas por el *gestor de políticas* de control de acceso. El gestor de políticas de control de acceso es el componente de control de acceso que determina si al usuario actual se le permite ejecutar la acción

especificada en el recurso especificado. Lo determina buscando en las políticas que son propiedad del propietario del recurso y en las organizaciones predecesoras. Si al menos una política otorga el acceso, se otorga el permiso.

La lista siguiente describe las acciones del diagrama de interacciones anterior. Estas acciones están ordenadas de la parte superior a la parte inferior del diagrama.

1. `isAllowed()`
   Los componentes de ejecución determinan si el usuario tiene acceso a nivel de mandatos para el mandato de controlador o la vista.
2. `getOwner()`
   El gestor de políticas de control de acceso determina el propietario del recurso a nivel de mandatos. La implementación por omisión devuelve el identificador de miembro (`memberId`) del propietario de la tienda (`storeId`) que está en el contexto de mandatos. Si no hay ningún identificador de tienda en el contexto de mandatos, se devuelve la organización raíz (`-2001`).
3. `getApplicablePolicies()`
   El gestor de políticas de control de acceso busca y procesa las políticas aplicables, basándose en la acción y el recurso especificados por el usuario.
4. `validateParameters()`
   Comprobación y resolución de parámetros iniciales
5. `getResources()`
   Devuelve un vector de acceso que es un vector de parejas recurso-acción.

   Si no se devuelve nada, no se realiza la comprobación de control de acceso a nivel de recursos. Si existen recursos que deben protegerse, se debe devolver un vector de acceso (que consta de parejas de recurso-acción).

   Cada *recurso* es una instancia de un objeto protegido (un objeto que implementa la interfaz `com.ibm.commerce.security.Protectable`). En muchos casos, el recurso es un bean de acceso.

   Aunque un bean de acceso puede no implementar la interfaz `com.ibm.commerce.security.Protectable`, la comprobación de control de acceso aún se puede producir a condición de que el bean enterprise correspondiente esté protegido, de acuerdo con la información incluida en el apartado "Implementación del control de acceso en beans enterprise" en la página 109.

   La *acción* es una serie que representa la operación a realizar en el recurso. En la mayoría de los casos, la acción es el nombre de interfaz del mandato.
6. `isAllowed()`
   Los componentes de ejecución determinan si el usuario tiene acceso a nivel de recursos a todas las parejas de recurso-acción especificadas por `getResources()`.
7. `getOwner()`
   El recurso devuelve el `memberId` de su propietario. Esto determina qué políticas se aplican. Sólo se aplican las políticas que son propiedad del propietario de recurso y de las organizaciones predecesoras.
8. `getApplicablePolicies()`
   El gestor de políticas de control de acceso busca las políticas aplicables y, a continuación, las aplica. Si se encuentra como mínimo una política por pareja de recurso-acción que otorga al usuario permiso para acceder al recurso, se otorga el acceso, de lo contrario, se rechaza el acceso.
9. `fulfills()`
   Si una política aplicable tiene especificado un grupo de relaciones, se realiza una comprobación en el recurso para ver si el miembro satisface la relación o las relaciones especificadas, respecto al recurso.

10. `performExecute()`
    Lógica de negocio del mandato.

Interfaz Protectable

Un factor clave para que las políticas de control de acceso de WebSphere Commerce protejan un recurso es que el recurso debe implementar la interfaz `com.ibm.commerce.security.Protectable`. Esta interfaz se utiliza más comúnmente con los beans enterprise y beans de datos, pero sólo los beans concretos que requieren protección necesitan implementar la interfaz.

Con la interfaz Protectable, un recurso debe proporcionar dos métodos clave: `getOwner()` y `fulfills(Long member, String relationship)`.

Las políticas de control de acceso son propiedad de las organizaciones o de las entidades de organización. El método `getOwner` devuelve el Id de miembro del propietario del recurso protegido. Cuando el gestor de políticas de control de acceso ha determinado el propietario del recurso, también obtiene el Id de miembro de cada uno de los predecesores del propietario en la jerarquía de miembros. Entonces se aplican todas las políticas de control de acceso que pertenecen al propietario de la petición getOwner original así como todas las políticas de control de acceso que pertenecen a cualquiera de los predecesores del propietario.

Se aplican las políticas de control de acceso que se aplican al propietario especificado, así como las políticas de control de acceso que se aplican a cualquiera de los predecesores de nivel superior del propietario en la jerarquía de miembros.

El método `fulfills` sólo devuelve true (verdadero) si el miembro en cuestión satisface la relación necesaria respecto al recurso. Normalmente el miembro es un usuario individual, sin embargo también puede ser una organización. Será una organización si está utilizando un grupo de relaciones en la política de control de acceso.

Interfaz Groupable

La aplicación de una política de control de acceso es específica de un grupo de recursos. Las agrupaciones de recursos pueden realizarse basándose en atributos, tales como el nombre de clase, el estado de un pedido o el valor del ID de tienda.

Si un recurso va a agruparse mediante un atributo distinto del nombre de clase con el fin de aplicar políticas de control de acceso, dicho recurso deberá implementar la interfaz `com.ibm.commerce.grouping.Groupable`.

El siguiente fragmento de código representa la interfaz Groupable:

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

Por ejemplo, para implementar una política que sólo se aplica a pedidos que están en estado pendiente (`status = P (pendiente)`), la interfaz remota del bean de entidad Order (Pedido) implementa la interfaz Groupable y el valor para el nombre de atributo se establece en `"status"`.

La utilización de la interfaz Groupable es poco habitual.

Cómo encontrar más información sobre el control de acceso

Para obtener más información sobre el modelo de control de acceso de WebSphere Commerce, consulte la publicación *WebSphere Commerce, Guía de control de acceso*. Esta guía proporciona una visión general detallada del control de acceso y describe cómo utilizar la Consola de administración para crear y modificar políticas, grupos de acciones y grupos de recursos.

Implementación del control de acceso

Este apartado describe cómo implementar el control de acceso en el código personalizado.

Identificación de recursos protegibles

En general, los beans enterprise y los beans de datos son recursos que quizá desee proteger. Sin embargo, no todos los beans enterprise y los beans de datos deben protegerse. En la aplicación de WebSphere Commerce existente, los recursos que necesita protección ya implementan la interfaz protegida (protectable). La pregunta de qué es lo que se debe proteger surge cuando se crean beans enterprise y beans de datos nuevos. La respuesta de qué recursos se deben proteger depende de la aplicación.

Si un mandato devuelve un bean enterprise en el método `getResources`, el bean enterprise debe protegerse porque el gestor de políticas de control de acceso llamará al método getOwner en el bean enterprise. El método `fulfills` también se llamará si se especifica una relación en la política de control de acceso a nivel de recursos correspondiente.

Si tuviera que implementar la interfaz protegida (protectable) (y, por consiguiente, poner el recurso bajo protección) para todos sus propios beans enterprise y beans de datos, la aplicación necesitaría muchas políticas. A medida que aumenta el número de políticas, puede que el rendimiento disminuya y el gestor de políticas se vuelva más exigente.

Se realiza una distinción teórica entre recursos primarios y recursos dependientes. Un *recurso primario* puede existir por sí solo. Un *recurso dependiente* sólo existe cuando existe su recurso primario relacionado. Por ejemplo, en el código de aplicación original de WebSphere Commerce, el bean de entidad Order (Pedido) es un recurso protegido, pero el bean de entidad OrderItem (Artículo de pedido) no lo es. La razón de ello es que la existencia de un Artículo de pedido depende de un Pedido -- Pedido es el recurso primario y Artículo de pedido es un recurso dependiente. Si un usuario debe tener acceso a un Pedido, también debe tener acceso a los artículos del pedido.

De forma similar, el bean de entidad User (Usuario) es un recurso protegido, pero el bean de entidad Address (Dirección) no lo es. En este caso, la existencia de la dirección depende del usuario, de modo que cualquier elemento que tenga acceso al usuario, también debe tener acceso a la dirección.

Los recursos primarios deben estar protegidos, pero los recursos dependientes normalmente no necesitan protección. Si a un usuario se le permite acceder a un recurso primario, tiene sentido que, por omisión, al usuario también se le permita acceder a los recursos dependientes.

Implementación del control de acceso en beans enterprise

Si crea beans enterprise nuevos que necesitan protección mediante políticas de control de acceso, deberá realizar lo siguiente:

1. Cree un bean enterprise nuevo, asegurándose de que se amplía desde `com.ibm.commerce.base.objects.ECEntityBean`.
2. Asegúrese de que la interfaz remota del bean amplía la interfaz `com.ibm.commerce.security.Protectable`.
3. Si los recursos con los que el bean interactúa están agrupados por un atributo distinto del nombre de clase Java del recurso, la interfaz remota del bean también debe ampliar la interfaz `com.ibm.commerce.grouping.Groupable`.
4. La clase de bean enterprise contiene implementaciones por omisión para los métodos siguientes:
   - `getOwner`
   - `fulfills`
   - `getGroupingAttributeValue`

   Altere temporalmente los métodos que necesite. Como mínimo, debe alterar temporalmente el método `getOwner`.
   Las implementaciones por omisión de estos métodos se muestran en los fragmentos de código siguientes.

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

   A continuación se proporcionan implementaciones de ejemplo de estos métodos que se basan en el bean OrderBean:

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

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

5. Cree (o vuelva a crear) el código generado y el bean de acceso del bean enterprise.

Implementación del control de acceso en beans de datos

Si un bean de datos debe estar protegido, puede protegerse directa o indirectamente mediante políticas de control de acceso. Si un bean de datos está protegido directamente, hay una política de control de acceso que se aplica a dicho bean de datos en particular. Si un bean de datos está protegido indirectamente, delega la protección en otro bean de datos, para el que existe una política de control de acceso.

Si crea un bean de datos nuevo que debe estar protegido directamente por una política de control de acceso, el bean de datos debe realizar lo siguiente:

1. Implementar la interfaz `com.ibm.commerce.security.Protectable`. De este modo, el bean debe proporcionar una implementación de los métodos `getOwner()` y `fulfills(Long member, String relationship)`. Estos deben implementarse en la interfaz remota del bean.

   Cuando un bean de datos implementa la interfaz Protectable, el gestor de beans de datos llama al método `isAllowed` para determinar si el usuario tiene los privilegios de control de acceso apropiados, de acuerdo con la política de control de acceso actual. El siguiente fragmento de código describe el método `isAllowed`:

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

2. Si los recursos con los que interactúa el bean están agrupados por un atributo distinto del nombre de clase Java del recurso, el bean debe implementar la interfaz `com.ibm.commerce.grouping.Groupable`.
3. Implementar la interfaz `com.ibm.commerce.security.Delegator`. El siguiente fragmento de código describe esta interfaz:

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

Nota: Para estar directamente protegido, el método `getDelegate` debe devolver el propio bean de datos (es decir el bean de datos delega en sí mismo para realizar el control de acceso).

La distinción entre qué beans de datos deben estar directamente protegidos y cuáles deben estar protegidos indirectamente es similar a la distinción entre recursos primario y secundarios. Si el objeto de bean de datos puede existir por sí mismo, debe estar protegido directamente. Si la existencia del bean de datos depende de la existencia de otro bean de datos, deberá delegar la protección en el otro bean de datos.

El bean de datos Order es un ejemplo de bean de datos que estará protegido directamente. El bean de datos OrderItem es un ejemplo de bean de datos que estará protegido indirectamente.

Si crea un bean de datos nuevos que debe estar protegido indirectamente mediante una política de control de acceso, el bean de datos debe realizar lo siguiente:

1. Implementar la interfaz `com.ibm.commerce.security.Delegator`. El siguiente fragmento de código describe esta interfaz:

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

   Nota: El bean de datos devuelto por `getDelegate` debe implementar la interfaz Protectable.

Si un bean de datos no implementa la interfaz Delegator, se llena de datos sin la protección de políticas de control de acceso.

Implementación del control de acceso en mandatos de controlador

Al crear un mandato de controlador nuevo, la clase de implementación para el nuevo mandato debe ampliar la clase `com.ibm.commerce.commands.ControllerCommandImpl` y su interfaz debe ampliar la interfaz `com.ibm.commerce.command.ControllerCommand`.

Para las políticas a nivel de mandato para los mandatos de controlador, el nombre de interfaz del mandato se especifica como un recurso. Para proteger un recurso, éste debe implementar la interfaz Protectable. Según el modelo de programación de WebSphere Commerce, esto se consigue haciendo que la interfaz de mandatos se amplíe a partir de la interfaz `com.ibm.commerce.command.ControllerCommand` y que la implementación de mandatos se amplíe a partir de `com.ibm.commerce.commands.ControllerCommandImpl`. La interfaz `ControllerCommand` amplía la interfaz `com.ibm.commerce.command.AccCommand` que, a su vez, amplía `Protectable`. La interfaz `AccCommand` es la interfaz mínima que debe implementar un mandato para tener la protección de control de acceso a nivel de mandatos.

Si el mandato accede a recursos que deben estar protegidos, cree una variable de instancia privada de tipo `AccessVector` para que contenga los recursos. A continuación, altere temporalmente el método `getResources` dado que la implementación por omisión de este método va a devolver un valor nulo y, por consiguiente, no se producirá ninguna comprobación de recursos.

En el método getResources nuevo, deberá devolver una matriz de recursos o de parejas de recurso-acción en la que el mandato pueda actuar. Cuando una acción no se especifica explícitamente, la acción toma por omisión el nombre de interfaz del mandato que se está ejecutando.

Adicionalmente, se recomienda que el método determine si debe crear una instancia del recurso o si puede utilizar la variable de instancia existente que contiene la referencia al recurso. La acción de comprobar si ya existe el objeto de recurso puede ayudar a mejorar el rendimiento del sistema. Entonces puede utilizar el mismo método getResources, si es necesario, en el método performExecute del nuevo mandato de controlador.

A continuación se proporciona un ejemplo del método getResources:

```
private AccessVector resources = null;

public AccessVector getResources() throws ECException {

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

Examine el mandato OrderItemUpdate como ejemplo. El método getResources de este mandato devuelve los objetos protegidos Order y User. Dado que no se ha especificado la acción, se toma por omisión la interfaz para el mandato OrderItemUpdate.

Puede que el método getResources devuelva varios recursos. Si ocurre esto, se deberá buscar una política que proporcione al usuario acceso a todos los recursos especificados, si la acción debe llevarse a cabo. Si un usuario tiene acceso a dos de tres recursos, puede que la acción no continúe (sería necesario que fueran tres de tres).

Si necesita realizar una comprobación adicional de parámetros o una resolución de parámetros en el mandato de controlador, puede utilizar el método validateParameters(). Esto es opcional.

Comprobación adicional a nivel de recursos

No siempre es posible determinar todos los recursos que necesitan estar protegidos, en el momento en que se llama al método getResources del mandato de controlador.

Si es necesario, un mandato de tarea también puede implementar un método getResources para devolver una lista de recursos, en los que el mandato puede actuar.

Otro modo de invocar la comprobación a nivel de recursos consiste en realizar llamadas directas al gestor de políticas de control de acceso, utilizando el método checkIsAllowed(Object resource, String action). Este método está disponible para cualquier clase que se amplíe desde la clase com.ibm.commerce.command.AbstractECTargetableCommand. Por ejemplo, las clases siguientes se amplían desde la clase AbstractECTargetableCommand:

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

El método checkIsAllowed también está disponible para las clases que amplían la clase com.ibm.commerce.command.AbstractECCommand. Por ejemplo, la clase siguiente se amplía desde la clase AbstractECCommand:

- com.ibm.commerce.command.TaskCommandImpl

El siguiente ejemplo muestra la signatura del método checkIsAllowed:

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

Este método emite una excepción ECApplicationException si el usuario actual no tiene autorización para efectuar la acción especificada en el recurso especificado. Si se otorga el acceso, el método simplemente emite un retorno.

Control de acceso para mandatos "create"

Dado que en un mandato se llama al método getResources antes que al método performExecute, se deberá utilizar un planteamiento diferente para el control de acceso de recursos que aún no se han creado. Por ejemplo, si tiene WidgetAddCmd, el método getResources no puede devolver el recurso que está a punto de crearse. En este caso, el método getResources debe devolver el creador de los recursos. Por ejemplo una fábrica de mandatos crea un mandato, un pedido se crea en una tienda y un usuario se crea en una organización.

Implementaciones por omisión para el control de acceso a nivel de mandatos

Para el control de acceso a nivel de mandatos, la implementación por omisión del método getOwner() devuelve el Id de miembro del propietario de la tienda, si se especifica el Id de tienda. Si no se especifica el Id de tienda, se devuelve el Id de miembro de la organización raíz (memberId = -2001).

La implementación por omisión del método getResources() devuelve null.

La implementación por omisión de validateParameters() no hace nada.

Implementación de políticas de control de acceso en las vistas

El control de acceso a nivel de recursos para las vistas lo realiza el gestor de beans de datos. El gestor de beans de datos se invoca en los casos siguientes:

1. Cuando la plantilla JSP incluye el código <useBean> y el bean de datos no está en la lista de atributos.
2. Cuando la plantilla JSP incluye el método de activación (activate) siguiente:

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

Nota: Cualquier bean de datos que deba estar protegido (directa o indirectamente) debe implementar la interfaz Delegator. Cualquier bean de datos que deba estar protegido directamente delegará en sí mismo y, por consiguiente, también debe implementar la interfaz Protectable. Los beans de datos que están protegidos indirectamente deben delegar en un bean de datos que implemente la interfaz Protectable.

Aunque no se recomienda, se ignoran las comprobaciones de control de acceso en los casos siguientes:

1. Si la plantilla JSP realiza llamadas directas a beans de acceso, en lugar de utilizar beans de datos.
2. Si la plantilla JSP invoca directamente el método populate() del bean de datos.

Si los resultados de un mandato de controlador deben reenviarse a una vista (utilizando ForwardViewCommand), el control de acceso a nivel de mandatos no se realiza en las vistas. Además, si el mandato de controlador pone los beans de datos llenos (que se utilizan en la vista) en la lista de atributos de la propiedad de respuesta y luego los reenvía a una vista, la plantilla JSP puede acceder a los datos sin pasar por el gestor de beans de datos. Para ello es necesario utilizar los códigos `<useBean>` en la plantilla JSP. Este puede ser un procedimiento para hacer que una plantilla JSP sea más eficiente, puesto que puede ignorar las comprobaciones redundantes de control de acceso a nivel de recursos en los recursos (beans de datos) en los que ya se ha otorgado acceso al usuario a través del mandato de controlador.

Parte 5. Apéndices

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en EE.UU.

Puede que, en otros países, IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Póngase en contacto con su representante de IBM local para obtener información acerca de los productos y servicios disponibles actualmente en su área. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo pueda utilizarse ese producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

Cualquier referencia a un programa bajo licencia de IBM hecha en esta publicación no pretende afirmar ni implicar que sólo se pueda utilizar el programa bajo licencia de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ninguno de los derechos de propiedad intelectual de IBM. La evaluación y verificación del funcionamiento conjunto con otros productos, excepto aquellos expresamente designados por IBM, son responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patente pendientes que cubran el tema principal tratado en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504–1785
EE.UU.

Para realizar consultas sobre licencias relacionadas con la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe sus consultas, por escrito, a:

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

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde tales disposiciones estén en contradicción con la legislación local:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGUNA CLASE, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INFRACCIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UNA FINALIDAD DETERMINADA. Algunas legislaciones no

contemplan la exclusión de garantías, ni implícitas ni explícitas, en determinadas transacciones, por lo que puede haber usuarios a los que no les afecte esta declaración.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información aquí contenida está sometida a cambios periódicos; dichos cambios se incorporarán en nuevas ediciones de la publicación. IBM se reserva el derecho de realizar cambios y/o mejoras, cuando lo considere oportuno y sin previo aviso, en los productos y/o programas descritos en esta publicación.

Todas las referencias hechas en este documento a sitios Web que no son de IBM se proporcionan únicamente para su información y no representan en modo alguno una recomendación de dichos sitios Web. El contenido de esos 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 con el remitente.

Los propietarios de licencias de este programa que deseen obtener información sobre el mismo con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, deberán ponerse en contacto con:

IBM Canada Ltd.
Office of the Lab Director
8200 Warden Avenue
Markham, Ontario
L6G 1C7
Canadá

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, que incluyen en algunos casos el pago de una cantidad.

IBM proporciona el programa bajo licencia descrito en este documento y todo el material con licencia disponible para el mismo bajo los términos del Contrato de cliente de IBM, el Acuerdo internacional de programas bajo licencia de IBM o cualquier acuerdo equivalente entre IBM y el cliente.

Todos los datos de rendimiento incluidos en este documento han sido determinados en un entorno controlado. Por consiguiente, los resultados obtenidos en otros entornos operativos pueden variar de forma significativa. Algunas mediciones pueden haberse realizado en sistemas de nivel de desarrollo y no hay ninguna garantía de que estas mediciones sean las mismas en sistemas de uso general. Asimismo, algunas mediciones se pueden haber estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar qué datos son aplicables a su entorno específico.

La información sobre productos que no son de IBM se ha obtenido de los distribuidores de dichos productos, de los anuncios publicados o de otras fuentes disponibles públicamente. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con productos que no son de IBM. Las preguntas sobre las prestaciones de productos no de IBM deben dirigirse a los distribuidores de dichos productos.

Todas las declaraciones sobre futuras tendencias o intenciones de IBM están sujetas a modificación o retirada sin previo aviso y representan únicamente metas y objetivos.

Esta información se proporciona únicamente con fines de planificación. Está sujeta a posibles cambios antes de que los productos que en ella se describen estén disponibles.

Esta información contiene ejemplos de datos e informes que se utilizan en operaciones comerciales cotidianas. Para ilustrar los ejemplos de la forma más completa posible, éstos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizados en empresas reales es pura coincidencia.

Las imágenes de tarjetas de crédito, las marcas registradas y las marcas que se proporcionan en este producto sólo deberán ser utilizadas por los comerciantes que estén autorizados por el propietario de la marca de la tarjeta de crédito a aceptar el pago a través de dicha tarjeta.

Marcas registradas

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

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

Domino es una marca registrada de Lotus Development Corporation en los Estados Unidos y/o en otros países.

Netscape es una marca registrada de Netscape Communications Corporation en los Estados Unidos y/o en otros países.

Solaris, Solaris Operating Environment, Java, JavaBeans y todas las marcas registradas y los logotipos basados en Java son marcas registradas de Sun Microsystems, Inc.

VeriSign y el logotipo de VeriSign son marcas registradas y marcas de servicio de VeriSign, Inc.

UNIX es una marca registrada de The Open Group en los Estados Unidos y en otros países.

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

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