IBM InfoSphere Information Services Director
Versión 8 Release 7

Guía de publicación de servicios seguros

SC11-8014-00

IBM InfoSphere Information Services Director
Versión 8 Release 7

Guía de publicación de servicios seguros

SC11-8014-00

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información de la sección “Avisos y marcas registradas” en la página 55.

Contenido

Publicación de servicios de seguros

Después de haber diseñado y desplegado un servicio utilizando IBM® InfoSphere Information Services Director, utilice la Consola de IBM InfoSphere Information Server o una herramienta de conjunto para proteger dicho servicio.

Antes de empezar

- Estos temas presuponen que está utilizando IBM InfoSphere Information Server y InfoSphere Information Services Director 8.5 con IBM WebSphere Application Server, Versiones 6.1 o 7.0, en los correspondientes niveles de fixpacks soportados. Para buscar el nivel de fixpack soportado para su versión instalada de WebSphere Application Server, consulte la página de requisitos del sistema IBM InfoSphere Information Server: http://www.ibm.com/software/data/infosphere/info-server/overview/requirements.html

Acerca de esta tarea

- Estas tareas presuponen que está familiarizado con servicios web, SOAP sobre HTTP o SOAP sobre JMS y conceptos de arquitectura orientada a servicios (SOA) y que tiene experiencia con InfoSphere Information Services Director y el entorno de diseño, despliegue y pruebas de servicios utilizando InfoSphere Information Server.
- Los ejemplos para asegurar un servicio desplegado en estas tareas utilizan SOAP sobre un enlace HTTP.
- Muchas de las tareas consisten en modificar archivos descriptores de despliegue de servicios. Puede utilizar una herramienta de conjunto, como IBM Rational Application Developer o IBM WebSphere Application Server Toolkit para manipular estos distintos archivos descriptores. Las tareas de estos temas utilizan Rational Application Developer 7.0 y IBM WebSphere Application Server Toolkit 6.0. La herramienta de conjunto que se utiliza para la mayoría de estos procedimientos es Rational Application Developer, Versión 7.5.4.
  - Rational Application Developer y Rational Software Architect comparten la misma base de código para que Rational Application Developer pueda intercambiarse con Rational Software Architect desde este momento en adelante. Rational Software Architect es un superconjunto de Rational Application Developer y otras ofertas de IBM Rational (Rational Web Developer y Rational Software Modeler, por ejemplo).
  - Entre las distintas herramientas de conjunto de IBM disponibles, Rational Software Architect o Rational Application Developer son los que proporcionan un mejor soporte para la seguridad de servicios web, en concreto, automatizando la mayoría de tareas y resumiendo la mayoría de detalles de seguridad encontrados en los descriptores de despliegue mediante una serie de asistentes. Además de los asistentes, las interfaces de usuario y los editores de Rational Application Developer 7.0 y IBM WebSphere Application Server Toolkit 6.0 son prácticamente idénticos.

Visión general de la seguridad de los servicios web

La seguridad de los servicios web es un estándar del sector que describe cómo se puede aplicar la seguridad específica de la carga útil a los servicios web basados en SOAP estándares.

Nota: Aunque el término "Servicios web" normalmente hace referencia a mensajes con formato SOAP transportados sobre HTTP, este tema describe una serie de estándares denominados Seguridad WS o Seguridad de servicios web. Por ejemplo, la autenticación de la señal de nombre de usuario de Seguridad WS es una de las muchas tecnologías de seguridad que forman parte de los estándares de la Seguridad WS. Algunos mecanismos de seguridad no forman parte de la Seguridad WS, por ejemplo, la autenticación básica HTTP, la autorización J2EE y el cifrado SSL.

La seguridad de los servicios web se basa en otros estándares aceptados tales como la firma digital XML y el cifrado XML, se aprovecha de algoritmos matemáticos, técnicas y activos de software existentes que hace tiempo que se vienen utilizando para la seguridad de la comunicación y de los datos en Internet y otros intercambios seguros más antiguos como transacciones de intercambio electrónico de datos (EDI). La seguridad de servicios web es necesaria porque HTTPS con SSL resulta insuficiente para aplicaciones complejas, especialmente aquellas que requieren flujos de proceso largos con distintos manejadores (aplicaciones) que participan en todo un servicio web “conversación” o actividad.

Un ejemplo de uso habitual es un servicio que abarca toda una solicitud de compra. Puede contener detalles de la tarjeta de crédito previstos para el departamento de facturación, información sobre actualización de la cuenta para el servicio al cliente e información sobre el número de producto para completar un pedido y entregarlo. En un entorno de servicio distribuido, las distintas aplicaciones de la empresa trabajar conjuntamente para proporcionar todo el servicio. Puede ser que sea fundamental que la aplicación de inventario tenga acceso a los detalles de pedido del producto para determinar si el producto deseado está en stock, pero también puede ser que resulte muy importante que la aplicación de inventario no tenga acceso a la información de la cuenta detallada o a los números de tarjeta de crédito. Es importante que las partes implicadas en las interacciones de servicios web puedan validar a la otra parte y asegurar que ninguna de ellas haya alterado el contenido del mensaje mientras éste estaba en tránsito.

La autenticación, la integridad y la confidencialidad son las funciones de seguridad esenciales de la seguridad de servicios web. Otros aspectos de la seguridad tales como una no repudiación, se pueden derivar de las funciones principales en la infraestructura de seguridad de servicios web.

La seguridad, y la seguridad de los servicios web en particular, está cada vez más presente en las discusiones sobre la arquitectura orientada a servicios (SOA) y la información como un servicio. La adopción del estándar de seguridad de los servicios web ha sido lenta por parte de los proveedores y los clientes, pero han pasado varios años ya desde que se confirmó el primer nivel de los estándares de seguridad de servicios web y el interés sigue creciendo. Los motivos de dicha lenta adopción incluyen la complejidad, la preocupación por el rendimiento, la falta de herramientas soportadas por el proveedor, la poca madurez de los estándares (o el miedo a los mismos) y el simple hecho de que para muchas implementaciones de servicios web no se considera necesaria la seguridad de servicios web. HTTPS con SSL ha sido "aceptable" para la mayoría de implementaciones de servicios web punto a punto, y los múltiples saltos complejos, donde la seguridad de los servicios web pasa a ser un imperativo, sigue siendo la herida sangrante de la mayoría de las empresas. Además, existen muchas implementaciones de servicios web de producción detrás de los cortafuegos o no exponga información sensible, pues elimina la necesidad de tener seguridad de servicios web.

Ahora que SOA es más común (al menos en la arquitectura corporativa y en las discusiones de planificación) y los servicios web se prescriben con mayor frecuencia para soluciones de múltiples saltos complejas, donde muchas de las partes "tocan" la carga útil de un mensaje, la seguridad de los servicios web está adquiriendo una mayor importancia. Por ello, la seguridad de los servicios web y la capacidad que tiene IBM InfoSphere Information Services Director para admitirla está en la mente de los arquitectos y los encargados de tomar decisiones tanto desde dentro de IBM como desde fuera.

La seguridad de los servicios web no resulta fácil. Su implementación requiere un alto grado de planificación y disciplina, y la cooperación entre los equipos de despliegue del cliente y del servidor. Ello implica una gran cantidad de reflexiones detalladas acerca de cosas como:

- ¿Qué tipos de seguridad de servicios web necesito y quiero? (autenticación, firmado, cifrado, etc.)
- ¿Qué direcciones? (¿De cliente a host? ¿De host a cliente? ¿Ambas direcciones para todos los tipos de seguridad de servicios web? ¿Reenvío e intermediarios?)
- ¿Qué partes y subpartes de un mensaje? ¿qué tecnologías (X.509, por ejemplo)?

Desde una perspectiva tecnológica, la mayoría de tecnología de ejecución definida por la seguridad de servicios web ya existe. En la seguridad de servicios web se utilizan técnicas probadas por el sector para firmas digitales, algoritmos de cifrado de clave privada y la integración con diversos protocolos. Lo que es nuevo es la sintaxis y las reglas para la definición de la seguridad de servicios web para los motores del solicitante y el proveedor, los nombres de archivo específicos, las ampliaciones y las propiedades personalizadas representadas por cada implementación de proveedor.

Cómo añadir seguridad utilizando la Consola de IBM InfoSphere Information Server

La utilización de IBM InfoSphere Information Services Director en la Consola de IBM InfoSphere Information Server permite añadir la autenticación básica HTTP, la autenticación de señal de nombre de usuario de Seguridad WS o la confidencialidad de datos que utilice el cifrado SSL.

Acerca de esta tarea

Puede añadir seguridad a sus servidores de dos formas: utilizando la Consola de IBM InfoSphere Information Server o utilizando una herramienta de conjuntos. La utilización de la Consola de IBM InfoSphere Information Server es el método preferido porque la Consola de IBM InfoSphere Information Server automatiza algunas tareas.

Cómo añadir una autenticación básica HTTP utilizando la Consola de IBM InfoSphere Information Server

Complete esta tarea para añadir la autenticación básica HTTP al servicio.

Acerca de esta tarea

Esta tarea presupone que el enlace conectado al servicio es SOAP sobre HTTP. La configuración es parecida para otros enlaces como REST, REST 2.0, RSS o EJB.

Procedimiento

1. En el espacio de trabajo Aplicaciones de servicios de información, seleccione una aplicación y pulse **Abrir**.
2. Pulse **Editar**.
3. Efectúe una doble pulsación sobre el servicio que desee proteger con la autenticación básica HTTP.
4. En el panel Visión general de servicio, seleccione **Requiere autenticación** en el panel Seguridad.
5. Pulse el panel Enlaces de servicio.
6. En el menú **Soporte de autenticación**, seleccione **HTTP Basic**.
7. Pulse **Guardar aplicación**.
8. Pulse **Cerrar aplicación**.

Qué hacer a continuación

Debe volver a desplegar el servicio para que estos cambios entren en vigor.

Cuando se añade la autenticación HTTP a un servicio utilizando la Consola de IBM InfoSphere Information Server, IBM InfoSphere Information Services Director añade una regla de autenticación predeterminada que sólo permite que los usuarios con los roles de consumidor, administrador o gestor de catálogos de InfoSphere Information Services Director invoquen las operaciones dentro de dichos servicios.

Cómo añadir la autenticación de señal de nombre de usuario utilizando la Consola de IBM InfoSphere Information Server

Complete esta tarea para añadir la autenticación de señal de nombre de usuario al servicio.

Acerca de esta tarea

Esta tarea presupone que el enlace conectado al servicio es SOAP sobre HTTP.

Procedimiento

1. En el espacio de trabajo Aplicaciones de servicios de información, seleccione una aplicación y pulse **Abrir**.
2. Pulse **Editar**.
3. Efectúe una doble pulsación sobre el servicio que desee proteger con la autenticación de señal de nombre de usuario.
4. En el panel Visión general de servicio, seleccione **Requiere autenticación** en el panel Seguridad.
5. Pulse el panel Enlaces de servicio.
6. En el menú **Soporte de autenticación**, seleccione **Señal de nombre de usuario de seguridad WS**.
7. Pulse **Guardar aplicación**.
8. Pulse **Cerrar aplicación**.

Qué hacer a continuación

Debe volver a desplegar el servicio para que estos cambios entren en vigor.

Cuando se añade la autenticación a un servicio utilizando la Consola de IBM InfoSphere Information Server, IBM InfoSphere Information Services Director añade una regla de autenticación predeterminada que sólo permite que los usuarios con los roles de consumidor, administrador o gestor de catálogos de InfoSphere Information Services Director invoquen las operaciones dentro de dichos servicios.

Cómo añadir confidencialidad de datos de cifrado SSL utilizando la Consola de IBM InfoSphere Information Server

Complete esta tarea para añadir confidencialidad de datos de cifrado SSL a su servicio.

Acerca de esta tarea

Esta tarea presupone que el enlace conectado al servicio es SOAP sobre HTTP. La configuración es parecida para otros enlaces tales como texto sobre HTTP, REST, REST 2.0 o RSS.

Procedimiento

1. En el espacio de trabajo Aplicaciones de servicios de información, seleccione una aplicación y pulse **Abrir**.
2. Pulse **Editar**.
3. Efectúe una doble pulsación sobre el servicio que desee proteger con la confidencialidad de datos de cifrado SSL.
4. En el panel Visión general de servicio, seleccione **Requiere confidencialidad** en el panel Seguridad. Si pulsa el panel Enlaces de servicio, verá qué HTTPS se necesita para invocar este servicio.
5. Pulse **Guardar aplicación**.
6. Pulse **Cerrar aplicación**.

Qué hacer a continuación

El servidor de aplicaciones debe estar configurado para que HTTPS y SSL utilicen un servicio de cifrado SSL.

Cómo añadir seguridad utilizando una herramienta de conjunto

La utilización de una herramienta de conjunto permite añadir autenticaciones, autorizaciones, confidencialidad de datos e integridad de datos.

Acerca de esta tarea

Puede añadir seguridad a sus servidores de dos formas: utilizando la Consola de IBM InfoSphere Information Server o utilizando una herramienta de conjuntos. La utilización de la Consola de IBM InfoSphere Information Server automatiza algunas tareas que deben efectuarse manualmente con una herramienta de conjunto. No obstante, dicha herramienta también permite garantizar un servicios de una forma que no se puede hacer utilizando la Consola de IBM InfoSphere Information Server.

Visión general de la estructura de enlaces

Para habilitar las características de seguridad sin utilizar una aplicación como una herramienta de conjunto, debe comprender la estructura interna básica de los enlaces para modificar sus valores.

Esta sección proporciona una visión general de la estructura interna de dos enlaces populares: SOAP sobre HTTP y SOAP sobre JMS.

SOAP sobre JMS

SOAP sobre JMS es un tipo de enlace que se puede adjuntar a un servicio. Lea este tema para comprender la estructura básica de un SOAP sobre enlace JMS, pues le resultará útil si tiene previsto habilitar valores de seguridad sin utilizar una aplicación como una herramienta de conjunto.

SOAP sobre enlace JMS es el responsable de desordenar las solicitudes SOAP que se envían a través de una cola o tema JMS al servicio, redirigiéndolas a la implementación de servicio de IBM InfoSphere Information Server como llamadas EJB y ordenando la respuesta en un mensaje de SOAP devuelto a la cola o tema JMS.

Un SOAP sobre enlace JMS consiste en los siguientes artefactos:

- Un archivo WSDL que describe el servicio.
- Un bean controlado por mensaje (MDB) de direccionador específico de servidor de aplicaciones (MDB) que escucha las solicitudes SOAP entrantes sobre JMS.
- EJB de sesión sin estado de patrón facade que redirecciona solicitudes a la implementación de servicio de InfoSphere Information Server real, que contiene la lógica empresarial que un cliente pretende invocar.
- Un conjunto de clases de serializador y deserializador que se correlacionan con mensajes SOAP en objetos Java (tipos de WSDL en un tipo de Java, por ejemplo) de acuerdo con las especificaciones de la API de Java para RPC basado en XML.

Estos artefactos se encuentran agrupados en:

- Un JAR de MDB (soapjrouter.jar) que contiene el MDB del direccionador y sus descriptores de despliegue.
- Un JAR de EJB (soapjbinding.jar) que contiene EJB de patrón facade, sus descriptores de despliegue, el archivo WSDL y las clases de serializador y deserializador.

Después de que IBM InfoSphere Information Services Director crea un archivo archivador empresarial (EAR) del servicio antes de su despliegue, InfoSphere Information Server crea y empaqueta los módulos MDB y EJB en el archivo EAR de implementación de servicio cuando se despliega el servicio, tal como se muestra en el diagrama siguiente.

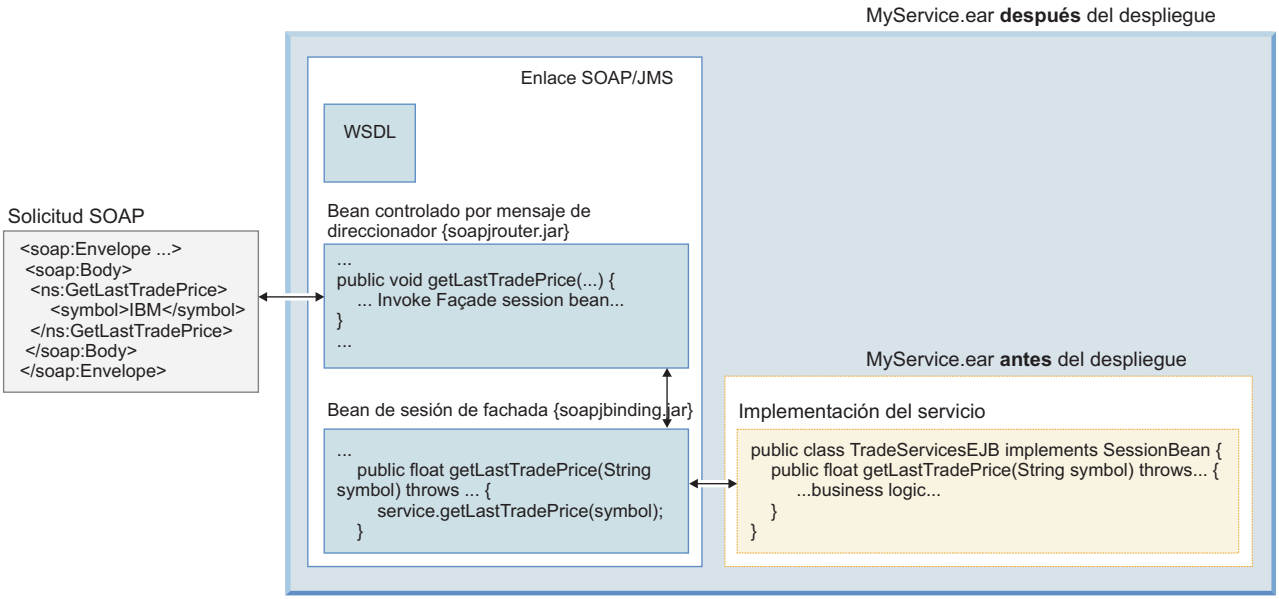

Figura 1. Un servicio desplegado con SOAP sobre enlace JMS

SOAP sobre HTTP

SOAP sobre HTTP es un tipo de enlace que se puede adjuntar a un servicio. Lea este tema para comprender la estructura básica de un SOAP sobre enlace HTTP, pues le resultará útil si tiene previsto habilitar valores de seguridad sin utilizar una aplicación como una herramienta de conjunto.

El SOAP sobre enlace HTTP puede ser visto como un componente de proxy de lado del servidor que se encuentra entre los clientes y los servicios. Es responsable de desordenar las solicitudes SOAP que se envían a través de HTTP al servicio, redireccionándolas a la implementación del servicio de IBM InfoSphere Information Server como llamadas EJB, y ordenar de nuevo la respuesta en un mensaje SOAP enviado a través de HTTP al cliente.

Un SOAP sobre enlace HTTP consiste efectivamente de los siguientes artefactos:

- Un archivo WSDL que describe el servicio.
- Un servlet de direccionador específico de servidor de aplicaciones que escucha las solicitudes SOAP entrantes sobre HTTP.
- EJB de sesión sin estado de patrón facade que redirecciona solicitudes a la implementación de servicio real, que contiene la lógica empresarial que un cliente pretende invocar.
- Un conjunto de clases de serializador y deserializador que se correlacionan con mensajes SOAP en objetos Java (tipos de WSDL en un tipo de Java, por ejemplo) de acuerdo con las especificaciones de la API de Java para RPC basado en XML.

Estos artefactos se encuentran agrupados en:

- Un módulo web (soaprouter.war) que contiene el servlet de direccionador y sus descriptores de despliegue.
- Un JAR EJB (soapbinding.jar) que contiene EJB de patrón facade, sus descriptores de despliegue, el archivo WSDL y las clases de serializador y deserializador.

Después de que IBM InfoSphere Information Services Director crea un archivo archivador empresarial (EAR) del servicio antes de su despliegue, InfoSphere Information Server crea y empaqueta los módulos web y EJB en el archivo EAR de implementación de servicio cuando se despliega el servicio, tal como se muestra en el diagrama siguiente.

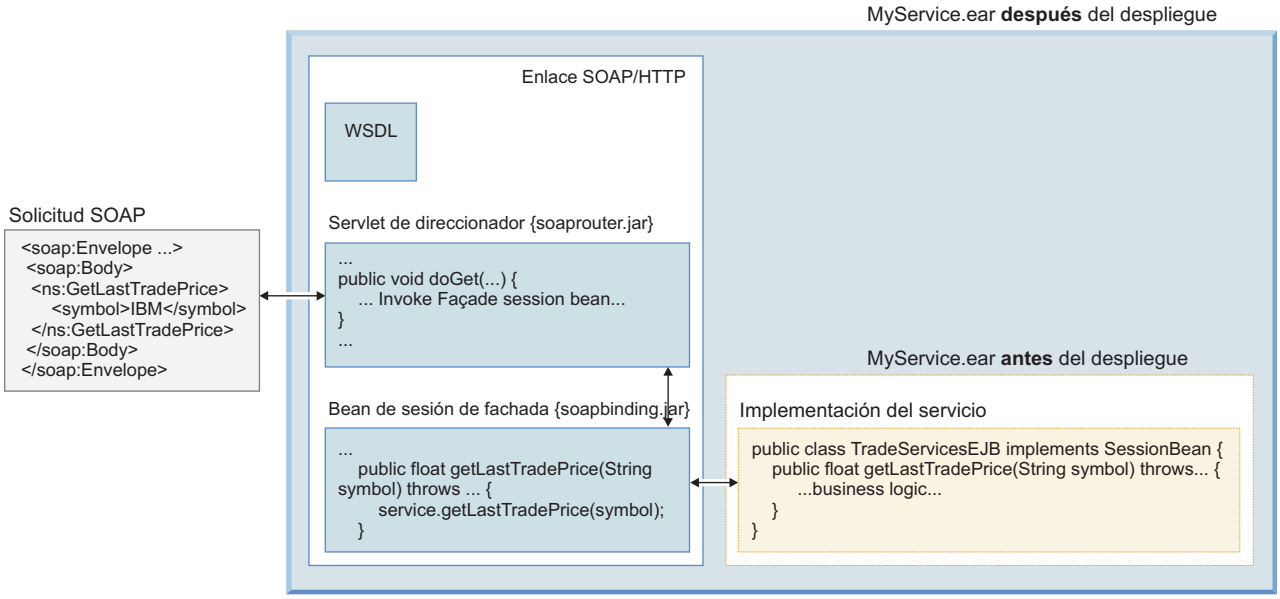

Figura 2. Un servicio desplegado con SOAP sobre enlace HTTP

Configuración de una herramienta de conjunto con IBM InfoSphere Information Server

Para publicar servicios seguros, configure una herramienta de conjunto para que le ayuda a modificar los archivos descriptores para enlaces de servicio.

Acerca de esta tarea

IBM InfoSphere Information Server Versión 8.5 incluye IBM WebSphere Application Server 6.1 o 7.0 y así debe reflejarse en la configuración de la herramienta de conjunto. (Para niveles de fixpack de WebSphere Application Server soportados, consulte la página de requisitos del sistema de IBM InfoSphere Information Server: http://www.ibm.com/software/data/infosphere/info-server/overview/requirements.html.) En concreto, las bibliotecas de tiempo de ejecución de WebSphere Application Server 6.0 o 7.0 deben ponerse a disposición para la herramienta de conjunto. Esto le ahorrará varios errores y avisos cuando importe el archivo EAR de aplicación de InfoSphere Information Server a la herramienta de conjunto y, también evitará errores de ejecución si tiene previsto probar el servicio utilizando un cliente de prueba de proxy generado por la herramienta de conjunto.

El siguiente procedimiento describe cómo configurar IBM Rational Application Developer con IBM WebSphere Application Server, Versión 6.1 o Versión 7.0.Los pasos para configurarIBM WebSphere Application Server Toolkit son los mismos.

Procedimiento

1. En Rational Application Developer, pulse **Ventana** > **Preferencias**.
2. En al lista de preferencias, seleccione **Servidor** > **Tiempos de ejecución instalados**.

3. En la ventana Entornos de ejecución del servidor instalado, pulse **Añadir** para añadir las bibliotecas de ejecución de InfoSphere Information Server.

   La ventana lista ejecuciones de IBM WebSphere Application Server de la versión 6.1 a la versión 7.0. Es posible que algunas bibliotecas de ejecución sean esbozos; otras pueden contener el código de implementación completo, en función de lo que haya seleccionado durante el proceso de instalación de Rational Application Developer.
4. En la ventana Servidor de ejecución nuevo, seleccione **WebSphere Application Server v6.1** o **WebSphere Application Server v7.0** en la carpeta **IBM** y pulse **Siguiente**.
5. En el campo **Nombre**, escriba `Information Server WAS v6.1` o `Information Server WAS v7.0` y el directorio de instalación (por ejemplo, `C:\IBM\WebSphere\AppServer`) para dicha ejecución y pulse **Finalizar**.
6. Pulse **Aceptar** para salir de la ventana Preferencias.

Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server

Antes de detener y exportar un servicio utilizando la consola de IBM WebSphere Application Server, debe inhabilitar la unidad de lógica empresarial (un trabajo de IBM InfoSphere DataStage, por ejemplo) que el servicio contiene. Para inhabilitar el servicio, utilice la Consola de IBM InfoSphere Information Server.

Antes de empezar

- Cree un servicio

Procedimiento

1. Inicie la sesión en la Consola de IBM InfoSphere Information Server y abra el proyecto que contiene el servicio que desea inhabilitar.
2. Seleccione **OPERATE** > **Aplicaciones de servicios de información desplegados**.
3. En el panel Vista, seleccione la aplicación que contiene el servicio que desea inhabilitar.
4. Pulse **Editar**.
5. En la parte inferior del panel Vista, pulse **Inhabilitar** y seleccione **Inhabilitar**.
6. Pulse **Guardar** y **Cerrar**.

Exportación de un servicio utilizando la consola de WebSphere Application Server:

Antes de poder habilitar características de seguridad para un servicio, exporte la aplicación que contenga el servicio para crear un archivo archivador empresarial (EAR). El archivo EAR contiene los archivos descriptores que debe modificar para habilitar características de seguridad como la autenticación.

Antes de empezar

- Cree un servicio
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server"

Procedimiento

1. En WebSphere Application Server, versión 6.1, seleccione **Aplicaciones** > **Aplicaciones empresariales**.

En WebSphere Application Server, versión 7.0, seleccione **Aplicaciones** > **Tipos de aplicaciones** > **Aplicaciones empresariales de WebSphere**.

2. Seleccione la aplicación que contenga el servicio que desea exportar y pulse **Detener**.
3. Seleccione la aplicación de nuevo y pulse **Exportar**.
4. En la ventana Exportar archivos EAR de aplicación, pulse el nombre de la aplicación.
5. Guarde el archivo en un directorio de su sistema.
6. En la ventana Exportar archivos EAR de aplicación, pulse **Atrás** para retroceder a la ventana Aplicaciones empresariales.

Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto

Tras haber inhabilitado el servicio no seguro y haberlo exportado como un archivo de archivador empresarial (EAR), puede utilizar ha herramienta de conjunto para importar el archivo de archivador empresarial (EAR) y habilitar características de seguridad tales como la autenticación, la autorización o la confidencialidad para un servicio.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivo EAR del servicio tal como está descrito en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9

Acerca de esta tarea

Este procedimiento muestra cómo importar un archivo EAR de servicio a IBM Rational Application Developer. Los pasos son parecidos si utiliza IBM WebSphere Application Server Toolkit para importar el archivo EAR de servicio.

Procedimiento

1. En el separador **Explorador de proyectos**, pulse con el botón derecho del ratón y seleccione **Importar** > **Archivo EAR**.
2. En la ventana Importar, pulse **Examinar** para seleccionar la ubicación del archivo EAR.
3. Seleccione un nombre de proyecto.
4. Seleccione el entorno de ejecución de destino que haya especificado al configurar la herramienta de conjunto. Si ha seguido la tarea para configurar Rational Application Developer con InfoSphere Information Server, el entorno de ejecución correcto será **Information Server WAS v6.1** o **Information Server WAS v7.0**.

   Importante: Si selecciona un entorno de ejecución que no sea el seleccionado al configurar la herramienta de conjunto, es posible que el archivo EAR no se importe correctamente.

5. Pulse **Siguiente** para moverse a la ventana siguiente Importar.
6. Pulse **Siguiente** para moverse a la ventana Proyectos de módulo EAR y JAR de programa de utilidad.
7. Pulse **Finalizar**.

Resultados

El archivo EAR se importa a la herramienta de conjunto. Ahora puede visualizar el archivo EAR y los módulos internos, como soapbinding, en el separador **Explorador de proyectos**.

Nota: Puede ignorar el siguiente aviso si se visualiza en el separador **Problemas**: **CHKJ2874W: Migrar este enlace de origen de datos predeterminado del módulo EJB a un enlace de fábrica de conexiones CMP (persistencia gestionada por contenedor) predeterminado**.

Cómo asegurar un servicio

Hay cuatro formas de asegurar un servicio.

Cómo añadir autorizaciones utilizando las restricciones de seguridad J2EE

Añadir autorizaciones como una forma de garantizar un servicio.

Acerca de esta tarea

Para añadir autorizaciones se definen permisos de método de EJB en el descriptor de despliegue de EJB. Puede editar el descriptor de despliegue en el archivo XML o puede utilizar una herramienta de conjunto como IBM WebSphere Application Server Toolkit.

En el modelo de seguridad definido por las especificaciones J2EE, el usuario define permisos de método de EJB de forma factual en el descriptor de despliegue en lugar de definirlos programáticamente en la implementación de servicio.

Por ejemplo, puede restringir el acceso a un servicio únicamente a aquellos usuarios que tengan el rol de administrador de la suite en IBM InfoSphere Information Server. En tal caso, se edita el descriptor de despliegue del bean de sesión de servicio `ejb-jar.xml` para definir roles de seguridad y permisos de método de seguridad.

Cómo añadir restricciones de seguridad J2EE sin utilizar una herramienta de conjunto:

Tal como se define en el modelo de seguridad de especificación J2EE, añada autorización a un servicio editando el descriptor de despliegue EJB. Puede editar el descriptor de despliegue en el archivo XML tal como se describe en esta tarea.

Antes de empezar

- Cree un servicio
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9

- Exporte el servicio para crear un archivo EAR del servicio tal como está descrito en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9

Procedimiento

1. Desempaquete el contenido del archivo *nombreAplicación*.ear en un directorio de trabajo temporal.
2. Edite el descriptor de despliegue del bean de sesión de servicio, *serviceName*.jar#META-INF/ejb-jar.xml y añada los siguientes elementos de seguridad en el elemento **<assembly-descriptor>**.

   security-role
   Este elemento es necesario y puede aparecer varias veces. Declara roles de seguridad que tienen autorización para llamar métodos definidos en estos EJB. Si especifica un rol utilizado por los elementos **<method-permission>**, asegúrese de declararlo en el elemento**<security-role>**. Las definiciones exactas de qué roles pueden invocar qué método EJB se encuentran en el elemento **<method-permission>**.

   description
   Este elemento es un elemento hijo del elemento **<security-role>** y es opcional. Una descripción de texto de este rol de seguridad.

   role-name
   Este elemento es un elemento hijo del elemento **<security-role>** y es necesario. Un nombre de rol al que se le han otorgado permisos para acceder a los EJB.

   method-permission
   Este elemento es necesario y puede aparecer varias veces. Define qué roles pueden invocar qué métodos EJB.

   role-name
   Este elemento es un elemento hijo del elemento **<method-permission>**. Este elemento es opcional y puede aparecer varias veces. Un nombre de rol puede invocar los métodos definidos por los elementos **<method>**. No se puede especificar junto con un elemento**<unchecked>**.

   unchecked
   Este elemento es un elemento hijo del elemento **<method-permission>** y es opcional. Especifica que no se necesita permiso de acceso para invocar los métodos definidos por los elementos **<method>**. No se puede especificar junto con un elemento **<role-name>**.

   method Este elemento es un elemento hijo del elemento **<method-permission>**. Este elemento es necesario y puede aparecer varias veces. Define un método EJB que está sujeto a un permiso de acceso **<role-name>** o **<unchecked>**.

   ejb-name
   Este elemento es un elemento hijo del subelemento **<method>** y es necesario. El nombre de los EJB donde se define este método.

method-name
Este elemento es un elemento hijo del subelemento **<method>** y es necesario. El nombre del método EJB.

Nota: Los elementos necesarios deben tenerse en cuenta en el contexto de la habilitación de la autenticación. Un elemento necesario no es obligatoriamente requerido por el esquema XML `ejb-jar.xml`, pero es necesario para habilitar la autorización.

3. Empaquete de nuevo el descriptor de despliegue editado junto con el resto de archivos sin tratar en el archivo *nombreAplicación*`.ear`.

Ejemplo

El siguiente ejemplo muestra los archivos `web.xml` y `ejb-jar.xml` de SOAP sobre enlace HTTP donde la autenticación básica HTTP (sin ningún cifrado SSL) se ha habilitado para todos los usuarios que no forman parte de los roles usuarioSuite ni adminSuite:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ejb-jar PUBLIC "-//Sun Microsystems, Inc.
//DTD Enterprise JavaBeans 2.0//EN"
"http://java.sun.com/dtd/ejb-jar_2_0.dtd">
<ejb-jar id="ejb-jar_ID">
<description/>
    <display-name>MyApp</display-name>
    <enterprise-beans>
      <session id="MyService">
         <description/>
         <display-name>MyService</display-name>
         <ejb-name>MyService</ejb-name>
         <home>com.ibm.isd.MyApp.MyService.server.MyServiceHome
         </home>

<remote>com.ibm.isd.MyApp.MyService.server.MyServiceRemote
</remote>
         <ejb-class>com.ibm.isd.MyApp.MyService.server.impl.
         MyServiceBean</ejb-class>
         <session-type>Stateless</session-type>
         <transaction-type>Container</transaction-type>
         <resource-ref id="ResRef_MyService_Ref">
           <res-ref-name>jca/AgentConnectionFactory
           </res-ref-name>
           <res-type>com.ascential.asb.agent.ra.ConnectionFactory
           </res-type>
           <res-auth>Application</res-auth>
           <res-sharing-scope>Unshareable</res-sharing-scope>
         </resource-ref>
      </session>
    </enterprise-beans>
    <assembly-descriptor>
      <security-role>
        <role-name>SuiteUser</role-name>
      </security-role>
      <method-permission>
        <role-name>SuiteUser</role-name>
        <method>
          <ejb-name>MyService</ejb-name>
          <method-name>doNothing</method-name>
          <method-params>
            <method-param>int</method-param>
          </method-params>
```

```
        </method>
      </method-permission>
    </assembly-descriptor>
</ejb-jar>
```

Cómo añadir restricciones de seguridad J2EE utilizando una herramienta de conjunto:

Tal como se define en el modelo de seguridad de especificación J2EE, añada autorización a un servicio editando el descriptor de despliegue EJB. Puede editar el descriptor de despliegue en el archivo XML o puede utilizar una herramienta de conjunto. Esta tarea documento el método de la herramienta de conjunto utilizando IBM WebSphere Application Server Server Toolkit.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivo EAR del servicio tal como está descrito en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10

Procedimiento

1. En el separador **Explorador de proyectos**, expanda **Proyectos EJB** > **svcs** y realice una doble pulsación sobre el archivo descriptor de despliegue para editarlo.
2. Pulse **Conjunto**.
3. En la sección **Roles de seguridad**, escriba el nombre del rol (usuarioSuite, por ejemplo) que desea añadir al campo **Nombre** y pulse **Añadir**.
4. En la sección **Permisos de método**, pulse **Añadir**.
5. En la ventana Añadir permiso de método, seleccione el rol de seguridad que desee añadir y pulse **Finalizar**.
6. Pulse **Guardar** para guardar los cambios.

Cómo añadir mecanismos de autenticación

Añadir autenticación como una forma de proteger un servicio.

Acerca de esta tarea

Los métodos de autenticación cubiertos por esta tarea son:

- Señal de seguridad sin firma
- Señal de seguridad con firma
- Autenticación básica HTTP

Cómo añadir señales de seguridad sin firma utilizando el asistente de Seguridad WS:

Una señal de seguridad sin firma que autentica solicitudes de servicio entrantes constituye una forma de proteger un servicio. Normalmente, una señal de seguridad sin firma hace referencia a una señal de nombre de usuario.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10

Acerca de esta tarea

Puede completar esta tarea utilizando el asistente de Seguridad WS o el editor de servicios web. El método Editor de servicios web es el método más manual.El siguiente procedimiento describe cómo añadir una señal de nombre de usuario a su servicio utilizando el asistente de Seguridad WS.

Procedimiento

1. Cambie a la **Perspectiva Java EE**.
2. En el separador **Explorador de proyectos**, expanda el módulo **soapbinding** del servicio que ha importado y luego expanda **Servicios**.
3. Pulse con el botón derecho del ratón el servicio y seleccione **Servicio web seguro** > **Añadir señal de seguridad autónoma**.
4. En la ventana Asistente de Seguridad WS - Señal de nombre de usuario autónoma del lado del servidor, seleccione el tipo de señal **Señal de nombre de usuario**.
5. Seleccione el nombre de configuración JAAS **system.wssecurity.UsernameToken**. Este nombre indica que las solicitudes de inicio de sesión entrantes serán procesadas por la pila de módulos de inicio de sesión definida en la configuración de inicio de sesión JAAS `system.wssecurity.UsernameToken`.
6. Pulse **Finalizar**.
7. Para validar que los descriptores de despliegue del servicio se han actualizado correctamente, en el separador **Explorador de proyectos**, expanda **soapbinding** > **Servicios** y pulse con el botón derecho del ratón el servicio. Seleccione **Mostrar** y, a continuación, pulse **Descriptor de despliegue**. Se abre el editor de servicios web.
8. Pulse el separador **Ampliaciones** para verificar que se haya creado una señal de nombre de usuario en **Detalles de configuración de enlace de consumidor de solicitudes** > **Señal de seguridad necesaria**.

9. Pulse el separador **Enlaces** para verificar que se haya creado una señal de nombre de usuario en **Detalles de configuración de enlace de consumidor de solicitudes** > **Consumidor de señales**.

Cómo añadir señales de seguridad sin firma utilizando el editor de servicios web:

Una señal de seguridad sin firma que autentica solicitudes de servicio entrantes constituye una forma de proteger un servicio. Normalmente, una señal de seguridad sin firma hace referencia a una señal de nombre de usuario.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10

Acerca de esta tarea

Puede completar esta tarea utilizando el asistente de Seguridad WS o el editor de servicios web. El método Editor de servicios web es el método más manual.Este procedimiento describe cómo añadir una señal de nombre de usuario a su servicio utilizando el editor de servicios web.

Procedimiento

1. En el separador **Explorador de proyectos** de Rational Application Developer, expanda **soapbinding** > **ejbModule** > **META-INF** y efectúe una doble pulsación sobre el archivo descriptor **webservice.xml**.
2. Pulse el separador **Ampliaciones** en el editor de servicios web.
3. Expanda **Ampliación de descripción de servicio web** y seleccione la descripción del servicio.
4. Expanda **Enlace de componente de puerto** y seleccione el enlace de su servicio.
5. Expanda **Detalles de de configuración de enlace de consumidor de solicitudes** > **Señal de seguridad necesaria**.
6. Pulse **Añadir**.
7. En la ventana Señal de seguridad necesaria, seleccione el tipo de señal **Señal de nombre de usuario** y complete el resto de campos.
8. Pulse **Aceptar**. La señal de nombre de usuario se visualiza en **Detalles de de configuración de enlace de consumidor de solicitudes** > **Señal de seguridad necesaria**.
9. Pulse el separador **Configuraciones de enlaces** y expanda **Consumidor de señales**.

10. Pulse **Añadir**.
11. En la ventana **Consumidor de señales**, complete los campos Nombre, Clase, Señal de seguridad, Tipo de valor y URI. Asegúrese de que selecciona la señal de seguridad creada recientemente en la lista desplegable **Señal de seguridad**. Asegúrese también de que selecciona el recuadro de selección **Utilizar jaas.config** y especifique `system.wssecurity.UsernameToken` en el campo **jaas.config name**. Para los otros campos, puede utilizar los valores predeterminados.
12. Pulse **Aceptar**. El consumidor de señal se visualiza en **Detalles de configuración de enlace de consumidor de solicitudes** > **Consumidor de señales**.

Cómo añadir señales de seguridad utilizando el editor de servicios web:

Una señal de seguridad con firma que autentica las solicitudes de servicio entrantes de una forma para asegurar un servicio.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10

Acerca de esta tarea

Los ejemplos de señales de seguridad con firma son señales de ticket de Kerberos, señales de certificado X.509 o señales de Lightweight Third Party Authentication (LTPA). En este procedimiento, IBM Rational Application Developer se utiliza para ilustrar la definición de una señal de certificado X.509 como mecanismo de autenticación para solicitudes de servicio entrantes.

Procedimiento

1. En el separador **Explorador de proyectos** de Rational Application Developer, expanda **soapbinding** > **ejbModule** > **META-INF** y efectúe una doble pulsación sobre el archivo descriptor `webservice.xml`.
2. Pulse el separador **Ampliaciones** en el editor de servicios web.
3. Expanda **Ampliación de descripción de servicio web** y seleccione la descripción del servicio.
4. Expanda **Enlace de componente de puerto** y seleccione el enlace de su servicio.
5. Expanda **Detalles de de configuración de enlace de consumidor de solicitudes** > **Señal de seguridad necesaria**.
6. Pulse **Añadir**.

7. En la ventana Señal de seguridad necesaria, seleccione el tipo de señal **Señal de certificado X509** y complete el resto de campos.
8. Pulse **Aceptar**. La señal de certificado X509 se visualiza en **Detalles de configuración de enlace de consumidor de solicitudes** > **Señal de seguridad necesaria**.
9. Pulse el separador **Configuraciones de enlaces** y expanda **Consumidor de señales**.
10. Pulse **Añadir**.
11. En la ventana **Consumidor de señales**, complete los campos Nombre, Clase, Señal de seguridad, Tipo de valor y URI. Los otros campos se pueden dejar con sus valores predeterminados.
12. Pulse **Aceptar**. El consumidor de señal aparece en **Detalles de configuración de enlace de consumidor de solicitudes** > **Consumidor de señales**.

Cómo añadir autenticación básica HTTP sin utilizar una herramienta de conjunto:

Utilice el método de autenticación básica HTTP para proteger un servicio dentro de una red segura como HTTPS o una intranet. Para habilitar la autenticación básica HTTP, edite descriptores de despliegue J2EE definidos en el módulo de enlaces SOAP.

Antes de empezar

- Cree un servicio
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivo EAR del servicio tal como está descrito en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9

Acerca de esta tarea

Para añadir autenticación a un servicio, edite el descriptor de despliegue EJB. Puede editar el descriptor de despliegue en el archivo XML o puede utilizar una herramienta de conjunto como IBM Rational Application Developer.

Procedimiento

1. Desempaquete el contenido del archivo EAR en un directorio de trabajo temporal.
2. Edite el descriptor de despliegue de web de servlet de direccionador, `soaprouter.war#WEB-INF/web.xml` y añada los siguientes elementos de seguridad bajo el elemento raíz **<web-app>**.

   security-constraint
   Este elemento es necesario. Define los privilegios de acceso a una recopilación de recursos web definida por el subelemento **<web-resource-collection>**.

   web-resource-collection
   Este elemento es un elemento hijo del elemento **<security-constraint>** y es necesario. Define los componentes de la aplicación web a la que se aplica esta restricción de seguridad.

web-resource-name
Este elemento es un elemento hijo del subelemento **<web-resource-collection>** y es necesario. Define el nombre de esta recopilación de recursos web.

description
Este elemento es un elemento hijo del subelemento **<web-resource-collection>** y es opcional. Una descripción de texto de esta recopilación de recursos web.

url-pattern
Este elemento es un elemento hijo del subelemento **<web-resource-collection>** y es necesario. Define a qué patrones URL se aplica esta restricción de seguridad. En el caso del servlet de direccionador SOAP, debería utilizarse el patrón de URL /*. El asterisco (*) sólo no es válido.

http-method
Este elemento es un elemento hijo del subelemento **<web-resource-collection>**. Este elemento es opcional y puede aparecer varias veces. Utilice uno o varios de los elementos **<http-method>** para declarar qué métodos HTTP (GET o POST, por ejemplo) están sujetos a la restricción de seguridad. De forma predeterminada, se aplica a todos los métodos HTTP. En el caso del servlet de direccionador SOAP/HTTP, las solicitudes se realizan utilizando el método POST. Si especifica el elemento **<http-method>**, asegúrese de que se liste el método POST. Para proteger el archivo WSDL, asegúrese de especificar también el método GET.

auth-constraint
Este elemento es un elemento hijo del elemento **<security-constraint>** y es necesario. Define qué grupos o principales tienen acceso a la colección de recursos web definidos en esta restricción de seguridad.

description
Es un elemento hijo del subelemento **<auth-constraint>** y es opcional. Una descripción de texto de esta restricción de seguridad.

role-name
Este elemento es un elemento hijo del subelemento **<auth-constraint>**. Este elemento es necesario y puede aparecer varias veces. Define qué roles de seguridad pueden acceder a los recursos definidos en esta restricción de seguridad (usuarioSuite o adminSuite, por ejemplo). Reproduce los roles que se han definido para la implementación de servicio.

user-data-constraint
Este elemento es un elemento hijo del elemento **<security-constraint>** y es opcional. Define cómo se comunica el cliente con el servidor. Normalmente se utiliza para habilitar SSL.

description
Este elemento es un elemento hijo del subelemento **<user-data-constraint>** y es opcional. Una descripción de texto de esta restricción de datos de usuario.

transport-guarantee
Este elemento es un elemento hijo del subelemento **<user-data-constraint>** y es opcional. Especifica el tipo de restricción de seguridad que debe imponerse en los datos transferidos entre cliente y servidor:

- NONE (sin restricción)
- INTEGRAL (integridad de datos)
- CONFIDENTIAL (que básicamente es SSL)

login-config
Este elemento es necesario. Define cómo se autentica un usuario.

auth-method
Este elemento es un elemento hijo del elemento **<login-config>** y es necesario. Especifica el método utilizado para autenticar un usuario. En este caso, sólo se establece en BASIC.

realm-name
Este elemento es un elemento hijo del elemento **<login-config>** y es opcional. Este elemento es opcional. El nombre del reino al que se hace referencia para autenticar credenciales de usuario.

security-role
Este elemento es necesario y puede aparecer varias veces. Declare roles de seguridad. Sólo debería haber un elemento **<security-role>** para cada rol listado bajo el elemento **<auth-constraint>**.

description
Este elemento es un elemento hijo del elemento **<security-role>** y es opcional. Una descripción de texto de este rol de seguridad.

role-name
Este elemento es un elemento hijo del elemento **<security-role>** y es necesario. Un nombre de rol al que se han otorgado algunos permisos en este módulo web.

Nota: Los elementos necesarios deben tenerse en cuenta en el contexto de la habilitación de la autenticación básica HTTP. Un elemento necesario no es necesariamente requerido por el esquema XML `web.xml`, pero sí que es necesario para habilitar la autenticación básica HTTP.

3. Edite el descriptor de despliegue EJB de enlace `soapbinding.jar#META-INF/ejb-jar.xml` y añada los siguientes elementos de seguridad bajo el elemento **<assembly-descriptor>**.

security-role
Este elemento es necesario y puede aparecer varias veces. Declara roles de seguridad que tienen autorización para llamar métodos definidos en estos EJB. Si especifica un rol utilizado por los elementos **<method-permission>**, asegúrese de declararlo en el elemento**<security-role>**. Las definiciones exactas de qué roles pueden invocar qué método EJB se encuentran en el elemento **<method-permission>**.

description
Este elemento es un elemento hijo del elemento **<security-role>** y es opcional. Una descripción de texto de este rol de seguridad.

role-name
Este elemento es un elemento hijo del elemento **<security-role>** y es necesario. Un nombre de rol al que se le han otorgado permisos para acceder a los EJB.

method-permission
Este elemento es necesario y puede aparecer varias veces. Define qué roles pueden invocar qué métodos EJB.

role-name
Este elemento es un elemento hijo del elemento **<method-permission>**. Este elemento es opcional y puede aparecer varias veces. Un rol que puede invocar los métodos definidos por los elementos **<method>**. No se puede especificar junto con un elemento**<unchecked>**.

unchecked
Este elemento es un elemento hijo del elemento **<method-permission>** y es opcional. Especifica que no se necesita permiso de acceso para invocar los métodos definidos por los elementos **<method>**. No se puede especificar junto con un elemento **<role-name>**.

method Este elemento es un elemento hijo del elemento **<method-permission>**. Este elemento es necesario y puede aparecer varias veces. Define un método EJB que está sujeto a un permiso de acceso **<role-name>** o **<unchecked>**.

ejb-name
Este elemento es un elemento hijo del subelemento **<method>** y es necesario. El nombre de los EJB donde se define este método.

method-name
Este elemento es un elemento hijo del subelemento **<method>** y es necesario. El nombre del método EJB.

Nota: Los elementos necesarios deben tenerse en cuenta en el contexto de la habilitación de la autenticación básica HTTP. Un elemento necesario no es necesariamente requerido por el esquema XML `web.xml`, pero sí que es necesario para habilitar la autenticación básica HTTP.

4. Empaquete de nuevo los descriptores de despliegue editados junto con el resto de archivos sin tratar en el archivo *nombreAplicación*`.ear`.

Ejemplo

El siguiente ejemplo muestra los archivos `web.xml` y `ejb-jar.xml` de SOAP sobre enlace HTTP donde la autenticación básica HTTP (sin ningún cifrado SSL) se ha habilitado para todos los usuarios que no forman parte de los roles usuarioSuite ni adminSuite:

Ejemplo de archivo`web.xml`

```
soaprouter.jar#WEB-INF/web.xml
<?xml version="1.0" encoding="UTF-8" ?>
<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd" id="WebApp_ID" version="2.4">
  <display-name>MyAppSOAPBinding_HTTPRouter</display-name>
  <servlet>
    <display-name>Web services Router servlet for port-componentMyServiceSOAP
    </display-name>
    <servlet-name>MyServiceSOAP</servlet-name>
    <servlet-class>com.ibm.ws.webservices.engine.transport.http.WebServicesServlet
    </servlet-class>
  </servlet>
  <servlet-mapping>
    <servlet-name>MyServiceSOAP</servlet-name>
    <url-pattern>MyService</url-pattern>
  </servlet-mapping>
  <security-constraint>
    <display-name>SoapRouterConstraints</display-name>
    <web-resource-collection>
      <web-resource-name>SecuredSoapRouterServlet</web-resource-name>
      <url-pattern>/*</url-pattern>
      <http-method>GET</http-method>
      <http-method>POST</http-method>
    </web-resource-collection>
    <auth-constraint>
      <description>Authorized roles</description>
      <role-name>SuiteUser</role-name>
      <role-name>SuiteAdmin</role-name>
    </auth-constraint>
    <user-data-constraint>
      <transport-guarantee>NONE</transport-guarantee>
    </user-data-constraint>
  </security-constraint>
  <login-config>
    <auth-method>BASIC</auth-method>
  </login-config>
  <security-role>
    <role-name>SuiteUser</role-name>
  </security-role>
  <security-role>
    <role-name>SuiteAdmin</role-name>
  </security-role>
</web-app>
```

Ejemplo de archivo ejb-jar.xml

```
soapbinding.jar#META-INF/ejb-jar.xml
<?xml version="1.0" encoding="UTF-8" ?>
<ejb-jar xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" id="ejb-jar_ID"
version="2.1" xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/ejb-jar_2_1.xsd">
  <enterprise-beans>
    <session id="MyServiceSOAP">
      <description></description>
      <ejb-name>MyServiceSOAP</ejb-name>
      <home>com.ibm.isd.MyApp.MyService.server.MyServiceHome
      </home>
      <remote>com.ibm.isd.MyApp.MyService.server.MyServiceRemote
      </remote>
      <service-endpoint>com.ibm.isd.MyApp.MyService.MyService
      </service-endpoint>
      <ejb-class>com.ibm.isd.MyApp.MyService.MyServiceSOAPBindingBean
      </ejb-class>
      <session-type>Stateless</session-type>
```

```
    <transaction-type>Container</transaction-type>
    <ejb-ref id="EjbRef_MyService_Ref">
      <ejb-ref-name>ejb/MyService</ejb-ref-name>
      <ejb-ref-type>Session</ejb-ref-type>
      <home>com.ibm.isd.MyApp.MyService.server.MyServiceHome</home>
      <remote>com.ibm.isd.MyApp.MyService.server.MyServiceRemote</remote>
    </ejb-ref>
  </session>
</enterprise-beans>
  <assembly-descriptor>
    <security-role>
      <role-name>SuiteUser</role-name>
    </security-role>
    <security-role>
      <role-name>SuiteAdmin</role-name>
    </security-role>
    <method-permission>
      <role-name>SuiteUser</role-name>
      <role-name>SuiteAdmin</role-name>
      <method>
        <ejb-name>MyServiceSOAP</ejb-name>
        <method-intf>Remote</method-intf>
        <method-name>doNothing</method-name>
        <method-params>
        <method-param>int</method-param>
        </method-params>
      </method>
    </method-permission>
    <method-permission>
      <unchecked/>
      <method>
        <ejb-name>MyServiceSOAP</ejb-name>
        <method-intf>Home</method-intf>
        <method-name>create</method-name>
        <method-params>
        </method-params>
      </method>
      <method>
        <ejb-name>MyServiceSOAP</ejb-name>
        <method-intf>Home</method-intf>
        <method-name>remove</method-name>
      </method>
    </method-permission></assembly-descriptor>
  </assembly-descriptor>
</ejb-jar>
```

Cómo añadir autenticación básica HTTP utilizando una herramienta de conjunto:

Utilice el método de autenticación básica HTTP para proteger un servicio dentro de una red segura como HTTPS o una intranet. Para habilitar la autenticación básica HTTP, edite descriptores de despliegue J2EE definidos en el módulo de enlaces SOAP.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en “Configuración de una herramienta de conjunto con IBM InfoSphere Information Server” en la página 8
- Inhabilite el servicio no seguro tal como está descrito en “Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server” en la página 9

- Exporte el servicio para crear un archivo EAR del servicio tal como está descrito en “Exportación de un servicio utilizando la consola de WebSphere Application Server:” en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en “Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto” en la página 10

Acerca de esta tarea

Para añadir autenticación a un servicio, edite el descriptor de despliegue EJB. Puede editar el descriptor de despliegue en el archivo XML, o puede utilizar una herramienta de conjunto como IBM Rational Application Developer, según se describe en este procedimiento.

Procedimiento

1. En el separador **Explorador de proyectos**, expanda el módulo **soaprouter**.
2. Efectúe una doble pulsación en el archivo descriptor de despliegue para editarlo.
3. Pulse el separador **Páginas**.
4. En la sección **Iniciar sesión**, seleccione **Método de autenticación** > **BASIC** y guarde el cambio.
5. Pulse el separador **Seguridad**.
6. En la sección **Roles de seguridad**, escriba el nombre del rol que desea añadir en el campo **Nombre** y pulse **Añadir**.
7. En la sección **Restricciones de seguridad**, pulse **Añadir**.

   Efectúe las restricciones de seguridad para la autenticación de forma que sean las mismas que las restricciones de seguridad que defina cuando añada autorización a un servicio.
8. Escriba un nombre para la restricción y pulse **Siguiente**.
9. Escriba un nombre de recurso web, seleccione **POST** y **GET** para el **método HTTP** y añada `/*` al campo **Patrón**. A fin de proteger el servicio WSDL, debe proteger el método HTTP GET.
10. Pulse **Finalizar**.
11. En la sección **Roles autorizados**, pulse **Añadir**.
12. Seleccione el **Nombre de rol** que haya añadido a la sección **Roles de seguridad** y pulse **Finalizar**.
13. En la sección **Restricción de datos de usuario**, seleccione **NONE** y guarde los cambios. Esta restricción sólo se utiliza para conexiones SSL.
14. En la sección **Proyectos EJB** del separador **Project Explorer** expanda el módulo **soapbinding**.
15. Efectúe una doble pulsación en el archivo descriptor de despliegue EJB para editarlo.
16. Pulse el separador **Conjunto**.
17. En la sección **Roles de seguridad**, pulse **Añadir** y escriba el mismo nombre de rol que haya añadido en el descriptor de despliegue web.
18. En la sección **Permisos de método**, pulse **Añadir**.
19. En la ventana Permiso de método, seleccione el rol de seguridad y pulse **Siguiente**.

20. En la ventana Selección de enterprise bean, seleccione el enterprise bean para el servicio y pulse **Siguiente**.
21. En la ventana Elementos de método, seleccione los métodos que desee proteger. En una situación típica, seleccione todos los métodos.
22. Pulse **Finalizar** y guarde los cambios.

Cómo añadir confidencialidad de datos utilizando el cifrado SSL

Cómo añadir confidencialidad de datos como una forma de garantizar un servicio.

Acerca de esta tarea

Añada confidencialidad utilizando el protocolo de capa de sockets seguros (SSL). Complete esta tarea para habilitar SSL en el lado del servidor del servicio. A continuación debe realizar los mismos cambios en la configuración en el lado del cliente. Por ejemplo, si cambia la configuración del lado del servidor para que utilice el protocolo de Seguridad de la Capa de Transporte (Transport Secure Layer - TSL) en lugar de SSL, también deberá configurar el cliente para que utilice TSL.

EL protocolo SSL se basa en la infraestructura de claves públicas (public key infrastructure - PKI). Como tal, las claves privadas y públicas para el cliente y el deben estar generadas y almacenadas, respectivamente, en almacenes de claves y tiendas de confianza para que la conexión SSL pueda completarse. Esta tarea utiliza almacenes de clave de muestra y certificados autofirmados. Sólo utilice almacenes de claves de muestra para realizar pruebas. En un entorno de producción real, implemente su propia infraestructura de claves públicas.

A continuación encontrará una visión general del proceso de habilitación de SSL:

- El cliente autentica el servidor después de que se haya iniciado una sesión. Esta autenticación se denomina "protocolo de reconocimiento SSL". De forma opcional, el cliente también puede autenticarse en el servidor.
- Si el reconocimiento SSL es satisfactorio, a continuación se inicia y se cifra la transferencia de datos. Esto se llama el protocolo de informe SSL.
- Si se han generado alarmas en algún momento durante la sesión, se encía un paquete de alertas al destinatario adecuado. Este paquete de alertas se denomina "protocolo de alertas SLL".

La siguiente tarea describe cómo añadir datos de forma confidencial utilizando el cifrado SSL:

Configuración de un servicio para que utilice el cifrado SSL:

Después de crear un repertorio de capa de sockets seguros (SSL) dentro de IBM WebSphere Application Server, complete esta tarea para habilitar SSL en el lado del servidor del servicio. A continuación debe realizar los mismos cambios en la configuración en el lado del cliente. Por ejemplo, si cambia la configuración del lado del servidor para que utilice el protocolo de Seguridad de la Capa de Transporte (Transport Secure Layer - TSL) en lugar de SSL, también deberá configurar el cliente para que utilice TSL.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en “Configuración de una herramienta de conjunto con IBM InfoSphere Information Server” en la página 8

- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivo EAR del servicio tal como está descrito en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10

Procedimiento

1. En el separador **Explorador de proyectos** de IBM Rational Application Developer, expanda **soaprouter** y efectúe una doble pulsación sobre el descriptor de despliegue para editarlo.
2. Seleccione el separador **Seguridad**.
3. En la sección **Restricciones de seguridad**, pulse **Añadir**.
4. Introduzca un nombre para la restricción en la página **Añadir restricciones** y pulse **Siguiente**.
5. Introduzca un nombre para el recurso en la página **Añadir recurso web**.
6. Seleccione un método HTTP de la lista **Métodos HTTP**. Como mínimo seleccione el método POST para proteger su servicio. Si no desea que la restricción de seguridad se aplica al archivo lenguaje de descripción de servicios web (Web Services Description Language - WSDL), no seleccione el método GET.
7. Añada `/*` al campo **Patrón** para especificar el patrón de URL que se aplica a la restricción de seguridad.
8. Pulse **Finalizar**.
9. En la sección **Restricción de datos de usuario**, seleccione **CONFIDENTIAL** en el campo **Tipo**.
10. Guarde los cambios.

Qué hacer a continuación

Cómo añadir integridad de datos

Añadir integridad de datos utilizando la firma digital XML como una forma de garantizar un servicio.

Acerca de esta tarea

Visión general del proceso de firma digital:

- El cliente (remitente) firma partes del mensaje de solicitud utilizando una clave privada. La clave privada del cliente se almacena en el almacén de claves del cliente.
- El servidor (receptor) valida las firmas digitales del cliente en el mensaje de solicitud utilizando la clave pública del cliente. La clave pública del cliente se almacena en el almacén de claves del servidor.

Cómo añadir una firma digital XML:

Para añadir integridad de datos al servicio utilizando una firma digital XML, edite el archivo descriptor de despliegue utilizando una herramienta de conjunto como IBM Rational Application Developer.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en “Configuración de una herramienta de conjunto con IBM InfoSphere Information Server” en la página 8
- Inhabilite el servicio no seguro tal como está descrito en “Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server” en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en “Exportación de un servicio utilizando la consola de WebSphere Application Server:” en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en “Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto” en la página 10

Acerca de esta tarea

Restricciones

En esta tarea va a utilizar el editor de servicios web en IBM Rational Application Developer para editar el archivo descriptor de despliegue. No utilice el asistente de seguridad de Rational Application Developer para editar el archivo descriptor de despliegue. El asistente no permite que controle las características de firma digital XML tales como los algoritmos de transformación y de firma.

Esta tarea muestra cómo firmar y validar firmas digitales para mensajes de solicitud, no mensajes de respuesta. No obstante, el procedimiento para firmar y validar firmas digitales para mensajes de respuesta es virtualmente idéntico y, por ello, no se ha documento aquí. Para resumir dicha tarea, configure el consumidor de respuestas (lado del cliente) y el generador de respuestas (lado del servidor) de la misma forma para que el generador de solicitudes (lado del cliente) y el consumidor de solicitudes (lado del servidor) se configuren en esta sección.

Procedimiento

1. En el separador **Explorador de proyectos** de Rational Application Developer, expanda **soapbinding** > **Servicios** y pulse con el botón derecho del ratón el servicio. Seleccione **Mostrar** y, a continuación, pulse **Descriptor de despliegue**. Se abre el editor de servicios web.
2. En el editor de servicio web, pulse el separador **Ampliaciones**.
3. Expanda **Ampliación de descripción de servicio web** y seleccione la descripción del servicio.
4. Expanda **Enlace de componente de puerto** y seleccione el enlace de su servicio.
5. Expanda **Detalles de configuración de enlace de consumidor de solicitudes** > **Integridad necesaria**.
6. En la ventana Integridad necesaria, pulse **Añadir**.
7. En el campo **Nombre de integridad necesaria** de la ventana Confidencialidad necesaria, escriba un nombre.
8. En el campo **Tipo de uso**, seleccione **Necesario** si desea que la integridad sea necesaria u **Opcional** si desea que la integridad sea opcional.

9. En el campo **Partes del mensaje**, seleccione las partes del mensaje que desee que se firmen. Puede utilizar palabras clave o expresiones XPath para firmar las partes del mensaje. Si desea añadir partes de mensaje:
   a. Pulse **Añadir**.
   b. Puede utilizar palabras clave para identificar partes genéricas de su mensaje, seleccionar **http://www.ibm.com/websphere/webservices/wssecurity/dialect-was** de la columna Dialecto de partes y seleccionar la parte del mensaje que desee firmar de la columna Palabra clave de partes.
   c. Puede utilizar expresiones XPath para identificar partes más específicas del mensaje; seleccione **http://www.w3.org/TR/1999/REC-xpath-19991116** en la columna Dialecto de partes.
   d. Opcional: En el campo **Partes de mensaje**, especifique un nonce para evitar ataques de respuesta.
   e. Opcional: En el campo **Partes de mensaje**, especifique una indicación de fecha y hora para asignar una vigencia al mensaje.
10. En el editor de servicios web, pulse el separador **Configuraciones de enlaces**.
11. Expanda **Configuración de enlace de consumidor de solicitudes** > **Ancla de confianza** y pulse **Añadir**.
12. En la ventana Ancla de confianza:
   a. Escriba un nombre de ancla de confianza.
   b. Escriba una contraseña para el almacén de claves.
   c. Escriba la vía de acceso completa al almacén de claves del lado del servidor, por ejemplo, `C:\sampleks\receiverkeys.jks`.
   d. Seleccione el tipo de almacén de claves.
   e. Pulse **Aceptar**.
13. En el editor de servicios web, expanda **Configuración de enlace de consumidor de solicitudes** > **Consumidor de señales** y pulse **Añadir**.
14. En la ventana Consumidor de señales:
   a. Escriba un nombre de consumidor de señales.
   b. Seleccione **com.ibm.wssip.wssecurity.token.X509TokenConsumer** como clase de consumidor de señales.
   c. No seleccione una señal de seguridad. Para firmar no es necesario especificar una señal de seguridad en las ampliaciones de servicio.
   d. Seleccione **Utilizar tipo de valor** y seleccione el tipo de valor **Señal de certificado X509 v3**.
   e. Seleccione **Utilizar jaas.config** y escriba `system.wssecurity.X509BST` en el campo **nombre de jaas.config**.
   f. Seleccione **Utilizar valores de vía de acceso de certificado** y **Referencia de vía de acceso de certificado** o **Confiar en todos los certificados**. Si selecciona **Utilizar valores de vía de acceso de certificado**, seleccione el nombre del ancla de confianza que haya creado arriba.
   g. Pulse **Aceptar**.
15. En el editor de servicios web, expanda **Configuración de enlace de consumidor de solicitudes** > **Localizador de claves** y pulse **Añadir**.
16. En la ventana Localizador de claves:
   a. Escriba un nombre de localizador de claves.

b. Seleccione la implementación de la clase de localizador de claves. Utilice **com.ibm.wsspi.wssecurity.keyinfo.X509TokenKeyLocator** si está utilizando la señal de seguridad X.509 del mensaje del remitente para la validación de la firma digital.

c. Pulse **Aceptar**.

17. En el editor de servicios web, expanda **Configuración de enlace de consumidor de solicitudes** > **Información de clave** y pulse **Añadir**.
18. En la ventana Información de clave:
    a. Escriba un nombre de información de clave.
    b. Seleccione un tipo de información de clave. Utilice **STRREF** como el tipo de información clave si la señal de seguridad utilizada para la validación de firma digital es directamente referenciada utilizando un URI en el remitente del remitente.
    c. Seleccione una clase de información clave. Si ha seleccionado **STRREF** como tipo de información clave, **com.ibm.ws.webservices.wssecurity.keyinfo. STRReferenceContentConsumer** se seleccionará automáticamente.
    d. Seleccione **Utilizar localizador de claves** y seleccione el nombre del localizador de claves que haya creado en la sección Localizador de claves.
    e. Seleccione **Utilizar señal** y seleccione el nombre del consumidor de señal que haya creado en la sección Consumidor de señales.
    f. Pulse **Aceptar**.
19. En el editor de servicios web, expanda **Configuración de enlace de consumidor de solicitudes** > **Información de firma** y pulse **Añadir**.
20. En la ventana Información de firma:
    a. Escriba un nombre de información de firma.
    b. Seleccione un algoritmo de método de canonicalización. El valor predeterminado es **http://www.w3.org/2001/10/xml-exc-c14n#**.
    c. Seleccione un algoritmo de método de firma. El valor predeterminado es **http://www.w3.org/2000/09/xmldsig#rsa-sha1**.
    d. Pulse **Añadir**, seleccione el elemento de información de clave que haya creado en la sección Información de clave y escriba un nombre de información de clave.
    e. Pulse **Aceptar**.
21. En el editor de servicios web, expanda **Configuración de enlace de consumidor de solicitudes** > **Referencia de componente** y pulse **Añadir**.
22. En la ventana Referencia de componente:
    a. Escriba un nombre de referencia de componente.
    b. Seleccione un componente de integridad necesario que haya creado en la sección Integridad necesaria.
    c. Seleccione un algoritmo de método de resumen. El valor predeterminado es **http://www.w3.org/2000/09/xmldsig#sha1**.
    d. Pulse **Aceptar**.
23. En el editor de servicios web, expanda **Configuración de enlace de consumidor de solicitudes** > **Transformaciones** y pulse **Añadir**.La sección Transformaciones pasa a estar disponible tras crear una referencia de componente. Los elementos de transformación contienen información sobre las operaciones que se han realizado en datos antes de su firma.
24. En la ventana Transformación:
    a. Escriba un nombre de transformación.

b. Seleccione un algoritmo para realizar la operación. El valor predeterminado es **http://www.w3.org/2002/10/xml-exc-c14n#**.
c. Pulse **Aceptar**.

25. Guarde los cambios.

Exportación de un archivo EAR de servicio seguro desde una herramienta de conjunto

Tras habilitar las características de seguridad como la autenticación, autorización o la confidencialidad para un servicio utilizando una herramienta de conjunto, podrá exportar el servicio seguro como archivo EAR.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10
- Proteja una servicio tal como está descrito en "Cómo asegurar un servicio" en la página 11

Acerca de esta tarea

Este procedimiento muestra cómo exportar un archivo EAR de servicio a IBM Rational Application Developer. Los pasos son parecidos si utiliza IBM WebSphere Application Server Toolkit para exportar el archivo EAR de servicio.

Procedimiento

1. En el separador **Explorador de proyectos**, pulse con el botón derecho del ratón sobre el archivo EAR y seleccione **Exportar** > **Archivo EAR**.
2. En la ventana Exportar, pulse **Examinar** para seleccionar la ubicación del archivo EAR.
3. Seleccione el recuadro de selección **Sobrescribir archivo existente** para sobrescribir el archivo EAR de servicio no seguro.
4. Pulse **Finalizar**.

Cómo volver a desplegar un servicio seguro con la consola de IBM WebSphere Application Server

Tras habilitar características de seguridad tales como la autenticación, la autorización o la confidencialidad de un servicio y haber exportado el servicio seguro como un archivo de archivador empresarial (EAR), vuelva a desplegar el servicio seguro utilizando la consola de IBM WebSphere Application Server.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en “Configuración de una herramienta de conjunto con IBM InfoSphere Information Server” en la página 8
- Inhabilite el servicio no seguro tal como está descrito en “Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server” en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en “Exportación de un servicio utilizando la consola de WebSphere Application Server:” en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en “Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto” en la página 10
- Proteja una servicio tal como está descrito en “Cómo asegurar un servicio” en la página 11
- Exporte un archivo EAR que contiene el servicio tal como se describe en “Exportación de un archivo EAR de servicio seguro desde una herramienta de conjunto” en la página 30

Procedimiento

1. Seleccione **Aplicaciones** > **Aplicaciones empresariales**.
2. Si no se admite su aplicación (indicado con una X roja en la columna de estado), seleccione la aplicación y pulse **Detener**.
3. Seleccione la aplicación y pulse **Desinstalar**.
4. En la ventana Desinstalar aplicación, pulse **Aceptar**.
5. Pulse **Guardar** para aplicar los cambios en la configuración maestra y pulse **Guardar** en la ventana que se visualiza.
6. En la ventana Aplicaciones empresarial, seleccione la aplicación y pulse **Instalar**.
7. En la ventana Cómo preparar la instalación de la aplicación, pulse **Examinar** para seleccionar la ubicación del archivo EAR del servicio seguro y pulse **Siguiente**.
8. Pulse **Siguiente** hasta que llegue al resumen de la aplicación.
9. Pulse **Finalizar**. Se visualizan mensajes que indican el progreso de la instalación.
10. Pulse **Guardar en configuración maestra** y pulse **Guardar** en la ventana que se visualiza.
11. En la ventana Aplicación empresarial, seleccione la aplicación que se acaba de instalar y pulse **Iniciar**.

Cómo habilitar un servicio seguro utilizando la Consola de IBM InfoSphere Information Server

Después de volver a desplegar el servicio seguro desde la IBM WebSphere Application Server, habilite el servicio desde la consola de Consola de IBM InfoSphere Information Server.

Antes de empezar

- Cree un servicio

- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10
- Proteja una servicio tal como está descrito en "Cómo asegurar un servicio" en la página 11
- Exporte un archivo EAR que contiene el servicio tal como se describe en "Exportación de un archivo EAR de servicio seguro desde una herramienta de conjunto" en la página 30
- Vuelva a desplegar el archivo EAR de servicio tal como se describe en "Cómo volver a desplegar un servicio seguro con la consola de IBM WebSphere Application Server" en la página 30

Procedimiento

1. Inicie la sesión en la Consola de IBM InfoSphere Information Server y abra el proyecto que contiene el servicio que desea habilitar.
2. Seleccione **OPERATE** > **Aplicaciones de servicios de información desplegados**.
3. En el panel Vista, seleccione la aplicación que contiene el servicio que desea habilitar.
4. Pulse **Editar**.
5. En la parte inferior del panel Vista, pulse **Inhabilitar** y seleccione **Habilitar**.
6. Pulse **Guardar** y **Cerrar**.

Generación de un cliente de prueba

Puede generar un cliente de prueba para probar sus servicios. Puede generar el cliente de prueba con la seguridad habilitada o inhabilitada.

Generación de un cliente de prueba con la seguridad inhabilitada

Utilice esta tarea para generar un cliente de prueba para un servicio con la seguridad inhabilitada.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8

Acerca de esta tarea

Si invoca un servicio seguro utilizando la autenticación de señal de nombre de usuario con un cliente de prueba no seguro recibirá la siguiente excepción de seguridad:

```
exception: com.ibm.wsspi.wssecurity.SoapSecurityException:
WSEC5509E: se necesita una señal de seguridad cuyo tipo es
http://myapp.wisd.ibm.com#UsernameTokenhttp:
//docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-
token-profile-1.0#UsernameToken].
```

Para una señal de certificado X.509, recibirá la siguiente excepción de seguridad:

```
exception: com.ibm.wsspi.wssecurity.SoapSecurityException:
WSEC5509E: se necesita una señal de seguridad cuyo tipo es
[X509Tokenhttp://docs.oasis-open.org/wss/2004
/01/oasis-200401-wss-x509-token-profile-1.0#X509].
```

Procedimiento

1. En el separador **Servidores** de IBM WebSphere Application Server, pulse con el botón derecho del ratón en cualquier punto de la ventana y pulse **Nuevo** > **Servidor**.
2. En la página **Definir un servidor nuevo** de la ventana Servidor nuevo, introduzca un nombre para el host de servidor, pulse **IBM** > **WebSphere v6.1 Server** o **WebSphere v7.0 Server** como tipo de servidor y pulse **Information Server WAS v6.1** o **Information Server WAS v7.0** como entorno de ejecución de servidor.
3. Pulse **Siguiente** y asegúrese de que la información de la página siguiente sea correcta, incluyendo el nombre del perfil y la información de autenticación. Opcionalmente, puede pulsar el enlace **Probar conexión** para asegurarse de que IBM Rational Application Developer puede conectarse a WebSphere Application Server utilizando la información de autenticación que se ha especificado.
4. Pulse **Siguiente**.
5. En la página **Añadir y eliminar proyectos**, pulse el archivo *MyApp*`.ear` en el campo **Proyectos disponibles** y pulse **Añadir >** para añadirlo a la lista de proyectos configurados.
6. Pulse **Siguiente** y, a continuación, pulse **Finalizar**. Con el servidor en su sitio, cuando sea preciso, puede añadir un proyecto a este servidor pulsando con el botón derecho del ratón sobre el servidor en el separador **Servidores** y seleccionando **Añadir y eliminar proyectos**.
7. En el separador **Servidores**, seleccione el servidor que ha creado y pulse el icono **Iniciar el servidor**.
8. Seleccione **Archivo** > **Nuevo** > **Proyecto** > **Proyecto web dinámico**.
9. En la ventana Nuevo proyecto web dinámico, introduzca un nombre de proyecto (MyAppClient, por ejemplo), seleccione la versión de WebSphere Application Server apropiada como la ejecución de destino, seleccione **Añadir proyecto a un EAR** e introduzca un nombre de proyecto de archivo de archivador empresarial (EAR) (MyAppClient.ear, por ejemplo) para el archivo EAR que contendrá el código de cliente.
10. Pulse **Finalizar**.
11. Pulse **Archivo** > **Nuevo** > **Otros**.
12. En la ventana **Nuevo**, expanda **Servicios web**, seleccione **Cliente de servicio web** y pulse **Siguiente**.

13. En la página **Servicios web** de la ventana Cliente de servicio web, introduzca el URL del lenguaje de descripción de servicios web (WSDL) (por ejemplo, http://localhost:9080/wisd/MyApp/MyService?wsdl) en el campo **Definición de servicio**.
14. Seleccione **Cliente de prueba** como nivel de automatización.
15. En el panel Configuración, verifique estos valores:

    Servidor
    Websphere v6.1 Server o Websphere v7.0 Server

    Ejecución de servicio web
    IBM WebSphere JAX-RPC

    Proyecto de cliente
    MyAppClient

    Proyecto de aplicación empresarial de cliente
    MyAppClient.ear
16. Pulse **Finalizar**.
17. En la página **Prueba de cliente de servicio web**, seleccione el recurso de prueba **JSP de muestra de servicio web** y todos los métodos que desee probar. Utilice los valores predeterminados para el resto de esta página y pulse **Finalizar**.
18. Para ver el cliente de prueba en el **Explorador de proyectos** en **Servicios web JSR-109** > **Clientes**, reinicie IBM Rational Application Developer. Necesitará ver el cliente de prueba si desea utilizarlo para ejecutar los asistentes de seguridad.
19. Opcional: Para probar el servicio utilizando el cliente de prueba, en el separador **Cliente de prueba de servicios web** que se abrirá, seleccione un método, introduzca un número de entrada y pulse **Invocar**. El panel **Resultado** muestra el resultado.
20. Opcional: Para invocar el cliente de prueba sin utilizar la herramienta de conjunto, utiliza un navegador web e introduzca el URL `https://`*`nombreHost`*`:`*`puertoCanalSSLWAS`*`/`*`nombreAplicación`*`/muestra`*`nombreServicio`*`PortTypeProxy/TestClient.jsp`

    nombreHost
    El nombre del servidor que hospeda al cliente de prueba (sistema principal local, por ejemplo)

    puertoCanalSSLWAS
    El número de puerto utilizado por el canal de transporte SSL (9443 es el valor predeterminado)

    nombreAplicación
    El nombre del cliente de prueba

    nombreServicio
    El nombre del servicio que desea invocar

Generación de un cliente de prueba con la autenticación habilitada

Utilice esta tarea para generar un cliente de prueba para un servicio con la autenticación habilitada.

Antes de empezar

- Cree un servicio

- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10
- Añada autenticación al servicio tal como se describe en "Cómo añadir mecanismos de autenticación" en la página 14
- Exporte un archivo EAR que contiene el servicio tal como se describe en "Exportación de un archivo EAR de servicio seguro desde una herramienta de conjunto" en la página 30
- Vuelva a desplegar el archivo EAR de servicio tal como se describe en "Cómo volver a desplegar un servicio seguro con la consola de IBM WebSphere Application Server" en la página 30
- Habilite el servicio seguro tal como se describe en "Cómo habilitar un servicio seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 31

Acerca de esta tarea

El asistente de seguridad de IBM Rational Application Developer se utiliza en esta tarea para mostrar cómo habilitar la autenticación de señal de nombre de usuario de Seguridad WS en el cliente de prueba. De forma alternativa, puede utilizar el editor de descriptor de despliegue de Rational Application Developer para habilitar la seguridad en el cliente.

Si invoca un servicio que requiera autenticación pero no especifica un nombre de usuario ni una contraseña, el sistema devolverá la siguiente excepción de seguridad o una parecida:

```
excepción: com.ibm.wsspi.wssecurity.SoapSecurityException: WSEC5509E:
se necesita una señal de seguridad cuyo tipo sea [http://docs.oasis-open.org/wss/2004/
01/oasis-200401-wss-username-token-profile-1.0#UsernameToken].
```

De forma parecida, si invoca un servicio que requiera autenticación de señal de nombre de usuario pero especifica un nombre de usuario o una contraseña que no son válidos, el sistema devolverá la siguiente excepción o una parecida:

```
excepción: com.ibm.wsspi.wssecurity.SoapSecurityException: WSEC6521E:
Ha fallado el inicio de sesión.
La excepción es : javax.security.auth.login.LoginException:
WSEC6690E: No se ha podido comprobar el nombre de usuario [admin] ni la contraseña en
UserRegsitry: UserRegistryProcessor.checkRegistry()=false
```

Procedimiento

1. En el separador **Servidores** de IBM WebSphere Application Server, pulse con el botón derecho del ratón en cualquier punto de la ventana y seleccione **Nuevo** > **Servidor**.

2. En la página **Definir un servidor nuevo** de la ventana Servidor nuevo, introduzca un nombre para el host de servidor, seleccione **IBM** > **WebSphere v6.1 Server** o **WebSphere v7.0 Server** como tipo de servidor y el entorno de ejecución. Si ha seguido la tarea para configurar IBMRational Application Developer con IBM InfoSphere Information Server, el entorno de ejecución correcto será**Information Server WAS v6.1** o **Information Server WAS v7.0**.
3. Pulse **Siguiente** y asegúrese de que la información de la página siguiente sea correcta, incluyendo el nombre del perfil y la información de autenticación.
4. Pulse **Siguiente**.
5. En la página **Añadir y eliminar proyectos**, seleccione su archivo EAR seguro en el campo **Proyectos disponibles** y pulse **Añadir >** para añadirlo a la lista de proyectos configurados.
6. Pulse **Siguiente** y, a continuación, pulse **Finalizar**.
7. En el separador **Servidores**, seleccione el servidor que ha creado y pulse el icono **Iniciar el servidor**.
8. Seleccione **Archivo** > **Nuevo** > **Proyecto** > **Proyecto web dinámico**.
9. En la ventana Nuevo proyecto web dinámico, introduzca un nombre de proyecto (MyAppClient, por ejemplo), seleccione **Information Server WAS v6.1** o **Information Server WAS v7.0** como la ejecución de destino, seleccione **Añadir proyecto a un EAR** e introduzca un nombre de proyecto de archivo EAR (MyAppClient.ear, por ejemplo) para el archivo EAR que contendrá el código de cliente.
10. Pulse **Finalizar**.
11. Seleccione **Archivo** > **Nuevo** > **Otros**.
12. En la ventana **Nuevo**, expanda **Servicios web**, seleccione **Cliente de servicio web** y pulse **Siguiente**.
13. En la página **Servicios web** de la ventana Cliente de servicio web, introduzca el URL del lenguaje de descripción de servicios web (WSDL) (por ejemplo, `http://localhost:9080/wisd/MyApp/MyService?wsdl`) en el campo **Definición de servicio**.
14. Seleccione **Cliente de prueba** como nivel de automatización.
15. En el panel Configuración, verifique estos valores:

    Servidor
    Websphere v6.1 Server o Websphere v7.0 Server

    Ejecución de servicio web
    API de Java para RPC basado en XML de IBM WebSphere

    Proyecto de cliente
    MyAppClient

    Proyecto de aplicación empresarial de cliente
    MyAppClient.ear
16. Pulse **Finalizar**.
17. En la página **Prueba de cliente de servicio web**, seleccione el recurso de prueba **JSP de muestra de servicio web** y el método que desee probar. Utilice los valores predeterminados para el resto de esta página y pulse **Finalizar**.
18. En el **Explorador de proyectos** expanda **Servicios web JSR-109** > **Clientes**.
19. Efectúe una pulsación con el botón derecho del ratón sobre el cliente de prueba que acaba de crear y seleccione **Cliente de servicio de servicio web** > **Añadir señal de seguridad autónoma** (presuponiendo que la seguridad que se ha habilitado en el servicio sea una señal de seguridad de nombre de usuario

para realizar autenticaciones). Si el cliente de prueba no se encuentra en la carpeta **Clientes**, reinicie Rational Application Developer.

20. En el asistente de Seguridad WS, seleccione el tipo de señal **Señal de nombre de usuario** y el manejador de retorno de llamada **com.ibm.wsspi.wssecurity.auth.callback.NonPromptCallbackHandler**. Podrá especificar las credenciales de inicio de sesión en la siguiente página del asistente.
21. Pulse **Siguiente**.
22. Introduzca un ID de usuario y una contraseña válidos para el servicio y pulse **Finalizar**.
23. Guarde los cambios y reinicie el cliente de prueba.
24. Opcional: Para probar el servicio utilizando el cliente de prueba, en el separador **Cliente de prueba de servicios web** que se abrirá, seleccione un método, introduzca un número de entrada y pulse **Invocar**. El panel **Resultado** muestra el resultado.
25. Opcional: Para invocar el cliente de prueba sin utilizar la herramienta de conjunto, utilice un navegador web e introduzca el URL`https://`*`nombreHost`*`:`*`puertoCanalSSLWAS`*`/`*`nombreAplicación`*`/muestra`*`nombreServicio`*`PortTypeProxy/TestClient.jsp`en el campo de dirección.

    nombreHost
    El nombre del servidor que hospeda al cliente de prueba (sistema principal local, por ejemplo).

    puertoCanalSSLWAS
    El número de puerto utilizado por el canal de transporte SSL (9443 es el valor predeterminado).

    nombreAplicación
    El nombre del cliente de prueba.

    nombreServicio
    El nombre del servicio que desea invocar.

Generación de almacenes de claves, claves y certificados

Cualquier tipo de cifrado, incluyendo SSL, requiere que genere almacenes de claves en los lados del cliente y del servidor. Los almacenes de claves contienen claves que firman y cifran mensajes. Utilice los almacenes de claves de muestra de este tema para probar su cifrado o ejecutar el script utilizando el programa de utilidad Keytool Java para generar usted mismo almacenes de claves de muestra.

Nota: Para conservar este simple ejemplo, los almacenes de claves de muestra se generaron utilizando certificados autofirmados en lugar de certificados firmados por una entidad emisora de certificados (CA).

Sólo utilice estos almacenes de claves de muestra para realizar pruebas. Implemente su propia infraestructura de claves públicas (PKI) en un entorno de producción real.

Puede generar almacenes de claves utilizando distintos métodos. Los almacenes de claves de muestra de este tema se generaron utilizando `keytool`, la herramienta de línea de mandatos de Java y el siguiente script. También puede utilizar iKeyman, la herramienta IBM Key Management, que es una interfaz gráfica de usuario para gestionar claves y almacenes de claves. Se instala con IBM WebSphere Application Server en *`dir-instalación`*`/WebSphere/AppServer/bin/ikeyman.bat`.

Cifrado SSL

- Almacén de claves de cliente (clientsslkeys.jceks):
  - Clave privada de cliente
- Almacén de confianza de cliente (clientssltrusts.jceks):
  - Certificado autofirmado de servidor con una única clave pública
- Almacén de claves de servidor (serversslkeys.jceks):
  - Clave privada de servidor
- Almacén de confianza de servidor (serverssltrusts.jceks):
  - Certificado autofirmado de cliente con una única clave pública

Los almacenes de claves de muestra también tienen las siguientes características.

Tabla 1. Características del almacén de claves de cliente `clientsslkeys.jceks`

Campo	**Valor**
Nombre de archivo	`C:\sampleks\clientsslkeys.jceks`
Storepass	contraseña
Storetype	JCEK
Nombre distinguido	CN=wasclient, O=IBM, C=US
Keypass	contraseña
Alias	wasclient

Tabla 2. Características del almacén de confianza de cliente `clientssltrusts.jceks`

Campo	**Valor**
Nombre de archivo	`C:\sampleks\clientssltrusts.jceks`
Storepass	contraseña
Storetype	JCEK
Archivo de certificado	wasserver.cert

Tabla 3. Características del almacén de claves de servidor `serversslkeys.jceks`

Campo	**Valor**
Nombre de archivo	`C:\sampleks\serversslkeys.jceks`
Storepass	contraseña
Storetype	JCEK
Nombre distinguido	CN=wasserver, O=IBM, C=US
Keypass	contraseña
Alias	wasserver

Tabla 4. Características del almacén de confianza de servidor `serverssltrusts.jceks`

Campo	**Valor**
Nombre de archivo	`C:\sampleks\serverssltrusts.jceks`
Storepass	contraseña
Storetype	JCEK
Archivo de certificado	wasclient.cert

Creación de un almacén de claves de cliente

La utilización de Java keytool permite generar el almacén de claves de cliente con el siguiente script.

```
REM  Generar almacén de claves de cliente y clave privada
keytool -genkey -v -alias wasclient -keypass password -keystore
clientsslkeys.jceks -storepass password -storetype jceks -dname
"CN=wasclient, O=IBM, C=US" -keyalg "RSA"
REM  Generar certificado autofirmado de cliente
keytool -export -v -alias wasclient -file wasclient.cert -rfc
-keystore
clientsslkeys.jceks -storepass password -storetype jceks
```

Creación de un almacén de claves de servidor

La utilización de Java keytool permite generar el almacén de claves de servidor con el siguiente script.

```
REM  Generar almacén de claves de servidor y clave privada
keytool -genkey -v -alias wasserver -keypass password -keystore
serversslkeys.jceks -storepass password -storetype jceks -dname
"CN=wasserver, O=IBM, C=US" -keyalg "RSA"
REM  Generar certificado autofirmado de servidor
keytool -export -v -alias wasserver -file wasserver.cert -rfc
-keystore
serversslkeys.jceks -storepass password -storetype jceks
```

Creación de un almacén de confianza de cliente

La utilización de Java keytool permite generar el almacén de confianza de cliente con el siguiente script.

```
REM  Importar el certificado de servidor en el almacén de confianza del cliente
keytool -import -v -noprompt -alias wasserver -file wasserver.cert -
keystore clientssltrusts.jceks -storepass password -storetype jceks
```

Creación de un almacén de confianza de servidor

La utilización de Java keytool permite generar el almacén de confianza de servidor con el siguiente script.

```
REM  Importar el certificado de cliente en el almacén de confianza del cliente
keytool -import -v -noprompt -alias wasclient -file wasclient.cert -
keystore serverssltrusts.jceks -storepass password -storetype jceks
```

Generación de un cliente de prueba con SSL habilitada

Utilice esta tarea para generar un cliente de prueba para un servicio que habilite la confidencialidad de datos utilizando el cifrado de la capa de sockets seguros (SSL).

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en "Configuración de una herramienta de conjunto con IBM InfoSphere Information Server" en la página 8
- Inhabilite el servicio no seguro tal como está descrito en "Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en "Exportación de un servicio utilizando la consola de WebSphere Application Server:" en la página 9

- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en "Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto" en la página 10
- Añada confidencialidad al servicio tal como se describe en "Cómo añadir confidencialidad de datos utilizando el cifrado SSL" en la página 25
- Exporte un archivo EAR que contiene el servicio tal como se describe en "Exportación de un archivo EAR de servicio seguro desde una herramienta de conjunto" en la página 30
- Vuelva a desplegar el archivo EAR de servicio tal como se describe en "Cómo volver a desplegar un servicio seguro con la consola de IBM WebSphere Application Server" en la página 30
- Habilite el servicio seguro tal como se describe en "Cómo habilitar un servicio seguro utilizando la Consola de IBM InfoSphere Information Server" en la página 31

Acerca de esta tarea

En una parte de esta tarea creará el nuevo repertorio Java Secure Socket Extension (JSSE) SSL utilizando IBM WebSphere Application Server. Para crear este nuevo repertorio necesitará utilizar los almacenes de claves de muestra de "Generación de almacenes de claves, claves y certificados" en la página 37.

Procedimiento

1. Inicie sesión en la consola de administración de IBM WebSphere Application Server.
2. En el panel de navegación, expanda **Seguridad** y pulse **SSL**.
3. En la ventana Repertorios de configuración SSL, pulse **Repertorio JSSE nuevo**.
4. En el separador **Configuración**:
   a. Escriba un nombre de alias para el repertorio. Por ejemplo, `WASClientSSL`.
   b. No seleccione el recuadro de selección **Autenticación de cliente**. El repertorio SSL actúa como un cliente SSL y no como un servidor, por lo que no hay ningún cliente que deba autenticarse.
   c. Para el nivel de seguridad, seleccione **HIGH**.
   d. Opcional: Seleccione cifrados de la lista **Suites de cifrado** si desea sustituir los cifrados predefinidos que cifran SSL de acuerdo con el nivel de seguridad que haya seleccionado.
   e. Opcional: Seleccione el recuadro de selección **Señal criptográfica**.
   f. Opcional: Seleccione o personalice el proveedor JSSE.
   g. Seleccione el protocolo **SSL**.
   h. Introduzca la ubicación, nombre y contraseña de este archivo de claves y seleccione un formato. Utilice el archivo de claves ubicado en el tema de referencia de almacenes de claves de muestra.
   i. Introduzca la ubicación, nombre y contraseña de este archivo de confianza y seleccione un formato. Utilice el archivo de confianza ubicado en el tema de referencia de almacenes de claves de muestra.
   j. Pulse **Aceptar**.
5. Guarde los cambios y reinicie IBM WebSphere Application Server.

6. En el separador **Servidores** de IBM Rational Application Developer, pulse con el botón derecho del ratón en cualquier punto dentro de la ventana y seleccione **Nuevo** > **Server**.
7. En la página **Definir un servidor nuevo** de la ventana Servidor nuevo, introduzca un nombre para el host de servidor, seleccione **IBM** > **WebSphere v6.1 Server** o **WebSphere v7.0 Server** como tipo de servidor y el entorno de ejecución. Si ha seguido la tarea para configurar IBMRational Application Developer con IBM InfoSphere Information Server, el entorno de ejecución correcto será**Information Server WAS v6.1** o **Information Server WAS v7.0**.
8. Pulse **Siguiente** y asegúrese de que la información de la página siguiente sea correcta, incluyendo el nombre del perfil y la información de autenticación.
9. Pulse **Siguiente**.
10. En la página **Añadir y eliminar proyectos**, seleccione su archivo EAR seguro en el campo **Proyectos disponibles** y pulse **Añadir >** para añadirlo a la lista de proyectos configurados.
11. Pulse **Siguiente** y, a continuación, pulse **Finalizar**.
12. En el separador **Servidores**, seleccione el servidor que ha creado y pulse el icono **Iniciar el servidor**.
13. Seleccione **Archivo** > **Nuevo** > **Proyecto** > **Proyecto web dinámico**.
14. En la ventana Nuevo proyecto web dinámico, introduzca un nombre de proyecto (MyAppClient, por ejemplo), seleccione **Information Server WAS v6.1** o **Information Server WAS v7.0** como la ejecución de destino, seleccione **Añadir proyecto a un EAR** e introduzca un nombre de proyecto de archivo EAR (MyAppClient.ear, por ejemplo) para el archivo EAR que contendrá el código de cliente.
15. Pulse **Finalizar**.
16. Seleccione **Archivo** > **Nuevo** > **Otros**.
17. En la ventana **Nuevo**, expanda **Servicios web**, seleccione **Cliente de servicio web** y pulse **Siguiente**.
18. En la página **Servicios web** de la ventana Cliente de servicio web, introduzca el URL del lenguaje de descripción de servicios web (WSDL) (http://localhost:9080/wisd/MyApp/MyService?wsdl, por ejemplo) en el campo **Definición de servicio**.
19. Seleccione **Cliente de prueba** como nivel de automatización.
20. En el panel Configuración, verifique estos valores:

    Servidor
    Websphere v6.1 Server o Websphere v7.0 Server

    Ejecución de servicio web
    API de Java para RPC basado en XML de IBM WebSphere

    Proyecto de cliente
    MyAppClient

    Proyecto de aplicación empresarial de cliente
    MyAppClient.ear
21. Pulse **Finalizar**.
22. En la página **Prueba de cliente de servicio web**, seleccione el recurso de prueba **JSP de muestra de servicio web** y el método que desee probar. Utilice los valores predeterminados para el resto de esta página y pulse **Finalizar**.
23. En el **Explorador de proyectos** de IBM Rational Application Developer, expanda **Servicios web JSR-109** > **Clientes** y efectúe una doble pulsación

sobre el cliente de prueba generado para editar el descriptor de despliegue. Reinicie Rational Application Developer si el cliente de prueba no está en la carpeta.

24. Pulse el separador **Enlace WS** de la ventana Descriptor de despliegue web y expanda la sección **Detalles de enlace de nombre calificado de puerto**.
25. En el campo **Configuración SLL HTTPNombre**, introduzca el nombre del repertorio SSL del cliente. Por ejemplo, *name2Node01/WASClientSSL*.
26. Guarde los cambios y reinicie el cliente de prueba.
27. Opcional: Para probar el servicio utilizando el cliente de prueba, en el separador **Cliente de prueba de servicios web** que se abrirá, seleccione un método, introduzca un número de entrada y pulse **Invocar**. El panel **Resultado** muestra el resultado.
28. Opcional: Para invocar el cliente de prueba sin utilizar la herramienta de conjunto, utilice un navegador web e introduzca el URL`https://`*`nombreHost`*`:`*`puertoCanalSSLWAS`*`/`*`nombreAplicación`*`/muestra`*`nombreServicio`*`PortTypeProxy/TestClient.jsp`en el campo de dirección.

    nombreHost
    El nombre del servidor que hospeda al cliente de prueba (sistema principal local, por ejemplo).

    puertoCanalSSLWAS
    El número de puerto utilizado por el canal de transporte SSL (9443 es el valor predeterminado).

    nombreAplicación
    El nombre del cliente de prueba.

    nombreServicio
    El nombre del servicio que desea invocar.

Ejemplo

Evite estos errores cuando habilite SSL utilizando IBM WebSphere Application Server:

- Si invoca un servicio SSL seguro utilizando HTTP en lugar de HTTPS, el sistema devuelve la siguiente excepción:

  ```
  excepción: WSWS3499W: nueva ubicación redirigida:
  http://localhost:9080/wisd/MyApp/MyService
  ```

- Si invoca un servicio SSL seguro utilizando un cliente de prueba no configurado para SSL, el sistema devuelve la siguiente excepción:

  ```
  excepción: WSWS3713E: conexión con sistema principal remoto
  sistema principal local fallido. Se ha recibido el siguiente error:
  el reconocimiento ha terminado el motor SSL: CLOSED
  ```

- Si invoca un servicio SSL seguro utilizando un cliente de prueba que no está bien configurado para SSL (el almacén de confianza de cliente no está bien configurado), el sistema devuelve la siguiente excepción:

  ```
  excepción: com.ibm.wsspi.channel.framework.exception
  ChannelException:com.ibm.wsspi.channel.framework.exception.
  ChannelException: nombre de archivo de confianza no válido o nulo
  ```

Rastreo de mensajes de SOAP

Rastrear los mensajes de SOAP intercambiados entre cliente y servidor para solucionar problemas con un servicio. Utilice la herramienta Supervisor TCP/IP Monitor en IBM Rational Application Developer para rastrear mensajes de SOAP.

Antes de empezar

- Cree un servicio
- Configure una herramienta de conjunto tal como se describe en “Configuración de una herramienta de conjunto con IBM InfoSphere Information Server” en la página 8
- Inhabilite el servicio no seguro tal como está descrito en “Cómo inhabilitar un servicio no seguro utilizando la Consola de IBM InfoSphere Information Server” en la página 9
- Exporte el servicio para crear un archivador empresarial (EAR) del servicio tal como se describe en “Exportación de un servicio utilizando la consola de WebSphere Application Server:” en la página 9
- Importe el archivo EAR de servicio en una herramienta de conjunto si desea utilizar la herramienta para habilitar características de seguridad en “Importación de un archivo EAR de servicio no seguro en una herramienta de conjunto” en la página 10
- Proteja una servicio tal como está descrito en “Cómo asegurar un servicio” en la página 11
- Exporte un archivo EAR que contiene el servicio tal como se describe en “Exportación de un archivo EAR de servicio seguro desde una herramienta de conjunto” en la página 30
- Vuelva a desplegar el archivo EAR de servicio tal como se describe en “Cómo volver a desplegar un servicio seguro con la consola de IBM WebSphere Application Server” en la página 30
- Habilite el servicio seguro tal como se describe en “Cómo habilitar un servicio seguro utilizando la Consola de IBM InfoSphere Information Server” en la página 31

Procedimiento

1. Seleccione **Ventana** > **Mostrar vista** > **Otros**.
2. En la ventana Mostrar vista, expanda **Depurar** , seleccione **Supervisor TCP/IP** y pulse **Aceptar**.
3. Pulse con el botón derecho del ratón la ventana Supervisor TCP/IP y seleccione **Propiedades**.
4. Pulse **Añadir** e introduzca o seleccione la siguiente información en la ventana Monitor nuevo:
   a. Introduzca un número de puerto de supervisión local no utilizado. Por ejemplo, *13557*. El cliente enviará solicitudes SOAP a este puerto.
   b. Introduzca el nombre del sistema principal que se está ejecutando en el servidor. Por ejemplo, si el cliente y el servidor se encuentran en el mismo sistema, el nombre de host será `sistema principal local`.
   c. Introduzca el número de puerto que debe supervisarse, que es el puerto al que el cliente enviaría solicitudes si la supervisión TCP/IP no estuviera habilitada. Por ejemplo, el número de puerto predeterminado es `9080` paraIBM WebSphere Application Server.

d. Seleccione el tipo de supervisión **HTTP** o **TCP/IP**. **TCP/IP** muestra los mensajes HTTP completos, incluyendo las cabeceras HTTP y los mensajes SOAP. **HTTP** sólo muestra los mensajes SOAP.

e. Pulse **Aceptar**.

5. En la ventana Preferencias del Supervisor TCP/IP que se abrirá, seleccione el supervisor y pulse **Iniciar** para comenzar la supervisión.
6. En el **Explorador de proyectos** expanda **Servicios web JSR-109** > **Clientes**, pulse con el botón derecho del ratón sobre el cliente de prueba y seleccione **Abrir**.
7. Seleccione el método **getEndpoint()** y pulse **Invocar**. Copie el URL de punto final devuelto.
8. Seleccione el método**setEndpoint()**, pegue el URL de punto final previamente devuelto por el método **getEndpoint()** y cambie el número de puerto para que apunte al número de puerto del Supervisor TCP/IP. Pulse **Invocar**. Por ejemplo, si el nombre de host y el número de puerto local es 13557, el punto final será `http://localhost:13557/wisd/MyApp/MyService`.
9. Invoque su servicio con el cliente de prueba utilizando uno de los siguientes métodos:
   - En **Cliente de prueba de servicios web**, seleccione un método que se haya definido en el servicio, introduzca algún número de entrada y pulse **Invocar**.
   - Para invocar el cliente de prueba sin utilizar la herramienta de conjunto, utilice un navegador web e introduzca el URL `https://`*`nombreHost`*`:`*`puertoCanalSSLWAS`*`/`*`nombreAplicación`*`/muestra`*`nombreServicio`*`PortTypeProxy/TestClient.jsp`en el campo de dirección.

     nombreHost
     El nombre del servidor que hospeda al cliente de prueba (sistema principal local, por ejemplo).

     puertoCanalSSLWAS
     El número de puerto utilizado por el canal de transporte SSL (9443 es el valor predeterminado).

     nombreAplicación
     El nombre del cliente de prueba.

     nombreServicio
     El nombre del servicio que desea invocar.
10. Tras invocar el servicio, analice los mensajes de HTTP y SOAP en la ventana Supervisor TCP/IP para solucionar los problemas que se produzcan en el servicio.

Comparación de tecnologías de seguridad

Para elegir una tecnología que se adapte a sus necesidades, puede comparar tecnologías de seguridad utilizando dos parámetros: el grado de seguridad que ofrece y el grado de dificultad para configurarlo.

Normalmente, una tecnología es más difícil de implementar cuando se basa en la criptografía de clave pública, que requiere la configuración de una infraestructura de claves públicas (PKI). Este es el caso de cualquier tipo de firma digital y de cifrado. Sin embargo, estas tecnologías generalmente ofrecen un mejor nivel de seguridad que otras tecnologías que podrían requerir menos trabajo de infraestructura.

Tabla 5. Métodos de autenticación y sus niveles de seguridad

Método de autenticación	**Nivel**	**Grado de seguridad proporcionado**	**Grado de dificultad que debe configurarse**	**Notas**
Autenticación básica HTTP	Transporte	bajo	bajo	El nombre de usuario y la contraseña se envían en texto común (base64) a través de la red. Sólo se utiliza en redes seguras (HTTPS o intranet).
Autenticación de resumen HTTP (no soportada por IBM WebSphere Application Server)	Transporte	medio	medio	El nombre de usuario y la contraseña están cifrados.
Señal de nombre de usuario	Mensaje	bajo	medio	El nombre de usuario y la contraseña se envían en texto común a través de la red. Sólo se utiliza en redes seguras(HTTPS, intranet o cifrado XML).
Señal de certificado X.509	Mensaje	alto	medio	Requiere una infraestructura de claves públicas.
Señal de ticket de Kerberos	Mensaje	alto	alto	Requiere una infraestructura de Kerberos.

Tabla 6. Método de autorización y su nivel de seguridad

Método de autorización	**Nivel**	**Grado de seguridad proporcionado**	**Grado de dificultad que debe configurarse**	**Notas**
Restricciones de seguridad declarativa J2EE	Aplicación	medio	medio	No requiere ninguna infraestructura de seguridad.

Las restricciones de seguridad declarativa J2EE son fáciles de configurar (sólo requieren cambios en los descriptores de despliegue J2EE) y, al mismo tiempo propocionan un buen nivel de control de accesos. A menudo constituyen el punto de inicio para poder asegurar los servicios.

Tabla 7. Método de confidencialidad y nivel de seguridad

Método de confidencialidad	Nivel	Grado de seguridad proporcionado	Grado de dificultad que debe configurarse	Notas
SSL	Transporte	medio	medio	Requiere una infraestructura de claves públicas. La confidencialidad se suministra de punto de red a punto de red.

SSL y seguridad de la capa de transporte (TLS) proporcionan características de seguridad adicionales en la parte superior del cifrado, incluyendo soporte de autenticación, de protección de datos y de señal criptográfica para conexiones HTTP seguras.

El cifrado es una operación de cálculo intensivo que puede afectar al rendimiento. También incrementa la sobrecarga de gestión y administración. Por tanto, debe utilizarse después de haber prestado la debida consideración a su aplicabilidad.

Tabla 8. Método de integridad digital y su nivel de seguridad

Método de integridad de datos	Nivel	Grado de seguridad proporcionado	Grado de dificultad que debe configurarse	Notas
Firma digital XML	Mensaje	alto	medio	Requiere una infraestructura de claves públicas

La firma digital es una operación de cálculo intensivo que puede desencadenar problemas de rendimiento. También incrementa la sobrecarga de gestión y administración. Por tanto, debe utilizarse después de haber prestado la debida consideración a su aplicabilidad.

Tecnologías de seguridad y enlaces

No todas las tecnologías de seguridad están disponibles para todos los enlaces.

Para algunos enlaces, sólo un subconjunto de la lista completa de tecnologías de seguridad existentes podría estar disponible (o podría ser aplicable). Por ejemplo, ninguna de las tecnologías de seguridad de servicios web puede aplicarse al enlace EJB. La siguiente tabla resume las tecnologías de seguridad disponibles por enlace.

Tabla 9. Tecnologías de seguridad y enlaces

	Tecnología de seguridad	EJB	SOAP sobre HTTP	SOAP sobre JMS	Texto sobre JMS
Autenticación	JAAS/EJB	Disponibles			
Autenticación	HTTP Basic		Disponibles		

Tabla 9. Tecnologías de seguridad y enlaces (continuación)

	Tecnología de seguridad	**EJB**	**SOAP sobre HTTP**	**SOAP sobre JMS**	**Texto sobre JMS**
Autenticación	Resumen HTTP		No soportado por IBM WebSphere Application Server 6.0 ni posteriores		
Autenticación	Señal de nombre de usuario de seguridad de servicios web		Disponibles	Disponibles	
Autenticación	Otra seguridad de servicios web (Kerberos, X509, LTPA, SAML)		Disponibles	Disponibles	
Autorización	J2EE	Disponibles	Disponibles	Disponibles	Disponibles
Confidencialidad de datos	HTTPS y SSL	Disponibles	Disponibles	Disponibles	Disponibles

Accesibilidad de los productos

Puede obtener información sobre el estado de accesibilidad de los productos de IBM.

Los módulos y las interfaces de usuario de los productos de IBM InfoSphere Information Server no son totalmente accesibles. El programa de instalación instala los siguientes módulos y componentes del producto:

- IBM InfoSphere Business Glossary
- IBM InfoSphere Business Glossary Anywhere
- IBM InfoSphere DataStage
- IBM InfoSphere FastTrack
- IBM InfoSphere Information Analyzer
- IBM InfoSphere Information Services Director
- IBM InfoSphere Metadata Workbench
- IBM InfoSphere QualityStage

Para obtener información sobre el estado de accesibilidad de los productos de IBM, consulte la información de accesibilidad de productos de IBM en http://www.ibm.com/able/product_accessibility/index.html.

Documentación accesible

Se proporciona documentación accesible sobre los productos de InfoSphere Information Server en un Information Center. El Information Center presenta la documentación en formato XHTML 1.0, que se puede ver en la mayoría de navegadores web. El formato XHTML permite establecer propiedades de visualización en el navegador. También permite utilizar lectores de pantalla y otras tecnologías de asistencia para acceder a la documentación.

IBM y la accesibilidad

Consulte el IBM Human Ability and Accessibility Center para obtener más información sobre el compromiso de IBM con respecto a la accesibilidad.

Acceso a la documentación de productos

La documentación se proporciona en diversas ubicaciones y formatos, también en la ayuda que se abre directamente desde la interfaz del producto, en un Information Center para toda la suite y en manuales en archivos PDF.

El Information Center se instala como un servicio común con IBM InfoSphere Information Server. El Information Center contiene una ayuda para la mayoría de interfaces del producto, así como documentación completa para todos los módulos de productos de la suite. Puede abrir el Information Center desde el producto instalado o bien desde un navegador Web.

Acceso a Information Center

Puede utilizar los métodos siguientes para abrir el Information Center instalado.

- Pulse el enlace **Ayuda** de la parte superior derecha de la interfaz de cliente.

  Nota: Desde IBM InfoSphere FastTrack e IBM InfoSphere Information Server Manager, el elemento Ayuda principal abre un sistema de ayuda local. Seleccione **Ayuda > Abrir Information Center** para abrir el Information Center de toda la suite.
- Pulse la tecla F1. La tecla F1 abre generalmente el tema que describe el contexto actual de la interfaz de cliente.

  Nota: La tecla F1 no funciona en clientes Web.
- Utilice un navegador Web para acceder al Information Center instalado, aunque no haya iniciado sesión en el producto. Especifique la siguiente dirección en un navegador Web: http://host_name:port_number/infocenter/topic/com.ibm.swg.im.iis.productization.iisinfsv.home.doc/ic-homepage.html. El nombre_host es el nombre del sistema de capa de servicios en el que está instalado en Information Center, y número_puerto es el número de puerto para InfoSphere Information Server. El número de puerto predeterminado es 9080.Por ejemplo, en un sistema Microsoft® Windows® Server denominado iisdocs2, la dirección Web tendrá este formato: http://iisdocs2:9080/infocenter/topic/com.ibm.swg.im.iis.productization.iisinfsv.nav.doc/dochome/iisinfsrv_home.html.

También hay disponible un subconjunto del Information Center, que se renueva periódicamente, en el sitio web de IBM http://publib.boulder.ibm.com/infocenter/iisinfsv/v8r7/index.jsp.

Obtener la documentación en PDF y en copia impresa

- También puede disponer de un subconjunto de manuales en archivos PDF mediante el instalador de software de InfoSphere Information Server y el soporte de distribución. El resto de manuales en archivos PDF está disponible en línea y pueden accederse desde este documento de soporte: https://www.ibm.com/support/docview.wss?uid=swg27008803&wv=1.
- También puede solicitar publicaciones de IBM en formato impreso, ya sea en línea o a través de su representante local de IBM. Para solicitar publicaciones en línea, vaya al Centro de publicaciones de IBM en http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss.

Facilitar comentarios sobre la documentación

Puede enviar sus comentarios sobre la documentación de la siguiente manera:

- Formulario de comentarios en línea de los lectores: www.ibm.com/software/data/rcf/
- Correo electrónico: comments@us.ibm.com

Enlaces a sitios web que no son de IBM

Este Information Center le proporciona enlaces o referencias sitios web y recursos que no son de IBM.

IBM no representa, garantiza ni se compromete en forma alguna en lo que respecta a los sitios web que no son de IBM o a los recursos de terceros (incluyendo cualquier sitio web de Lenovo) a los que se pueda hacer referencia, ofrecer acceso o tengan enlaces a cualquier sitio de IBM. Un enlace a un sitio que no es de IBM no implica que IBM apoye el uso o los contenidos del sitio web o de su propietario. Asimismo, IBM no es parte ni responsable de las transacciones que usted pueda realizar con terceros, incluso si ha recibido información de los mismos (o utilizado un enlace a éstos) procedente de un sitio de IBM. Por consiguiente, acepta que IBM no se hace responsable de la disponibilidad de los mencionados sitios o recursos externos, ni de los contenidos, servicios, productos u otros materiales disponibles procedentes de estos sitios o recursos.

Cuando accede a un sitio web que no es de IBM, aunque alguno contenga el logotipo de IBM, es independiente de IBM, e IBM no controla el contenido de ese sitio web. Es responsabilidad del usuario tomar las precauciones necesarias para protegerse de virus, gusanos, troyanos y otros programas potencialmente destructivos, así como de proteger la información como estime oportuno.

Avisos y marcas registradas

La presente información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Avisos

Es posible que IBM no comercialice en otros países los productos, servicios o características que se describen en este manual. Consulte al representante local de IBM para obtener información sobre los productos y servicios que actualmente pueden adquirirse en su zona. Cualquier referencia a un producto, programa o servicio de IBM no pretende afirmar ni implicar que sólo se pueda utilizar dicho producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patentes en tramitación que afecten al tema tratado en este documento. La posesión de este documento no otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a la siguiente dirección:

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

Para formular consultas relacionadas con el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de la propiedad intelectual de IBM de su país o envíe las consultas, por escrito, a la siguiente dirección:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japón

El párrafo siguiente no es aplicable al Reino Unido ni a ningún país en donde tales disposiciones sean incompatibles con la legislación local:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN TAL CUAL, SIN GARANTÍA DE NINGUNA CLASE, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN DE DERECHOS, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN DETERMINADO. Algunos estados no permiten la declaración de limitación de responsabilidad de garantías expresas o implícitas en determinadas transacciones. Por consiguiente, es posible que esta declaración no se aplique en su caso.

Esta información podría contener imprecisiones técnicas o errores tipográficos. La información de este documento está sujeta a cambios periódicos; dichos cambios se incorporarán en nuevas ediciones de la publicación. Es posible que IBM realice

mejoras o efectúe cambios en el(los) producto(s) y/o el(los) programa(s) descritos en esta publicación en cualquier momento sin previo aviso.

Las referencias hechas en esta publicación a sitios Web que no son de IBM se proporcionan sólo para la comodidad del usuario y no constituyen un aval de esos sitios Web. La información contenida en estos sitios Web no forma parte de la información del presente producto IBM, y el usuario es responsable de la utilización de dichos sitios.

IBM puede utilizar o distribuir cualquier información que se le facilite de la manera que considere adecuada, sin contraer por ello ninguna obligación con el remitente.

Los licenciatarios de este programa que deseen obtener información sobre él con el fin de habilitar: (i) el intercambio de información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deben ponerse en contacto con:

IBM Corporation
J46A/G4
555 Bailey Avenue
San José, CA 95141-1003 EE.UU.

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

El programa bajo licencia descrito en este documento y todo el material bajo licencia asociado a él los proporciona IBM según los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas Bajo Licencia de IBM o cualquier acuerdo equivalente entre el usuario e IBM.

Los datos de rendimiento contenidos en este documento se obtuvieron en un entorno controlado. Por consiguiente, es posible que los resultados obtenidos en otros entornos operativos varíen de forma significativa. Algunas mediciones pueden haberse efectuado en sistemas a nivel de desarrollo, y no existe ninguna garantía de que dichas mediciones sean las mismas en sistemas de disponibilidad general. Además, es posible que algunas mediciones se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información relacionada con productos ajenos a IBM se ha obtenido a partir de los proveedores de dichos productos, los anuncios que han publicado u otras fuentes de dominio público. IBM no ha probado dichos productos ni puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación sobre productos ajenos a IBM. Las preguntas sobre las prestaciones de productos que no son de IBM deben dirigirse a los proveedores de esos productos.

Todas las declaraciones de intenciones de IBM están sujetas a cambio o cancelación sin previo aviso, y sólo representan objetivos.

Esta información sólo tiene como objeto la planificación. La información de este documento está sujeta a cambios antes de que los productos descritos estén disponibles.

Este manual contiene ejemplos de datos e informes que se utilizan en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos

incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres y direcciones utilizados por una empresa real es totalmente fortuita.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en código fuente que ilustran técnicas de programación en diferentes plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma, sin pagar a IBM, con la finalidad de desarrollar, utilizar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones para la plataforma operativa para la que se han escrito los programas de ejemplo. Estos ejemplos no se han probado bajo todas las condiciones posibles. IBM, por lo tanto, no puede garantizar ni dar por sentada la fiabilidad, la capacidad de mantenimiento ni el funcionamiento de dichos programas. Los programas de ejemplo se suministran "TAL CUAL", sin garantía de ninguna clase. IBM no se hace responsable de los daños que se hayan podido causar debido al uso de los programas de ejemplo.

Todas las copias o partes de estos programas de ejemplo, o cualquier trabajo derivado, deberán incluir un aviso de copyright como el siguiente:

© (nombre de la empresa) (año). Partes de este código provienen de programas de ejemplo de IBM Corp. © Copyright IBM Corp. _entrar el año o los años_. Reservados todos los derechos.

Si está visualizando esta información en copia software, es posible que las fotografías o las ilustraciones en color no aparezcan.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp. en muchos países o regiones de alrededor del mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Encontrará una lista actualizada de las marcas registradas de IBM en www.ibm.com/legal/copytrade.shtml.

Los términos siguientes son marcas registradas de otras compañías:

Adobe es una marca registrada de Adobe Systems Incorporated en los Estados Unidos y/o en otros países.

IT Infrastructure Library es una marca registrada de Agencia Central de Telecomunicaicones e informática and Telecommunications Agency que es ahora parte de la Oficina de Comercio Gubernamental.

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas comerciales o marcas registradas de Intel Corporation o de sus subsidiarias en los Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o otros países.

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

ITIL es un marca registrada y es una marca registrada comunitaria de la Oficina de Comercio Gubernamental, y está registrada en la Oficina de marcas registradas y patentes de los EE.UU.

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

Cell Broadband Engine es una marca registrada de Sony Computer Entertainment, Inc. en los Estados Unidos y/o en otros países y se utiliza bajo la licencia correspondiente.

Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus afiliadas.

El servicio postal de los Estados Unidos (United States Postal Service) es propietario de las siguientes marcas registradas: CASS, CASS Certified, DPV, LACS^{Link}, ZIP, ZIP + 4, ZIP Code, Post Office, Postal Service, USPS y United States Postal Service. IBM Corporation tiene titularidad no exclusiva de licencias de DPV y LACS^{Link} de United States Postal Service.

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

Cómo ponerse en contacto con IBM

Puede ponerse en contacto con IBM para obtener soporte al cliente, servicios de software, información sobre el producto e información general. También puede facilitar comentarios a IBM acerca de productos y documentación.

La siguiente tabla enumera los recursos para soporte al cliente, servicios de software, formación, e información de productos y soluciones.

Tabla 10. Recursos de IBM

Recurso	Descripción y ubicación
Portal de soporte de IBM	Puede personalizar la información de soporte seleccionando los productos y los temas que sean de su interés en www.ibm.com/support/entry/portal/Software/Information_Management/InfoSphere_Information_Server
Servicios de software	Puede encontrar información sobre servicios de software, de tecnologías de la información y de consultoría empresarial en el sitio de soluciones, en www.ibm.com/businesssolutions/
Mi IBM	Puede gestionar enlaces a sitios web de IBM y a información que satisfaga sus necesidades específicas de soporte técnico creando una cuenta en el sitio Mi IBM: www.ibm.com/account/
Formación y certificación	Puede obtener información sobre formación técnica y servicios de educación diseñados para personas, empresas y organizaciones públicas, a fin de adquirir, mantener y optimizar sus habilidades de TI en http://www.ibm.com/software/sw-training/
Representantes de IBM	Puede contactar con un representante de IBM para obtener información sobre soluciones en www.ibm.com/connect/ibm/us/en/

Facilitar comentarios

La tabla siguiente describe la forma en que se facilitan comentarios a IBM acerca de productos y documentación de productos.

Tabla 11. Facilitar comentarios a IBM

Tipo de comentarios	Acción
Comentarios sobre el producto	Puede proporcionar comentarios generales sobre productos mediante la encuesta de consumo en el sitio web www.ibm.com/software/data/info/consumability-survey

Tabla 11. Facilitar comentarios a IBM (continuación)

Tipo de comentarios	Acción
Comentarios sobre la documentación	Para realizar comentarios acerca del Information Center, pulse el enlace Comentarios situado en la parte superior derecha de cualquiera de los temas del Information Center. También puede enviar sus comentarios sobre los manuales en archivos PDF, el Information Center o cualquier otra documentación de los siguientes modos: • Formulario de comentarios en línea de los lectores: www.ibm.com/software/data/rcf/ • Correo electrónico: comments@us.ibm.com

Índice

Impreso en España

SC11-8014-00