WebSphere®

IBM WebSphere Partner Gateway Enterprise Edition y Advanced Edition

Versión 6.2.1

Guía de configuración del concentrador

IBM

Nota

Antes de utilizar esta información y el producto que soporta, lea la información que se incluye en el apartado “Avisos” en la página 469.

Febrero de 2011

Esta edición se aplica a la versión 6, release 2, modificación 1 de IBM WebSphere Partner Gateway Enterprise Edition (número de producto 5724-l69) y a la versión 6, release 2, modificación 1 de Advanced Edition (número de producto 5724-L68) y a todos los releases y modificaciones posteriores, a menos que se indique lo contrario en nuevas ediciones.

Contenido

Capítulo 1. Acerca de esta publicación

Este documento describe cómo configurar el servidor IBM (R) WebSphere (R) Partner Gateway.

A quién va dirigida

Los administradores mantienen WebSphere Partner Gateway. En esta publicación se asumen dos tipos de administradores:

- Administrador del concentrador
- Administrador de cuentas

El administrador del concentrador es el superusuario de la comunidad. El administrador del concentrador es el responsable de toda la configuración y gestión de la comunidad del concentrador, incluidos la configuración del socio y la activación de la conexión. El administrador de cuentas tiene acceso a un subconjunto de dispositivos del administrador del concentrador y es el usuario administrativo principal del el socio interno o externo.

Nota: La consola de Administrador del concentrador, Socios externos y Socios internos variará según los derechos/controles de acceso de quienes lo utilicen.

Convenios tipográficos

En este documento se utilizan los convenios siguientes.

Tabla 1. Convenios tipográficos

Convenio	Descripción
`Fuente monoespaciada`	El texto en este font indica el texto escrito por el usuario, los valores de argumentos u opciones de mandato, ejemplos y ejemplos de código o información que el sistema muestra por pantalla (texto de mensaje o solicitudes).
Negrita	El texto en negrita indica los controles de la interfaz gráfica de usuario (por ejemplo, los nombres de botón en línea, los nombres del menú o las opciones del menú) y las cabeceras de la columna en tablas y texto.
cursiva	El texto en cursiva indica el énfasis, los títulos de publicaciones, los términos nuevos y los que se definen en el texto, los nombres de variable o las letras del alfabeto utilizadas como letras.
`Fuente monoespaciada en cursiva`	El texto que aparece en font monoespaciado en cursiva indica nombres de variables dentro del texto de font monoespaciado.
ProductDir	*ProductDir* representa el directorio en el que está instalado el producto. Todos los nombres de vías de acceso del producto IBM WebSphere Partner Gateway son relativos al directorio en el que está instalado el producto IBM WebSphere Partner Gateway en el sistema.

Tabla 1. Convenios tipográficos (continuación)

Convenio	Descripción
%texto% y *$texto*	El texto entre caracteres de porcentaje (%) indica el valor de la variable de usuario o la variable del sistema de `texto` de Windows(R). La notación equivalente en un entorno UNIX(R) es $*texto*, que indica el valor de la variable de entorno UNIX *texto*.
Texto en color subrayado	El texto en color subrayado indica una referencia cruzada. Pulse en el texto para ir al objeto de referencia.
Texto con contorno azul	(Sólo en archivos PDF) Un contorno alrededor del texto indica una referencia cruzada. Pulse el texto con el contorno para ir al objeto de la referencia. Este convenio es el equivalente para los archivos PDF del convenio "Texto en color subrayado" incluido en esta tabla.
" " (comillas)	(Sólo en archivos PDF) Las comillas rodean las referencias cruzadas con otros apartados del documento.
{ }	En una línea de sintaxis, las llaves señalan un conjunto de opciones de entre las que debe seleccionar sólo una.
[ ]	En una línea de sintaxis, se colocan corchetes alrededor de parámetros opcionales.
< >	Los corchetes angulares se colocan alrededor de un elemento de variable para distinguirlos entre ellos. Por ejemplo, <*nombre_servidor*><*nombre_conector*>`tmp.log`.
/ o \	Las barras inclinadas invertidas (\) se utilizan como separadores en las vías de acceso de directorios en instalaciones Windows. Para las instalaciones en UNIX, sustituya las barras inclinadas (/) por barras inclinadas invertidas.

Documentos relacionados

La documentación completa que se proporciona con este producto incluye información exhaustiva sobre la instalación, la configuración, la administración y la utilización de WebSphere Partner Gateway Enterprise Edition y Advanced Edition.

Puede descargar la documentación o leerla directamente en línea en el sitio siguiente:

http://www.ibm.com/software/integration/wspartnergateway/library/

Nota: Puede encontrar información importante sobre este producto en las Notas técnicas de soporte técnico y las Noticias de último momento publicadas posteriormente a este documento. Las encontrará en el sitio web de soporte de WebSphere Business Integration:

http://www.ibm.com/software/integration/wspartnergateway/support/

Seleccione el área del componente que desee y examine los apartados de Technotes y Flashes.

Novedades del release 6.2.1

WebSphere Partner Gateway V6.2.1 da soporte a las características nuevas siguientes:

- El correo electrónico Web (Web Mail) tiene soporte en línea para permitir la interacción B2B. Socios, clientes y proveedores interactúan con el concentrador de WebSphere Partner Gateway utilizando solo el navegador de Internet.
- Soporte del servidor integrado SFTP además del servidor FTP integrado.
- En WebSphere Partner Gateway se da soporte al certificado OpenPGP.
- Soporte para WebSphere Application Server ND V7.0.0.13, WebSphere Messaging Queue 7.0 y WTX 8.3.
- Soporte de plataforma para Windows 2008, Windows 7 y SLES 11.
- Soporte Power 7 - Modalidad de tolerancia (P6/P6+ Modalidades compatibles).
- Soporte de virtualización - VMware® ESX con Windows y Linux, Power VM con AIX.

Capítulo 2. Introducción a la configuración del concentrador

Después de instalar WebSphere Partner Gateway y antes de poder intercambiar cualquier documento entre los socios internos y los socios externos, deberá configurar el servidor de WebSphere Partner Gateway (el concentrador).

Este capítulo incluye los siguientes temas:

Visión general de la configuración del concentrador

El objetivo es habilitar el socio interno para que envíe un documento o conjunto de documentos (electrónicamente) a un socio externo o para recibir un documento o conjunto de documentos enviado por un socio externo. El concentrador gestiona la recepción de los documentos, la transformación en otros formatos (si fuera preciso) y la entrega de los documentos. El concentrador también puede ser configurado para proporcionar seguridad para documentos entrantes o salientes.

Los documentos intercambiados entre el concentrador y un socio están generalmente en un formato estándar y representan una interacción de empresa específica. Por ejemplo, un socio puede enviar una solicitud de pedido de compra como 3A4 PIP de RosettaNet, un documento OrderRequest cXML o un intercambio EDI-X12 con una transacción 850. El concentrador transforma el documento en un formato que una aplicación puede utilizar en el socio interno. De forma similar, una aplicación de programa de fondo de socio interno puede enviar una respuesta de pedido de compra en su propio formato personalizado, que se transformará en un formato estándar. El documento transformado se envía entonces al socio.

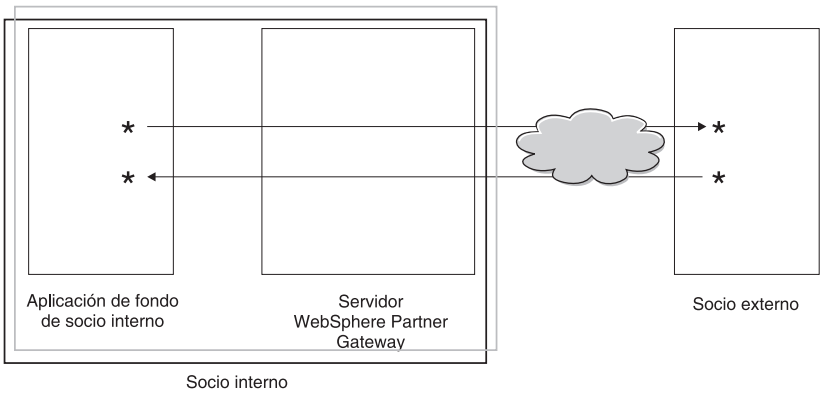


Figura 1. Cómo fluyen los documentos a través del concentrador

En esta publicación, se explica cómo configurar el concentrador y, a continuación, cómo establecer los socios. También se muestra cómo configurar la seguridad del concentrador.

Observe en la Figura 1 en la página 5 que el servidor de WebSphere Partner Gateway y la aplicación de fondo del socio interno son propiedad del socio interno. El socio interno es la empresa propietaria del concentrador. Como verá en capítulos posteriores, se define un perfil para los socios internos de la misma manera que lo haría para socios externos.

Nota: En este documento se muestra cómo crear conexiones que fluyen de la aplicación de programa de fondo de socio interno a un destino de socio, y de un socio externo al destino de socio interno. Una vez los documentos llegan al destino del socio interno, es posible que desee integrarlos con una aplicación de programa de fondo, como WebSphere InterChange Server o WebSphere MQ Broker. Las tareas necesarias para realizar la integración entre WebSphere Partner Gateway y dichas aplicaciones de programas de fondo se definen en la publicación *Guía de integración empresarial de WebSphere Partner Gateway*.

Información necesaria para configurar el concentrador

Para configurar el concentrador, necesita alguna información sobre los tipos de intercambios en los que participará el socio interno. Por ejemplo, necesita la información siguiente:

- ¿Qué tipos de documentos (por ejemplo, EDI-X12 o XML personalizado) enviarán los socios internos y sus socios externos a través del concentrador?
- ¿Qué tipos de transportes (por ejemplo, HTTP o FTP) utilizarán los socios internos y sus socios externos para enviar los documentos?
- ¿Será necesario dividir en varios documentos un documento que llega al concentrador o será necesario agrupar los documentos individuales que llegan al concentrador antes de enviarlos?
- ¿Se transformarán los documentos antes de entregarse?
- ¿Se validarán los documentos antes de entregarse?
- ¿Se comprobará un documento para ver si es un duplicado antes de ser entregado?
- ¿Se cifrarán o firmarán digitalmente los documentos o se utilizará alguna otra técnica de seguridad?

Una vez que se determina esta información, ya puede empezar a configurar el concentrador.

Después de definir el concentrador, puede definir los socios externos utilizando información (como una dirección IP y números de DUNS) proporcionada por los socios externos. Como se ha indicado anteriormente, también se define el socio interno como un tipo especial de socio de concentrador.

Visión general de transportes

Los documentos pueden enviarse desde socios a WebSphere Partner Gateway (el concentrador) a través de una gran variedad de transportes. Un socio puede enviar documentos a través de redes públicas utilizando HTTP, HTTPS, JMS, FTP, FTPS, FTP Scripting, SMTP, SFTP o un directorio de archivos. Un socio puede enviar documentos a través de una VAN (Value Added Network), una red privada, utilizando el transporte FTP Scripting. También es posible crear su propio transporte.

Nota: cuando se utiliza el directorio de archivos entre un socio y un concentrador, el administrador debe ocuparse de todos los temas relacionados con la seguridad.

Asimismo, el concentrador envía documentos a aplicaciones de fondo a través de diversos transportes. Los transportes más utilizados frecuentemente entre el concentrado y las aplicaciones de fondo son: HTTP, HTTPS, JMS, directorio de archivos, script de FTP, FTP, SFTP y SMTP.

La Figura 2 muestra los transportes HTTP, HTTPS, JMS y de directorio de archivos.

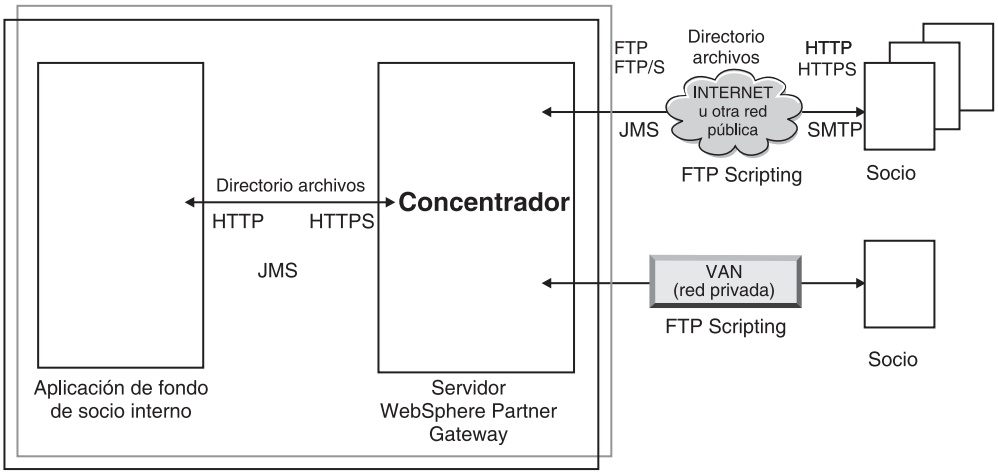


Figura 2. Los transportes más comunes soportados por WebSphere Partner Gateway

El tipo de transporte utilizado para enviar y recibir documentos que afectan a la configuración de receptores y destinos. Un *receptor* es un punto de entrada en el concentrador, el lugar donde los documentos enviados por socios o aplicaciones de fondo son recibidos en el concentrador. Un *destino* es un punto de entrada en el sistema del socio en el sistema del programa de fondo donde el concentrador envía documentos. Para preparar la utilización de los transportes FTP, FTPS, FTP Scripting, JMS y directorio de archivos, debe realizar algún trabajo de configuración, como se describe en el apartado Capítulo 4, “Preparación para la configuración del concentrador”, en la página 35.

Visión general de las definiciones de documento

Cuando configure el intercambio de documentos entre socios externos y socios internos, especifique varias cosas acerca del documento:

- El *paquete* que rodea al documento
- El *protocolo* de empresa que define una clase de documentos que comparten algunas características comunes
- El *tipo de documento* que identifica uno de los documentos proporcionados por el protocolo empresarial

El empaquetado del documento, el protocolo del documento y el tipo de documento conforman la *definición del documento*. Suponga que utiliza la definición de documento proporcionada con el producto de:

- Paquete: AS
- Protocolo: EDI-X12
- Tipo de documento: ISA

Esto es lo que sucede cuando se recibe un documento que cumple con esta definición de direccionamiento. Una vez el concentrador recibe el documento, el

paso de desempaquetado de flujo de trabajo entrante fijo determina que se ha utilizado el paquete AS con el documento. Esto se debe a la presencia de cabeceras de transporte especificadas para el empaquetado AS. El concentrador descubre otros tipos de empaquetado de una manera parecida, generalmente examinando las cabeceras de transportes incluidas en el documento. Cuando no coincide con ningún tipo de empaquetamiento, se asignará el tipo de paquete Ninguno al documento. En el caso del empaquetamiento AS, los identificadores de empresa De y A se obtienen a partir de las cabeceras de transporte del mensaje. También incluido en las cabeceras de transporte AS se encuentran otras cabeceras que puede especificar si el mensaje está o no cifrado, comprimido o firmado.

Después de identificar el empaquetado, el paso de análisis entrante fijo del concentrador determina el protocolo y el tipo de documento del documento. Esto se hace examinando el contenido real del mensaje y buscando características en el documento que identifican el protocolo y el tipo de documento. El paso de flujo de trabajo de análisis de protocolo también extrae otra información del documento dependiendo del protocolo utilizado.

Una vez se sabe que el documento utiliza un paquete, protocolo o tipo de documento determinado, el concentrador puede seguir procesando el documento. En este punto se conocerán los ID de empresa De y A además del paquete, protocolo y tipo de documento. Con esta información, el concentrador puede buscar una conexión entre los socios De y A que tenga el paquete entrante, protocolo y tipo de documento.

Una vez se ha encontrado la conexión, el concentrador sabe cómo direccionar y procesar el documento ya que puede encontrar la siguiente información adicional:

- Certificados para los socios de origen y de destino (si es necesario)
- Valores de atributos para el direccionamiento de origen y el direccionamiento de destino
- La Acción que debe realizarse cuando se direccione el documento
- La correlación de transformación correspondiente (si hay alguna)
- La correlación de validación correspondiente (si hay alguna)

Paquete

El empaquetado proporciona información que pertenece a la transmisión del documento. Tal como se ha mencionado en el apartado anterior, si el empaquetado es AS, el concentrador utiliza información de la cabecera AS para determinar el origen y destino para el documento. Si un socio envía un PIP de RosettaNet al socio interno, el PIP se empaquetará como RNIF.

La Figura 3 en la página 9 muestra los tipos de empaquetado que pueden configurarse para los documentos intercambiados entre el concentrador y un socio externo y entre el concentrador y una aplicación de fondo.

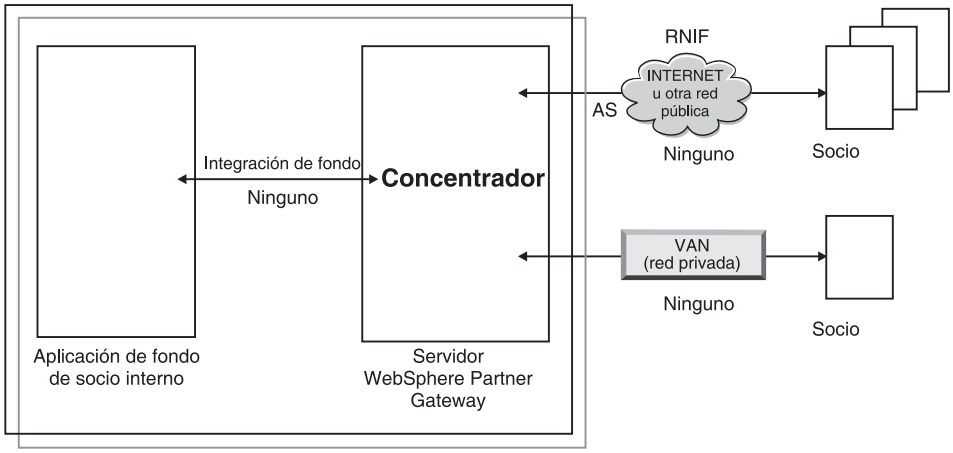


Figura 3. Tipos de paquetes de documentos

Los paquetes se asocian con protocolos específicos. Por ejemplo, un socio debe especificar un empaquetado RNIF cuando se envía un documento de RosettaNet al concentrador.

Integración de programas de fondo: Tal como se muestra en la Figura 3, la integración de programas de fondo sólo están disponibles entre el concentrador y la aplicación de fondo. Al especificar el empaquetado de integración de programas de fondo, a los documentos enviados por el concentrador al sistema de fondo se incluye información de cabecera especial añadida. Asimismo, cuando una aplicación de fondo envía documentos con un paquete de integración de programas de fondo al concentrador, debe añadir información de cabecera. El paquete de integración de programas de fondo y los requisitos para la información de cabecera se describen en la publicación *Guía de integración empresarial de WebSphere Partner Gateway*.

AS: El paquete AS es el más comúnmente utilizado entre socios y el concentrador. El paquete AS puede ser utilizado para aquellos documentos que cumplan con los estándares AS1, AS2 y AS3. AS1 es un estándar que se utiliza para transmitir de forma segura documentos a través de SMTP y AS2 es un estándar utilizado para transmitir de forma segura documentos a través de HTTP o HTTPS. AS3 es un nuevo estándar utilizado para transmitir documentos de forma segura a través de FTP o FTPS. Los documentos enviados por un socio con un empaquetado AS tienen información de cabecera AS1, AS2 o AS3. Los documentos enviados a un socio que espera cabeceras AS1, AS2 o AS3 deben estar empaquetados (en el concentrador) como AS.

Ninguno: El paquete Ninguno puede ser utilizado para enviar y recibir documentos entre el concentrador y los socios y entre el concentrador y una aplicación de fondo. Cuando un documento está empaquetado como Ninguno, no se añade (ni se espera) ninguna información de cabecera.

RNIF: El paquete RNIF se proporciona en el soporte de instalación. El paquete RNIF se sube (junto con cualquier PIP que desee intercambiar), tal y como se describe en el apartado “documentos de RosettaNet” en la página 114. El paquete RNIF se utiliza para enviar documentos de RosettaNet del socio al concentrador o del concentrador al socio.

ebMS: El mecanismo ebXML Message Service (ebMS) proporciona una forma estándar de intercambiar mensajes empresariales entre los socios comerciales de

ebXML. Proporciona una manera fiable de intercambiar mensajes de empresa sin basarse en tecnologías y soluciones de propiedad. Un mensaje ebXML contiene estructuras de una cabecera de mensaje (necesaria para el direccionamiento y entrega) y una sección de carga.

ebMS proporciona una forma estándar de intercambiar mensajes empresariales entre socios comerciales de ebXML. Un mensaje ebXML es un sobre de mensaje MIME/Multipart independiente del protocolo de comunicaciones.

N/D: Algunos tipos de documentos terminan en WebSphere Partner Gateway o se originan internamente en WebSphere Partner Gateway. Para aquellos tipos de documentos que finalizan en WebSphere Partner Gateway, no es necesario ningún empaquetado. Los tipos de documentos que se originan internamente WebSphere Partner Gateway no tienen empaquetamiento de origen. Por lo tanto, para dichos flujos, el empaquetado se especifica como N/D.

Para la mayoría de las transmisiones unidireccionales entre un socio externo y el socio interno (o viceversa), WebSphere Partner Gateway recibe un documento de un socio externo y se lo envía al socio interno. En WebSphere Partner Gateway, al crear la conexión de socio, se especifica el empaquetamiento en el que WebSphere Partner Gateway recibirá el documento y el empaquetamiento que WebSphere Partner Gateway utilizará para enviar el documento. En la Figura 4, un documento empaquetado como AS fluye de un socio externo al programa de fondo del socio interno. El documento se entrega en el destino del socio interno sin cabeceras de transporte. En la Figura 4, hay una actividad acción asociada al intercambio de documentos.

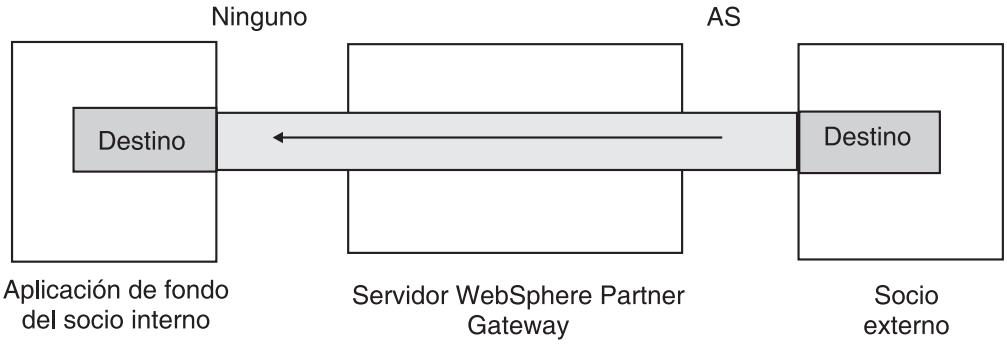


Figura 4. Conexión unidireccional típica

Sin embargo, determinados protocolos implican múltiples operaciones (como desensobrar y transformar), algunas de las cuales se ejecutan como partes intermedias del intercambio global. Por ejemplo, si un socio envía un intercambio EDI al concentrador, correspondiente a una entrega ocasional al socio interno, el intercambio se desensobra y se procesan las transacciones EDI individuales. El intercambio EDI original tiene un paquete asociado cuando se envía desde el socio. No obstante, puesto que el intercambio en sí mismo no se entrega al socio interno (se desensobra dentro del concentrador y no se produce ningún proceso adicional en el intercambio), el intercambio no se empaqueta. Por eso, cuando establece la interacción para el paso de desensobrado, especificará un paquete en el lado que envía aunque especificará N/D para el lado que recibe.

El proceso para configurar las definiciones de documento necesarias para un intercambio EDI se describe en el apartado Capítulo 10, “Configuración de flujos de documentos EDI”, en la página 173.

Protocolos

Los protocolos que se proporcionan con el sistema son:

- Binario

  El protocolo Binario puede utilizarse con los paquetes AS, Ninguno y de integración de programas de fondo. Un documento binario no contiene datos sobre el origen o el destino del documento.

- EDI-X12, EDI-Consent, EDI-FACT

  Estos protocolos EDI pueden utilizarse con los paquetes AS o Ninguno. Como se describe en el apartado “ N/D” en la página 10, si el intercambio o la transacción EDI se origina en el concentrador o finaliza en el concentrador, debe especificar N/D para el paquete. X12 y EDIFACT son estándares EDI utilizados para el intercambio de datos. EDI-Consent hace referencia a los tipos de contenido que se especifican en la especificación EDI-Consent.

- Servicio web

  Las peticiones de servicio web sólo pueden utilizarse con el paquete Ninguno.

- cXML

  Los documentos de cXML sólo pueden utilizarse con el paquete Ninguno.

- XMLEvent

  XMLEvent es un protocolo especial que se utiliza para proporcionar notificación de sucesos para los documentos que fluyen hacia y desde una aplicación de fondo. Sólo puede utilizarse con el paquete de integración de programas de fondo. Este protocolo se describe en la publicación *Guía de integración empresarial de WebSphere Partner Gateway*.

Al subir paquetes RNIF, también se obtienen los protocolos asociados (RosettaNet y RNSC). RosettaNet (que es el protocolo utilizado entre el socio y el concentrador) está asociado con el paquete RNIF. RNSC (que es el protocolo utilizado entre el concentrador y la aplicación de fondo del socio interno) se asocia al paquete de integración del programa de fondo.

Para obtener información acerca de las transacciones EDI o de documentos XML o ROD, el cliente de Data Interchange Services (DIS) o el estudio de diseño WTX se utiliza para crea correlaciones de transformación.

En Data Interchange Services Client, los diccionarios se definen para el protocolo asociado con esta transformación. Un diccionario contiene información sobre todas las definiciones de documento EDI, segmentos, elementos de datos compuestos y elementos de datos que forman el estándar EDI. WDI proporciona las definiciones de los documentos fuente de EDI, mientras que para ROD y XML deberá crearlas en el cliente DIS. A partir de la versión 6.2.1, las correlaciones estándar y de transformación se pueden compilar por separado. Si desea información detallada sobre un estándar EDI concreto, consulte las publicaciones EDI correspondientes. Para obtener información sobre Data Interchange Services Client, consulte la publicación *WebSphere Partner Gateway Mapping Guide* o la ayuda en línea que se proporciona con Data Interchange Services Client.

Nota: los ID de emisor y receptor deben formar parte de la definición de documentos ROD asociada a la correlación de transformación. La información necesaria para determinar el tipo de documento y los valores de diccionario también deben estar en la definición de documento. Asegúrese de que el

especialista de correlaciones de Data Interchange Services Client conoce estos requisitos al crear la correlación de transformación.

Puede crear protocolos personalizados que definan exactamente cómo desea que se estructure un documento. Para los documentos XML, puede definir un formato XML, como se describe en el apartado "Proceso de documentos de XML personalizado" en la página 159.

Tipo de documento

El documento puede tener distintos formatos. Los tipos de documentos proporcionados por el producto y sus protocolos asociados son:

- Binario, que puede utilizarse con el protocolo Binario.
- ISA, que representa el intercambio X12 (sobre) y que está asociado al protocolo EDI-X12
- BG, que representa el sobre EDI-Consent y que está asociado al protocolo EDI-Consent
- UNB, que representa el sobre EDIFACT y que está asociado al protocolo EDI-EDIFACT
- XMLEvent, que puede utilizarse con el protocolo XMLEvent

La siguiente lista describe otros tipos de documentos y el origen de su definición:

- Un PIP de RosettaNet (que sube desde el soporte de instalación), que puede utilizarse con el protocolo RosettaNet
- Un servicio web (que sube como archivo WSDL), que puede utilizarse con el protocolo de servicios web
- Un documento cXML (que se crea especificando el tipo de documento cXML)
- Una transacción estándar EDI específica, que se importa de Data Interchange Services Client
- Datos orientados a registro (ROD) o un documento XML, que se importa de Data Interchange Services Client

También puede crear sus propios tipos de documentos, tal y como se describe en el apartado "Proceso de documentos de XML personalizado" en la página 159.

Visión general del proceso de documentos

Antes de empezar a configurar el concentrador, resulta útil revisar los componentes de WebSphere Partner Gateway y cómo se utilizan para el proceso de documentos.

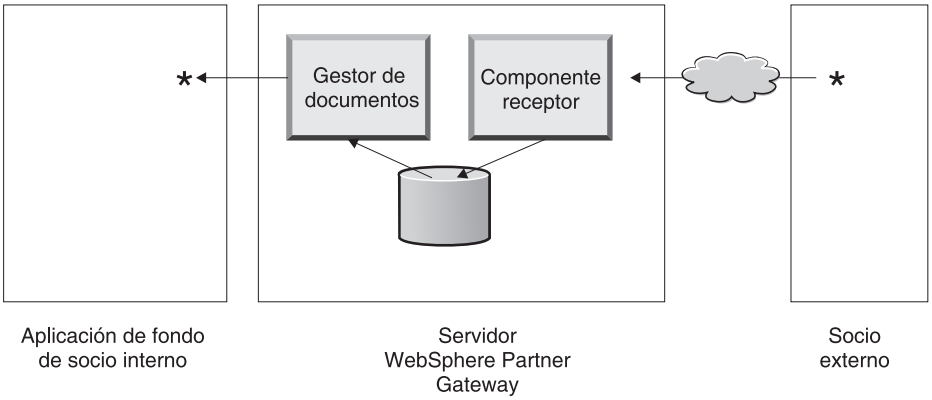


Figura 5. Los componentes Receptor y Gestor de documentos

La Figura 5 es un ejemplo de cómo se envía un documento desde un socio, se recibe en el concentrador, se procesa en el concentrador y se envía a una aplicación de fondo del socio interno.

Nota: a efectos de ilustración, los dibujos en este documento muestran un componente Receptor y un Gestor de documentos, instalados en el mismo sistema servidor. (No se muestra el tercer componente, la Consola, que es la interfaz a WebSphere Partner Gateway). De hecho, pueden existir varios de estos componentes y estar instalados en distintos servidores. Todos los componentes deben utilizar el mismo sistema de archivos común. Consulte la *Guía de instalación de WebSphere Partner Gateway* para obtener información acerca de las diferentes topologías que se pueden utilizar para configurar WebSphere Partner Gateway.

El componente Receptor recibe un documento en WebSphere Partner Gateway. El componente Receptor es responsable de la supervisión de documentos entrantes, recuperando los documentos que llegan, llevando a cabo ciertos procesos básicos en los mismos y, a continuación, colocándolos en una cola para que el Gestor de documentos pueda recuperarlos.

Las instancias de receptores son específicas del transporte. Se configurará un receptor para cada tipo de transporte que soporte el concentrador. Por ejemplo, si los socios van a enviar documentos a través de HTTP, debe establecer un receptor HTTP para que los reciba.

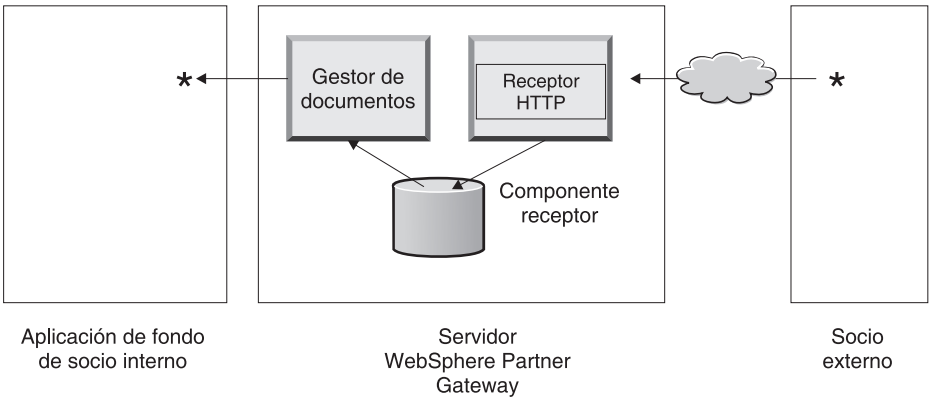


Figura 6. Un receptor HTTP

Si la aplicación de fondo del socio interno va a enviar documentos a través de JMS, debe configurar un receptor JMS en el concentrador para que los reciba.

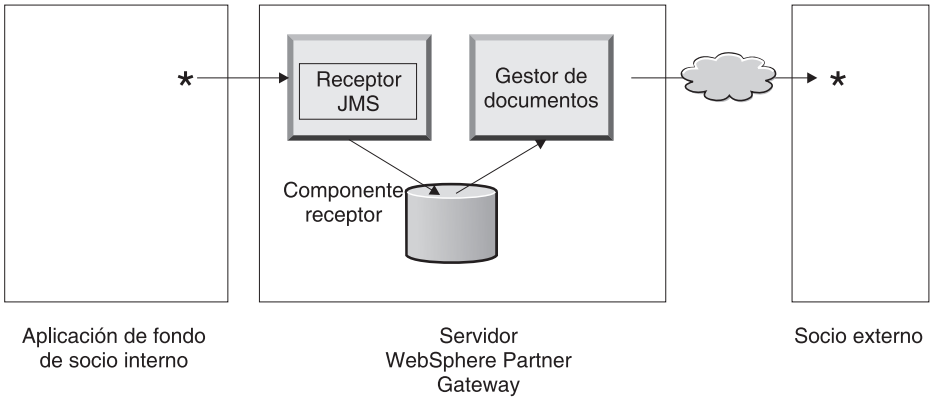


Figura 7. Un receptor JMS

Tal y como se describe en el apartado "Visión general de transportes" en la página 6, WebSphere Partner Gateway da soporte a diversos transportes, pero también puede subir su propio transporte definido por el usuario para definir un receptor (como se describe en el apartado " Configuración de un receptor para un transporte definido por el usuario" en la página 77).

El componente Receptor envía el documento a un sistema de archivos compartido. Para varios componentes que se encuentren en un único archivo (por ejemplo, documentos XML o ROD o intercambios EDI enviados conjuntamente), el receptor divide los documentos o intercambios antes de enviarlos al sistema de archivo compartido. El componente del Gestor de documentos recupera el documento del sistema de archivos y determina la información de direccionamiento y si es necesaria alguna transformación.

Por ejemplo, el socio interno puede enviar un documento EDI-X12 con el empaquetado Ninguno al concentrador para su entrega a un socio que está esperando el documento EDI-X12 con el empaquetado AS2. El socio proporciona el URL de HTTP donde debe entregarse el documento empaquetado con AS2 y el Gestor de documentos empaqueta el documento tal y como espera el socio. El Gestor de documentos utiliza la configuración del destino de dicho socio (que debe haber sido configurada con el URL de HTTP donde el socio espera recuperar documentos AS2) para enviar el documento al socio.

Configuración de componentes de proceso de documentos con manejadores

Este apartado describe con más detalle los componentes de WebSphere Partner Gateway y muestra los distintos puntos en los que puede (o debe) cambiar el comportamiento proporcionado con el producto de los componentes para procesar un documento de empresa.

Puede utilizar *manejadores* para cambiar el comportamiento proporcionado por el producto de receptores, destinos, pasos de flujo de trabajo fijos y acciones. Existen dos tipos de manejadores: los proporcionados por WebSphere Partner Gateway y los definidos por el usuario. Consulte la publicación *WebSphere Partner Gateway Programmer Guide* si desea obtener información sobre cómo crear manejadores.

Después de crear un manejador, debe subirlo para que esté disponible. Sólo se suben los manejadores definidos por el usuario. Los manejadores proporcionados por WebSphere Partner Gateway ya están disponibles.

Los apartados siguientes describen los puntos de proceso en los que pueden especificarse manejadores.

Destinatarios

Los receptores tienen tres *puntos de configuración* que es posible especificar: preproceso, comprobación síncrona y postproceso.

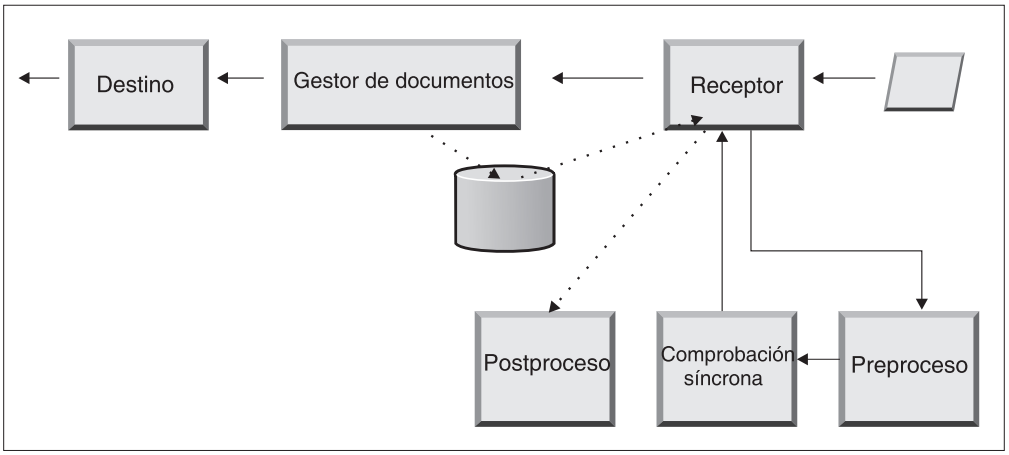


Figura 8. Puntos de configuración de receptor

El proceso se produce en el siguiente orden:

1. El componente Receptor llama a los pasos de preproceso y de comprobación síncrona después de recibir el documento.
2. Luego llama al Gestor de documentos para que procese el documento.
3. En el caso de flujos síncronos, el Gestor de documentos proporciona una respuesta síncrona. El componente Receptor llama a continuación al paso de preproceso con la respuesta devuelta en el Gestor de documentos.

Los pasos se describen en los siguientes apartados:

- Preproceso

  El paso de preproceso normalmente se utiliza para cualquier proceso del documento que sea necesario realizar antes de enviarlo al Gestor de documentos. Por ejemplo, si va a recibir varios documentos ROD en un sólo archivo, configure el manejador del divisor ROD cuando defina el receptor. El divisor ROD, junto con los otros dos divisores proporcionados con el producto, está disponible cuando configure un receptor. Si crea manejadores adicionales para el paso de preproceso, dichos manejadores también estarán disponibles.

  Consulte el apartado " Preproceso" en la página 78 para obtener más información sobre cómo configurar el punto de configuración de preproceso.

- comprobación síncrona

  La comprobación síncrona se utiliza para determinar si WebSphere Partner Gateway debe procesar el documento de manera síncrona o asíncrona. Por ejemplo, en el caso de los documentos AS2 recibidos a través de HTTP, determina si una MDN (Message Disposition Notification) debe devolverse de forma síncrona a través de la misma conexión HTTP. WebSphere Partner

Gateway proporciona diversos manejadores para la comprobación síncrona. La lista de manejadores varia dependiendo del transporte asociado con el receptor.

La comprobación síncrona sólo es válida para los transportes (como HTTP, HTTPS y JMS) que dan soporte a la transmisión síncrona.

Nota: para aquellos documentos AS2, cXML, RNIF o SOAP que serán utilizados en intercambios síncronos, deberá especificar el manejador de comprobación síncrona en el receptor HTTP o HTTPS.

Consulte el apartado " Comprobación síncrona" en la página 81 para obtener información sobre cómo configurar el punto de configuración de comprobación síncrona.

- Postproceso

  El postproceso se utiliza para procesar el documento de respuesta que el concentrador envía como resultado de una transacción síncrona.

  Consulte el apartado " Postproceso" en la página 82 para obtener información sobre cómo configurar el punto de configuración de postproceso.

gestor de documentos

Los documentos recibidos por receptores son recopilados por el Gestor de documentos desde el sistema de archivos para seguir siendo procesados. El Gestor de documentos utiliza conexiones de socio para direccionar los documentos. Todos los documentos que fluyen a través del Gestor de documentos pasan a través de una serie de flujos de trabajos: flujo de trabajo entrante fijo, flujo de trabajo variable y flujo de trabajo saliente fijo. Al final del flujo de trabajo entrante, se determinará la conexión de socio. La conexión de socio especifica la acción a realizar en este documento. Después de ejecutar el flujo de trabajo variable, el Gestor de documentos procesa el flujo de trabajo saliente en este documento.

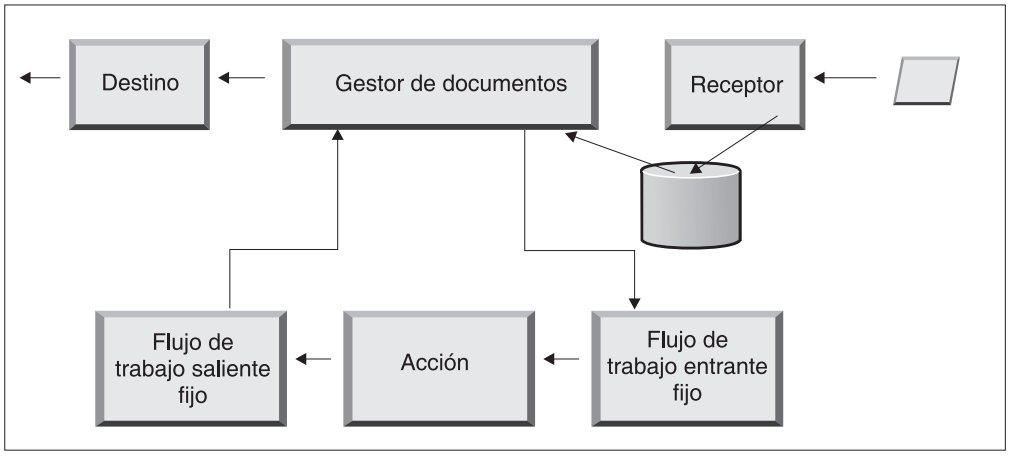


Figura 9. Flujos de trabajo y acciones fijos

En la Figura 9 se muestra la ruta que seguiría un documento como un PIP de RosettaNet o un servicio web. No obstante, algunos documentos necesitarán varios flujos configurados. Por ejemplo, un intercambio EDI puede constar de varias transacciones. El primer flujo utiliza una acción para desensobrar el conjunto de transacciones individuales. Todas estas transacciones se vuelven a introducir y procesar en su propio flujo configurado.

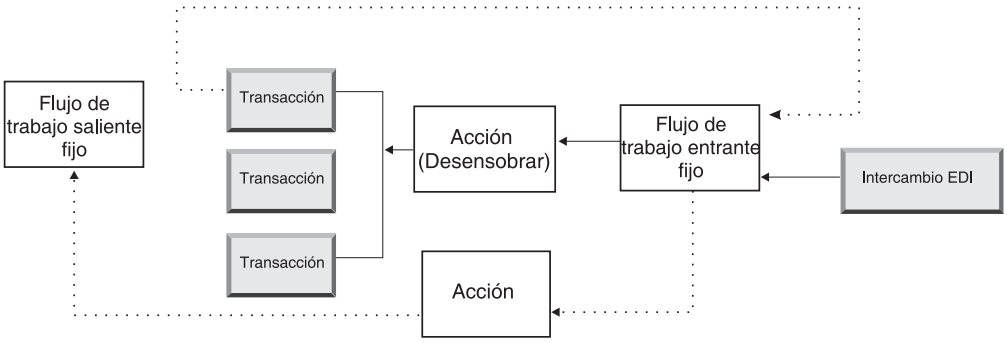


Figura 10. Flujos de trabajo y acciones fijos para un intercambio EDI

Flujo de trabajo fijo entrante

El flujo de trabajo fijo entrante consta del conjunto estándar de los pasos del proceso que se han realizado en todos los documentos que llegan al Gestor de documentos procedentes de un receptor. El flujo de trabajo es fijo porque el número y los tipos de pasos son siempre los mismos. No obstante, puede proporcionar, a través de las salidas de usuario, manejadores personalizados para procesar los siguientes pasos: desempaquetado de protocolo y proceso de protocolo. El último paso que un flujo de trabajo fijo de entrada realiza es la búsqueda de una conexión de socio, que determina el flujo de trabajo variable que se ejecuta para este documento de empresa.

Por ejemplo, si se recibe un mensaje AS2, el mensaje se descifra y se recuperan los ID de empresa del remitente y el receptor. Los pasos del flujo de trabajo fijo entrante convierten el documento AS2 en texto sin formato para que más adelante lo procese WebSphere Partner Gateway y extraiga información que determine la acción correspondiente al mensaje.

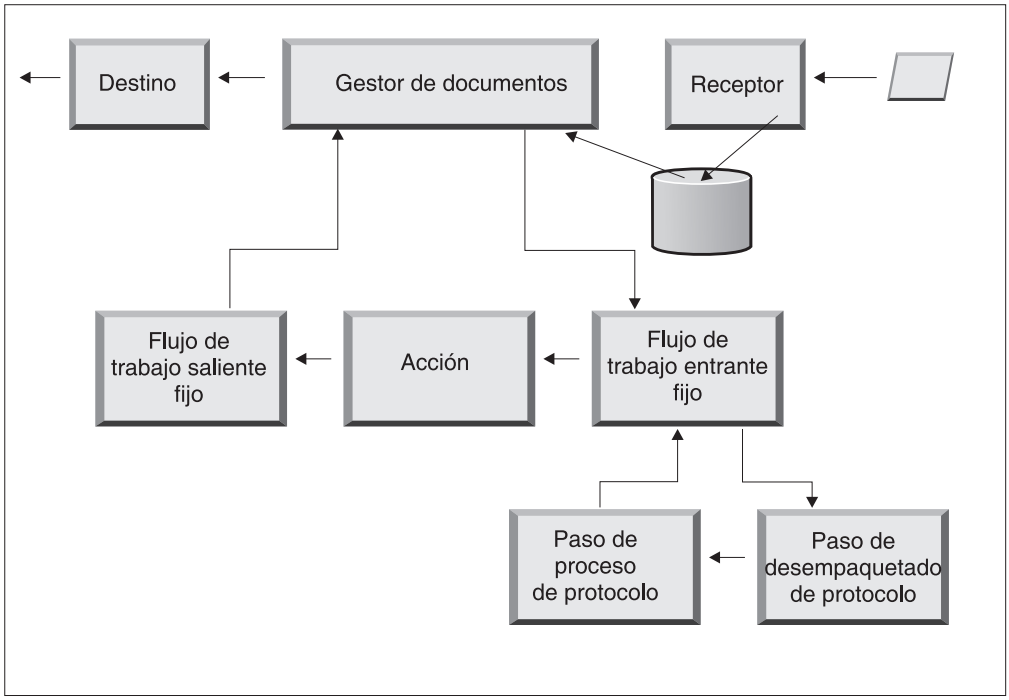


Figura 11. Pasos del flujo de trabajo fijo entrante

Desempaquetado de protocolo: Durante el desempaquetado de protocolo, se desempaqueta un documento para que pueda realizarse un proceso adicional. Este proceso puede incluir el descifrado, la descompresión, la verificación de firmas, la extracción de información de direccionamiento, la autenticación de usuario o la extracción de partes del documento de empresa.

WebSphere Partner Gateway proporciona manejadores para los paquetes RNIF, AS, de integración de programas de fondo y ninguno. Si son necesarios manejadores para otros protocolos de paquetes, pueden desarrollarse como salidas de usuario. Consulte la publicación *WebSphere Partner Gateway Programmer Guide* para obtener información acerca de la grabación de salidas de usuario.

No es posible modificar el paso de desempaquetado de protocolo; no obstante, sí se puede añadir lógica empresarial al paso añadiendo manejadores.

Consulte el apartado “Configuración de flujos de trabajo fijos” en la página 86 para obtener información sobre cómo configurar este paso.

Paso de proceso de protocolo: Proceso de protocolo implica determinar información específica del protocolo, que puede incluir analizar el mensaje para determinar la información de direccionamiento (como el ID de remitente y el ID de receptor), información de protocolo e información de tipo de documento. WebSphere Partner Gateway proporciona el proceso para una variedad de protocolos, tal y como se listan en el apartado “ Manejadores de proceso de protocolos” en la página 87. El proceso para otros protocolos, por ejemplo, CSV (valores separados por comas), pueden proporcionarse con una salida de usuario.

No es posible modificar el paso de proceso de protocolo; no obstante, sí puede añadir lógica empresarial al paso añadiendo manejadores.

Consulte el apartado “Configuración de flujos de trabajo fijos” en la página 86 para obtener información sobre cómo configurar este paso.

Puede utilizar el manejador predeterminado que se aplica al protocolo para el documento, o bien puede especificar un manejador distinto para los pasos de flujo de trabajo fijo de desempaquetado de protocolo y proceso de protocolo.

Acciones

El paso siguiente en la secuencia de proceso se produce de acuerdo con las acciones que se hayan configurado para el intercambio del documento. Las acciones constan de un número variable de pasos que pueden realizarse en el documento. Ejemplos de acciones son la validación de un documento (de forma que se ajuste a un determinado conjunto de normas) y la transformación del documento al formato que necesita el destinatario.

Si el documento no tiene pasos específicos necesarios, puede utilizar la acción Paso a través proporcionada con el producto, que no efectúa cambio alguno en el documento.

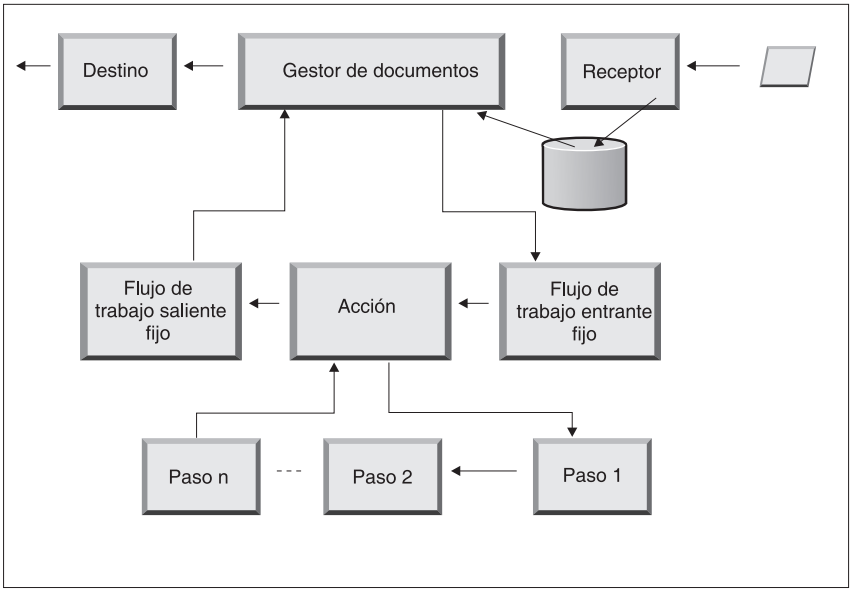


Figura 12. Pasos de acción

No es posible modificar una acción proporcionada con un producto. Puede, no obstante, crear una acción (y añadir manejadores a la lista configurada) o copiar una acción proporcionada con el producto y, a continuación, modificar la lista de manejadores.

Consulte el apartado “Configuración de acciones” en la página 88 para obtener más información acerca de la creación o copia de una acción proporcionada con el producto o sobre cómo configurar una acción definida por el usuario.

Conceptos relacionados

“Configuración de acciones” en la página 88

Flujo de trabajo fijo saliente

El flujo de trabajo fijo saliente consta de un paso: el empaquetado del documento con su información de protocolo. Por ejemplo, si un documento ha sido configurado para ser recibido por una aplicación de fondo utilizando el

empaquetado de integración de programas de fondo, se añadirá determinada información de cabecera al documento antes de ser pasado al destino.

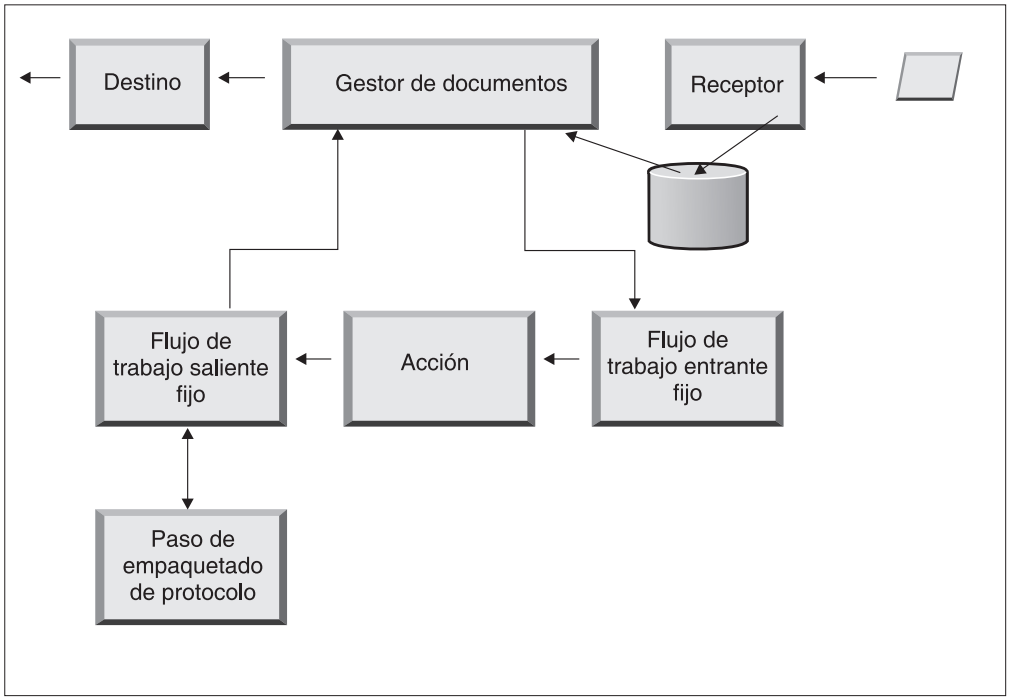


Figura 13. Pasos del flujo de trabajo fijo saliente

WebSphere Partner Gateway proporciona manejadores para diversos paquetes y protocolos, que se listan en el apartado "Flujo de trabajo saliente" en la página 87. Si son necesarios otros manejadores de paquetes, éstos pueden desarrollarse como pasos de salida de usuario. Generalmente estos pasos se ocupan de uno o más de los siguientes procesos:

- Montaje o ensobrado
- Cifrado
- Firma
- Compresión
- Configuración de cabeceras de transporte específicas de protocolos empresariales

No es posible modificar el paso de empaquetado de protocolo; no obstante, sí puede añadir lógica empresarial al paso añadiendo manejadores.

Consulte el apartado "Configuración de flujos de trabajo fijos" en la página 86 para obtener información sobre cómo configurar este paso del flujo de trabajo.

Destinos

Los destinos se configuran en la consola para cada socio al que necesite enviar mensajes. La configuración de un destino incluye el transporte que será utilizado para enviar mensajes y la configuración necesaria para enviarlo como el URL del proceso de recepción del socio.

Una vez el documento abandona el Gestor de documentos, se envía utilizando un destino a su destinatario. El destino tiene dos puntos de configuración: preproceso

y postproceso.

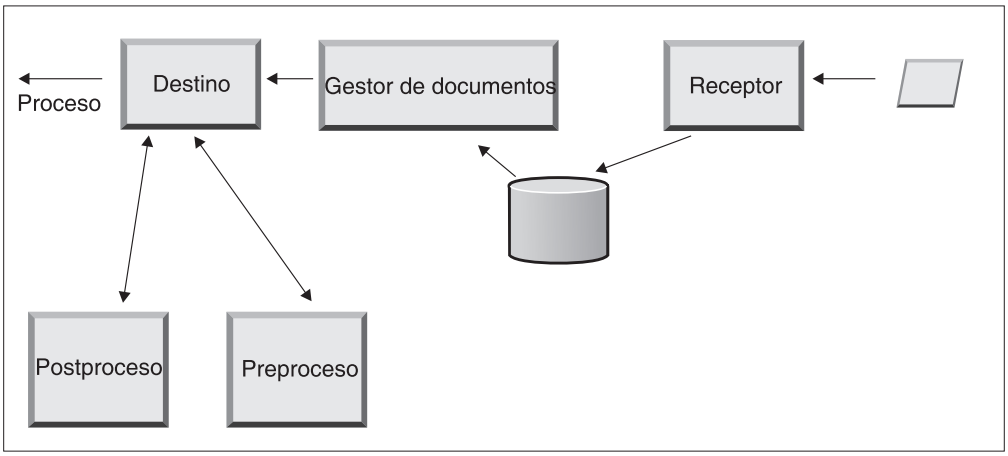


Figura 14. Puntos de configuración de destino

- Preproceso

  El preproceso afecta al proceso de un documento antes de enviarlo al destinatario. El proceso es el envío en sí del documento. El sistema no proporciona ningún manejador para configurar el paso de preproceso, aunque puede subir un manejador definido por el usuario.
- Postproceso

  El postproceso actúa sobre los resultados de la transmisión del documento (por ejemplo, sobre la respuesta que recibe del destinatario durante una transmisión síncrona). El sistema no proporciona ningún manejador para configurar el paso de postproceso, aunque puede subir un manejador definido por el usuario.

Consulte el apartado "Configuración de manejadores" en la página 243 para obtener información sobre cómo configurar los pasos de preproceso y postproceso.

Visión general de la configuración del concentrador

Después de haber analizado las necesidades de la empresa, tal como se describe en el apartado "Información necesaria para configurar el concentrador" en la página 6, debe crear el concentrador y crear los perfiles de los socios. En este apartado se proporciona una visión general de alto nivel de las tareas implicadas.

Nota: Durante la configuración del concentrador, consulte la publicación *Guía del administrador de WebSphere Partner Gateway* para obtener información acerca de los códigos de suceso, así como consejos para la resolución de problemas.

Configuración del concentrador

Acerca de esta tarea

Como el administrador de concentrador, para configurar el concentrador debe realizar las tareas siguientes:

1. Realice cualquier configuración preliminar (si es necesaria) para los transportes que está utilizando. La configuración preliminar se describe en el apartado Capítulo 4, "Preparación para la configuración del concentrador", en la página 35.

2. Si lo desea, personalice la consola y cambie la contraseña predeterminada y la política de permisos. Estas tareas se describen en el apartado Capítulo 6, “Configuración de la Consola de comunidad”, en la página 53.
3. Cree receptores para los tipos de transporte que se utilizarán para recibir documentos en el concentrador (desde el socio interno y los socios externos). La creación de receptores se describe en el apartado Capítulo 7, “Definición de receptores”, en la página 59.

   Nota: si va a configurar el receptor con manejadores definidos por el usuario, deberá actualizar los manejadores antes de crear el receptor. La subida de manejadores se describe en el apartado “ Subida de manejadores definidos por el usuario” en la página 60.
4. Configure todas las acciones o todos los pasos de flujo de trabajo entrante. Este paso es *opcional* y sólo lo necesitan los que tienen requisitos específicos para el proceso de documentos que no proporciona WebSphere Partner Gateway. Si no necesita modificar el comportamiento de los flujos de trabajo o acciones que proporciona el producto, puede ignorar este paso. La configuración de pasos de flujo de trabajo y acciones se describe en el apartado Capítulo 8, “Configuración de pasos de flujos de trabajo fijos y acciones”, en la página 85.

   Nota: debe subir los manejadores definidos por el usuario antes de configurar los flujos de trabajo o las acciones. La subida de manejadores proporcionados por el usuario se describe en el apartado “ Subida de manejadores” en la página 85.
5. Cree definiciones de documento (o verifique que las que ha creado ya están disponibles) para definir los tipos de documentos que puede enviar o recibir en el concentrador.
6. Cree interacciones para indicar la combinación válida de dos definiciones de documento.

   La creación de definiciones de documento y la creación de interacciones se describen en los apartados Capítulo 9, “Configuración de tipos de documento”, en la página 107 y Capítulo 10, “Configuración de flujos de documentos EDI”, en la página 173.
7. Cree un perfil para el socio interno, proporcionando información acerca del socio interno y estableciendo tipos de documentos que el socio interno puede enviar y recibir (las funciones B2B del socio interno). La creación del perfil se describe en el apartado Capítulo 3, “Creación y configuración de socios”, en la página 25.

Creación de socios

Cuando haya configurado el concentrador, cree un perfil para cada socio externo que intercambiará documentos con el socio interno. Sólo el administrador de concentrador puede crear socios.

Como administrador de concentrador, también puede configurar las funciones B2B de los socios, establecer sus destinos y configurar sus perfiles de seguridad. Estos pasos pueden ser realizados, como alternativa, por los mismos socios.

La creación de socio se describe en el apartado Capítulo 3, “Creación y configuración de socios”, en la página 25. La creación de destinos se describe en el apartado Capítulo 11, “Creación de destinos”, en la página 223. La configuración de perfiles de seguridad se describe en el apartado Capítulo 13, “Habilitación de la seguridad para intercambios de documentos”, en la página 251.

Establecimiento de conexiones de documentos

Después de configurar el concentrador y crear los perfiles de socio, ya puede empezar a configurar conexiones. Las conexiones indican las combinaciones válidas de emisores y receptores, así como los documentos que pueden intercambiar. La gestión de conexiones se describe en el apartado Capítulo 12, “Gestión de conexiones”, en la página 247.

Visión general de los certificados OpenPGP

En WebSphere Partner Gateway se da soporte a OpenPGP. Utiliza una combinación de clave pública fuerte y criptografía simétrica para proporcionar los servicios de seguridad. Las distintas funciones de OpenPGP, que se incluyen en este release, son las siguientes:

- Mensajes empaquetados según RFC 4880.

  Nota: No se da soporte a RFC 2440 ni RFC 3156 en este release.
- Cifrado, Cifrado con detección de modificaciones y Compresión.

  Nota: En este release, WebSphere Partner Gateway no da soporte al inicio de sesión utilizando OpenPGP.
- Los algoritmos cifrados soportados son CAST5 (clave de 128 bit), TripleDES (clave de 168), Blowfish (clave de 128 bit), Twofish (clave de 256 bit), AES (clave de 128, 192 & 256 bit).

  Nota: Twofish, TripleDES y AES (clave de 192 & 256 bit) necesitan archivos de política de jurisdicción criptográfica sin restricción.
- Los algoritmos de compresión soportados son ZIP, ZLIB y BZip2.
- Mensajes blindados ASCII.
- Se modifica la migración del socio y la característica de conformidad FIPS para dar soporte a OpenPGP.
- El tratamiento parcial de los documentos no está soportado en OpenPGP.

Hay requisitos previos que tienen que llevarse a cabo antes de trabajar con los certificados OpenPGP.

Obtenga externamente los siguientes archivos de biblioteca y cópielos en la ubicación de la carpeta HUB INSTALLED LOCATION>/lib/openpgp:

- Biblioteca BouncyCastle OpenPGP versión 1.45 para JDK 1.5
- Biblioteca BouncyCastle JCE versión 1.45 para JDK 1.5

  Importante: Obtenga o proceda con estos archivos de biblioteca externamente, ya que IBM no los proporciona. Para obtener más información sobre la obtención de archivos de biblioteca, consulte el enlace de la página inicial de Bouncy castle - http://www.bouncycastle.org. Los archivos jar a extraer son http://www.bouncycastle.org/download/bcpg-jdk15-145.jar y http://www.bouncycastle.org/download/bcprov-jdk15-145.jar. En el caso de modalidad distribuida, coloque los archivos jar en todos los sistemas donde están instalados el Gestor de documentos y la Consola.

Después de copiar los archivos a la ubicación especificada, reinicie el servidor.

Capítulo 3. Creación y configuración de socios

Existen dos tipos de socios: socios internos y socios externos. El socio interno es generalmente la empresa que tiene en propiedad el servidor de WebSphere Partner Gateway y que utiliza el servidor para comunicarse con otras empresas. El socio interno posee las aplicaciones de fondo (aplicaciones internas de la empresa propietaria). Puede haber cualquier número de socios internos, pero el socio predeterminado es el primer socio definido. Las otras empresas con las que se comunica el socio interno son los socios externos.

Para cada socio con el que esté intercambiando documentos, necesitará crear un perfil de socio. Además de crear perfiles, también necesitará configurarlos, un proceso que implica diversos pasos necesarios y opcionales.

Este capítulo muestra los pasos básicos para crear y configurar un perfil de socio. Para obtener información más detallada sobre un paso, consulte la referencia en la parte final de dicho paso o apartado para obtener más información. Este capítulo incluye los siguientes apartados:

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado la sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Creación de perfiles de socio

Acerca de esta tarea

Este es el primer paso para definir un socio en WebSphere Partner Gateway. Este paso define información básica acerca del socio tal como su nombre, nombre de inicio de sesión e ID de empresa.

Para crear un socio, necesita conocer la siguiente información acerca del mismo:

- Se recomienda ID de empresa que el socio utiliza. Puede ser:
  - DUNS, que es el número Dun & Bradstreet estándar asociado con una empresa
  - DUNS+4, que es la versión ampliada del número DUNS
  - Formato libre, que puede ser cualquier número que el socio elija para identificar a la empresa

Siga este procedimiento con cada socio que desee añadir a la comunidad del concentrador:

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Crear**.
3. Especifique el **Nombre de inicio de sesión de empresa**. Se trata del nombre que utilizará el socio en el campo de empresa mientras inicia una sesión en el concentrador. No se permiten espacios en blanco en el nombre de inicio de sesión de empresa.
4. En **Nombre de visualización de socio**, especifique el nombre de la empresa u otro nombre descriptivo del socio. Este es el nombre que aparece en la lista **Búsqueda de socio**.
5. Seleccione el tipo de socio. Si este es el primer socio, es probable que esté configurando la empresa que tiene WebSphere Partner Gateway en propiedad. Por lo tanto, seleccionaría **Socio interno**. En la pantalla de configuración de socio, marque el recuadro de selección **Socio interno predeterminado** si desea establecer este socio interno actual como predeterminado. Cuando marque este recuadro de selección para cualquier otro socio, la selección predeterminada se elimina automáticamente de este socio interno. No puede borrar la selección en esta página. Para el primer socio interno que se crea, este recuadro de selección está marcado de forma predeterminada.
6. Si lo desea, especifique el nombre de usuario de administrador del Administrador. El nombre de usuario de administración debe ser único entre todos los socios. El administrador del socio puede realizar actividades de gestión para este socio, como la gestión de destinos, funciones B2B y usuarios. El Operador de concentrador siempre tiene acceso completo a la gestión de socios.
7. Seleccione el estado del socio. Seleccione **Habilitado** si el estado del socio es Inhabilitado. **Habilitado** es el estado predeterminado del socio.
8. Si lo desea, especifique el tipo de empresa en el campo **Tipo de proveedor**.
9. Si lo desea, especifique el **Sitio web** del socio.
10. Pulse **ID de empresa** > **Nuevo**.
11. Especifique un tipo de la lista e indique el identificador adecuado. WebSphere Partner Gateway utiliza el número que especifique aquí para direccionar el documento de y al socio.

    Siga las directrices siguientes cuando escriba el identificador:

    a. Los números DUNS deben tener nueve dígitos.
    b. Los números DUNS+4 deben tener 13 dígitos.
    c. Los números de ID con formato libre aceptan hasta 60 caracteres alfanuméricos y especiales.

    Nota: puede asignar más de un ID de empresa a un socio. En ocasiones, se requiere más de un ID de empresa. Por ejemplo, cuando el concentrador envía y recibe documentos EDI X12 o EDIFACT, utiliza los identificadores de DUNS y Formato libre durante el intercambio de documentos.

    Tanto el socio interno como los socios externos implicados en estos tipos de flujos de documentos deben tener un ID de DUNS y un ID de formato libre. El ID de formato libre se utiliza para representar los ID de EDI que tienen un identificador y un calificador. Por ejemplo, suponga que el calificador de EDI es "ZZ" y el identificador de EDI es "810810810". EL ID de formato libre podría especificarse como ZZ-810810810.

Al pulsar **Nuevo**, el cuadro de texto del ID de correo electrónico también se habilita y se muestra para que cree un ID de correo electrónico.

12. Pulse **Nuevo** para crear un nuevo ID de correo electrónico y escriba su ID de correo electrónico en Identificador de correo electrónico. Del mismo modo, puede pulsar Nuevo para crear varios ID de correo electrónico.
13. Si lo desea, especifique una dirección IP para el socio. La dirección IP se utiliza junto con un destino cuando se configura el valor de "Validar IP de cliente". Especifique una dirección IP llevando a cabo los siguientes pasos:
    a. Bajo **Dirección IP**, pulse **Nuevo**.
    b. Especifique la modalidad de funcionamiento.
    c. Especifique la dirección IP del socio.
14. Pulse **Guardar**.
15. Si ha especificado un nombre de usuario de administración se le mostrará una contraseña que el socio utilizará para iniciar sesión en el concentrador. Escriba la contraseña. La suministrará al usuario del socio Administrador.

Creación de destinos

Acerca de esta tarea

Después de crear un perfil para un socio, necesitará establecer los destinos que el socio utilizará para enviar documentos al socio.

Utilice el siguiente procedimiento para crear destinos para un socio:

1. Asegúrese de que el perfil de socio para el que desea crear destinos está seleccionado.

   Si acaba de crear un perfil, ya estará seleccionado. Si no está seleccionado, siga estos pasos:
   a. Pulse **Administración de cuentas** > **Perfiles** > **Socio**.
   b. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
   c. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
2. Pulse **Destinos**.
3. Pulse **Crear**.
4. Escriba un **Nombre de destino** para identificar el destino.
5. Si lo desea, indique el **Estado** del destino.
6. Si lo desea, indique si el destino está **En línea** o **Fuera de línea**.
7. Si lo desea, especifique una **Descripción** para el destino.
8. Seleccione un **Transporte**.
9. Después de seleccionar un transporte, el apartado **Configuración de destino** de esta página mostrará información específica de dicho transporte. Para obtener información acerca de cómo rellenar este apartado para cada transporte, consulte uno de los siguientes tres apartados:
   - "Configuración de los valores de transporte global" en la página 224

     Nota: estos valores sólo corresponden al destino de FTP Scripting.
   - "Configuración de un destino HTTP" en la página 226
   - "Configuración de un destino HTTPS" en la página 228
   - "Configuración de un destino FTP" en la página 229

Establecimiento de posibilidades B2B

Acerca de esta tarea

Cada socio tiene funciones B2B que definen los tipos de documentos que el socio puede enviar y recibir.

Como administrador del concentrador, puede configurar las funciones B2B de los socios o los socios pueden realizar esta tarea por sí mismos. Utilice la característica de funciones B2B para asociar las funciones B2B de un socio con una definición de documento.

Utilice el siguiente procedimiento para configurar las funciones B2B de cada socio:

1. Asegúrese de que el perfil del socio para el que desea configurar las funciones B2B está seleccionado. El perfil seleccionado aparece en la parte superior de la página después del **Perfil** .

   Si acaba de crear un perfil, ya estará seleccionado. Si no está seleccionado, siga estos pasos para hacerlo:

   a. Pulse **Administración de cuentas**.
   b. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
   c. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
2. Pulse **Posibilidades B2B**. Aparece la página de funciones B2B. La parte derecha de la página muestra los paquetes, protocolos y documentos soportados por el sistema como definiciones de documento.
3. Pulse el icono **El rol no está activo** bajo la columna **Establecer origen** para los paquetes. El paquete tiene documentos que los socios externos envían al socio interno.
4. Seleccione **Establecer origen** y **Establecer destino** si los socios enviarán y recibirán estos mismos documentos. La Consola muestra una marca de selección si la definición del documento está habilitada.

   Nota: la selección de Establecer origen será la misma para todas las acciones en PIP bidireccional independientemente de que la solicitud se origine en un socio y la correspondiente confirmación en otro. Esto también se aplica a Establecer destino.
5. Pulse el icono **Expandir** en el nivel de **Paquete** para ampliar un nodo individual en el nivel de definición de documento correspondiente o seleccione un número de **0-4** o **Todos** para expandir todas las definiciones de documento mostradas al nivel seleccionado.
6. De nuevo, seleccione **Establecer origen**, **Establecer destino** o ambos roles para los niveles inferiores de **Protocolo** y **Tipo de documento** para cada definición de documento que esté soportada en el sistema.

Si una definición está activada en el nivel de **Tipo de documento**, las definiciones de **Acción** y **Actividad** (si existe alguna) se activarán automáticamente.

7. Si lo desea, pulse **Habilitado** bajo la columna **Habilitado** para colocar una definición de documento fuera de línea. (Cuando se selecciona **Establecer origen** o **Establecer destino**, el registro se habilita automáticamente). Pulse **Inhabilitado** para ponerla en línea.

   Si un paquete no está habilitado, todas las definiciones de documento de nivel inferior en ese mismo nodo estarán también inhabilitadas, independientemente de si su estado individual estaba habilitado. Si una definición de documento de nivel inferior está inhabilitada, todas las definiciones de nivel superior dentro del mismo contexto permanecerán habilitadas. Cuando una definición de documento está inhabilitada, todas las conexiones y atributos dejan de funcionar.

8. Si lo desea, pulse el icono **Editar** si desea editar cualquiera de los atributos de un protocolo, paquete, tipo de documento, acción, actividad o señal. Entonces verá los valores de los atributos (si existe algún atributo). Puede modificar los atributos especificando un valor o seleccionando un valor en la columna **Actualizar** y, a continuación, pulsando **Guardar**.

Carga de certificados

Acerca de esta tarea

Los certificados permiten que los socios envíen y reciban documentos seguros utilizando varios métodos: cifrado, firma digital o SSL. Una vez un socio ha recibido un certificado de otro socio, el socio puede utilizar cualquiera de dichos métodos para enviar el documento.

Siga los pasos que se proporcionan en “Cómo subir certificados con el asistente” en la página 284 para cargar certificados para un socio.

Para obtener más información sobre la utilización de certificados, consulte el apartado Capítulo 13, “Habilitación de la seguridad para intercambios de documentos”, en la página 251.

Creación de usuarios

Acerca de esta tarea

Los usuarios son las personas que iniciarán sesión para realizar tareas de administración para este socio. Los nuevos usuarios que se añaden al servidor LDAP y a la Consola administrativa de WAS también se deben añadir a la consola de WebSphere Partner Gateway para que estén activos.

Utilice el siguiente procedimiento para crear usuarios para un socio:

1. Asegúrese de que el perfil del socio para el cual desea crear usuarios está seleccionado. El perfil seleccionado aparece en la parte superior de la página después de **Perfil >**. Si el perfil no está seleccionado, siga estos pasos para crear un perfil:
   a. Pulse **Administración de cuentas > Perfiles>**.
   b. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.

c. Pulse el icono **Ver detalles** para mostrar el perfil del socio.

2. Pulse **Usuarios**.
3. Pulse **Crear**.
4. Escriba el nombre del usuario.

   Nota: Los nombres de usuario deben ser exclusivos entre todos los socios del sistema.
5. Asegúrese de que el estado es **Habilitado**.
6. Si lo desea, escriba el nombre proporcionado, apellido y cualquier otra información personal del usuario.
7. Seleccione **Idioma** y **Entorno local de formato** y **Zona horaria** del usuario.
8. Cambie el estado de alerta del estado del usuario a **Habilitado**.
9. Seleccione la visibilidad suscrita del usuario.
10. Pulse **Generar la contraseña automáticamente** para crear una contraseña para dicho usuario o escriba y vuelva a escribir una.
11. Pulse **Guardar**.

Nota:

1. debido a que es necesario contar con nombres de usuario exclusivos en un servidor LDAP, los nombres de usuario deben ser exclusivos también en WebSphere Partner Gateway. Si está creando un nuevo usuario y el nombre de usuario ya existe en el mismo socio o en otro, verá un mensaje de error que informa de que `Ya existe un usuario con este nombre`.
2. Si está migrando a WebSphere Partner Gateway desde una versión anterior en la que los nombres de usuarios no están restringidos, aparecerán dos asteriscos (**) junto a cualquier nombre de usuario duplicado mostrando que también existe en el mismo o en otro socio. Cambie uno de los nombres de usuario para que sean exclusivos entre sí. Los nuevos usuarios y grupos, que se añaden al servidor LDAP y a la consola administrativa de WAS, también se deben añadir a la consola de WebSphere Partner Gateway para que sean activos.

Para permitir que LDAP funcione con WebSphere Partner Gateway, necesitará configurar la autenticación del servidor LDAP utilizando la consola de WebSphere Application Server y la autorización de usuarios LDAP utilizando la Consola de comunidad de WebSphere Partner Gateway. Para obtener más información acerca de cómo establecer una autenticación LDAP, consulte la publicación *Guía de instalación de WebSphere Partner Gateway*. Para obtener más información acerca de la gestión de usuarios y el establecimiento de la autorización de usuarios LDAP, consulte la publicación *Guía de administración de WebSphere Partner Gateway*.

Para obtener más información sobre la gestión de usuarios, consulte el apartado "Managing users" en la publicación *WebSphere Partner Gateway Partner Guide*.

Configuración de FTP

Para configurar un usuario de FTP o SFTP, realice una de las siguientes tareas:

- “Creación de usuarios de FTP y SFTP” en la página 31Cree un usuario en la pantalla Gestión de FTP de la consola.
- “Habilitación de usuarios existentes para FTP y SFTP” en la página 31

Creación de usuarios de FTP y SFTP

En este paso, durante la creación, los usuario se configuran como usuarios FTP o SFTP.

Acerca de esta tarea

Puede crear usuarios FTP y SFTP desde la página **Gestión de usuarios de FTP**de la consola.

Procedimiento

1. Pulse **Administración de cuentas > Gestión de usuarios de FTP**.
2. Pulse **Crear**.
3. Escriba los detalles del usuario y pulse **Guardar**. Para obtener más información sobre la creación de usuarios, consulte el apartado "Creación de usuarios" en la página 29.La información del usuario creado se muestra en modalidad de sólo lectura.
4. Pulse **Configuración FTP**.
5. En la pantalla Configuración FTP, seleccione `Habilitado` en **Usuario de FTP habilitado** o en **Usuario de SFTP habilitado**. Puede habilitar un usuario para los dos servidores FTP y SFTP.
6. Especifique los siguientes detalles de la configuración de FTP:
   a. Introduzca el **Directorio de inicio**, que es la vía de acceso relativa del valor especificado para bcg.ftp.config.rootdirectory.
   b. Habilite o inhabilite el **Permiso de escritura** del directorio de inicio.
   c. Habilite o inhabilite el permiso en **Crear/Eliminar directorio**.
   d. Seleccione **Nº máx. de inicios de sesión**. Es el número máximo de veces que puede realizar inicios de sesión concurrentes.
   e. Seleccione **Nº máx. de inicios de sesión desde la misma dirección IP**. Es el número máximo de veces que puede realizar inicios de sesión concurrentes desde la misma dirección IP.
   f. Seleccione **Tiempo de inactividad máximo (segundos)**. Es el tiempo máximo de inactividad en segundos para que se descarte la conexión del usuario.
   g. Seleccione **Descarga upload (bytes/sec)**. Es la velocidad de subida máxima en bytes/seg.
   h. Seleccione **Descarga Download (bytes/sec)**. Es la velocidad de descarga máxima en bytes/seg.

   Nota: Algunos campos tienen el valor `Límite personalizado` en la lista desplegable. Si selecciona `Límite personalizado` en la lista desplegable, introduzca el valor personalizado en el recuadro de texto.
7. Para la configuración de SFTP, especifique **Clave (sólo SFTP)**. El archivo subido se utilizará para la autenticación basada en claves. El icono de la carpeta indica que una Clave ya está subida. También puede utilizar **Examinar** para subir una clave.
8. Pulse **Guardar**.

Habilitación de usuarios existentes para FTP y SFTP

En este paso, puede establecer un usuario existente como usuario FTP o usuario SFTP.

Acerca de esta tarea

Para configurar un usuario de FTP o SFTP, habilite propiedades de FTP o SFTP para un usuario existente.

Procedimiento

1. Pulse **Administración de cuentas > Perfiles > Usuarios**.
2. Especifique los criterios de búsqueda y pulse **Buscar**.
3. En los resultados de búsqueda, si la columna **Estado** está inhabilitada para el contacto, pulse el icono de `Habilitado`. El icono cambia entre los estado habilitar e inhabilitar.
4. Pulse el icono de **Ver detalles** del usuario para configurar el acceso a FTP.
5. En la pantalla de detalles del usuario, pulse **Configuración FTP**.
6. En la pantalla **Configuración FTP**, seleccione `Habilitado` en **Usuario de FTP habilitado** o en **Usuario de SFTP habilitado**. Un usuario se puede habilitar para los dos servidores FTP y SFTP.
7. Especifique los detalles de la configuración de FTP o SFTP. Consulte "Creación de usuarios de FTP y SFTP" en la página 31 para obtener más información acerca del usuario de FTP y SFTP.
8. Pulse **Guardar**.

Creación de grupos

Acerca de esta tarea

Agrupar usuarios permite gestionar los permisos de más de un usuario al mismo tiempo. Los nuevos grupos que se añaden al servidor LDAP y a la Consola administrativa de WebSphere Application Server también se deben añadir a la consola de WebSphere Partner Gateway para que estén activos.

Utilice el siguiente procedimiento para crear grupos para cada socio:

1. Asegúrese de que el perfil de socio para el que desea crear grupos está seleccionado.

   Si acaba de crear un perfil, ya estará seleccionado. Si no está seleccionado, siga estos pasos para hacerlo:

   a. Pulse **Administración de cuentas** > **Perfiles** > **Socio**.
   b. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
   c. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
2. Pulse **Grupos**.
3. Pulse **Crear**.
4. Escriba el nombre de este grupo.
5. Pulse **Guardar**.
6. Para añadir usuarios a este grupo, pulse el enlace **Miembros**.

   Los usuarios que están asociados con este socio aparecen bajo **Usuarios no en el grupo** o **Usuarios en el grupo**. Para añadir un usuario a un grupo, lleve a cabo los siguientes pasos,

   a. Pulse el icono **Editar registro** junto al grupo.
   b. Seleccione el usuario que desea añadir y pulse **Añadir a grupo**.

c. Pulse **Guardar**.

7. Para cambiar los permisos de los usuarios en este grupo, pulse el enlace **Permisos**.

   Los permisos para los usuarios de este grupo aparecen por **Módulo**. Para cambiar los permisos de este grupo, complete los siguientes pasos,

   a. Pulse el icono **Editar registro** junto al grupo.
   b. Pulse los botones de selección en la parte derecha de cada módulo especificando el permiso como **Sin acceso**, **Sólo lectura** o **Lectura/Escritura**.
   c. Pulse **Guardar**.

   Nota: los usuarios pueden pertenecer a más de un grupo. En estos casos, cuando los permisos en los distintos grupos son diferentes, el usuario hereda el nivel más alto de permisos asignado a los usuarios en todos los grupos.

Nota: Todos los miembros del grupo hubadmin pueden tener permisos de superusuario. Esto permite que muchas personas compartan las responsabilidades de hubadmin al tiempo que se conserva la seguridad de contraseñas.

Para obtener más información sobre la gestión de grupos, consulte el apartado "Managing groups" en la publicación *WebSphere Partner Gateway Partner Guide*.

Creación de contactos

Acerca de esta tarea

WebSphere Partner Gateway permite crear contactos que pueden ser notificados cuando se producen distintos tipos de sucesos. Utilice el siguiente procedimiento para crear contactos para cada socio:

1. Asegúrese de que el perfil de socio para el que desea crear contactos está seleccionado. El perfil seleccionado aparece en la parte superior de la página después de **Perfil >**.

   Si no se ha seleccionado el perfil, siga estos pasos:

   a. Pulse **Administración de cuentas > Perfiles>**.
   b. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
   c. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
2. Pulse **Contactos**.
3. Pulse **Crear**.
4. Escriba el **Nombre** y **Apellido** de este contacto.
5. Si lo desea, escriba la **Dirección** de este contacto.
6. Si lo desea, seleccione el **Tipo de contacto**.
7. Si lo desea, escriba la dirección de **Correo electrónico**, número de **Teléfono** y **Número de fax** de este contacto.
8. Seleccione el **Idioma** y **Entorno local de formato** y **Zona horaria** del contacto.
9. Cambie el **Estado de alerta** del estado de usuario a **Habilitado**.
10. Seleccione la **Visibilidad suscrita** del usuario.
11. Pulse **Guardar**.

Para obtener más información sobre la gestión de contactos, consulte el apartado "Managing contacts" en la publicación *WebSphere Partner Gateway Partner Guide*.

Creación de direcciones

Acerca de esta tarea

WebSphere Partner Gateway permite crear direcciones para socios. Utilice el siguiente procedimiento para crear una dirección para un socio:

1. Asegúrese de que el perfil de socio para el que desea crear direcciones está seleccionado. El perfil seleccionado aparece en la parte superior de la página después de **Perfil >**.

   Si acaba de crear un perfil, ya estará seleccionado. Si no está seleccionado, siga estos pasos para hacerlo:

   a. Pulse **Administración de cuentas > Perfiles>**.
   b. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
   c. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
2. Pulse **Direcciones**.
3. Pulse **Crear nueva dirección**.
4. Seleccione un **Tipo de dirección**.
5. Si lo desea, escriba la **Dirección**.
6. Pulse **Guardar**.

Para obtener más información sobre la gestión de direcciones, consulte el apartado "Managing addresses" en la publicación *WebSphere Partner Gateway Partner Guide*.

Capítulo 4. Preparación para la configuración del concentrador

En los siguientes capítulos, configurará los receptores y destinos descritos en el apartado Capítulo 2, “Introducción a la configuración del concentrador”, en la página 5. Dependiendo de los tipos de transporte que se utilicen para enviar y recibir documentos, es necesario configurar receptores y destinos.

Este capítulo incluye los siguientes temas:

- “ Creación de un destino de directorio de archivos”
- “Configuración del servidor FTP para la recepción de documentos”
- “Configuración del concentrador para el protocolo de transporte JMS” en la página 39
- “Configuración de la compresión RNIF” en la página 45

También proporciona una breve visión general de los scripts FTP necesarios para los receptores y destinos de FTP Scripting y describe Data Interchange Services Client, que puede ser utilizado para crear correlaciones de transformación, validación y acuses de recibo funcionales para documentos EDI, XML y ROD (datos orientados a registros).

- “Utilización de scripts de FTP para receptores y destinos de FTP Scripting” en la página 45
- “Utilización de correlaciones desde Data Interchange Services Client” en la página 46

Si no está planeando establecer ninguno de estos tipos de receptores o destinos, sáltese este capítulo y vaya al apartado Capítulo 5, “Inicio del servidor y visualización de la Consola de comunidad”, en la página 49.

Creación de un destino de directorio de archivos

El directorio que especifique en el destino de directorio de archivos será creado por el usuario si es necesario. Si ya existe, lo utilizará el destino.

Configuración del servidor FTP para la recepción de documentos

Nota: este apartado se aplica únicamente a la recepción de documentos de socios a través de FTP o FTPS. El envío de documentos a socios se describe en los apartados “Configuración de un destino FTP” en la página 229 y “Configuración de un destino FTPS” en la página 236.

Si va a utilizar FTP o FTPS para el transporte de los documentos entrantes, debe disponer de un servidor FTP instalado. Si tiene intención de utilizar FTP y no dispone de un servidor instalado, instálelo antes de continuar. Asegúrese de que uno de los siguientes casos de ejemplo se corresponde con su instalación:

- El servidor FTP está instalado en la misma máquina en la que está instalado WebSphere Partner Gateway.
- El bcguser de la máquina WebSphere Partner Gateway tiene acceso de lectura/escritura a la ubicación en la que el servidor FTP guardará los archivos.

Nota: Si la configuración de instalación se encuentra en varias máquinas, se debe instalar un servidor FTP donde se instale el receptor.

Configuración de la estructura de directorios necesaria en el servidor FTP

Acerca de esta tarea

Una vez que haya instalado el servidor FTP, el paso siguiente es la creación de la estructura de directorios necesaria bajo el directorio inicial del servidor FTP. WebSphere Partner Gateway requiere una estructura de directorios en particular que el componente Receptor y los componentes del Gestor de documentos utilizan para identificar correctamente el socio que envía el documento entrante. La estructura se muestra en la Figura 15.

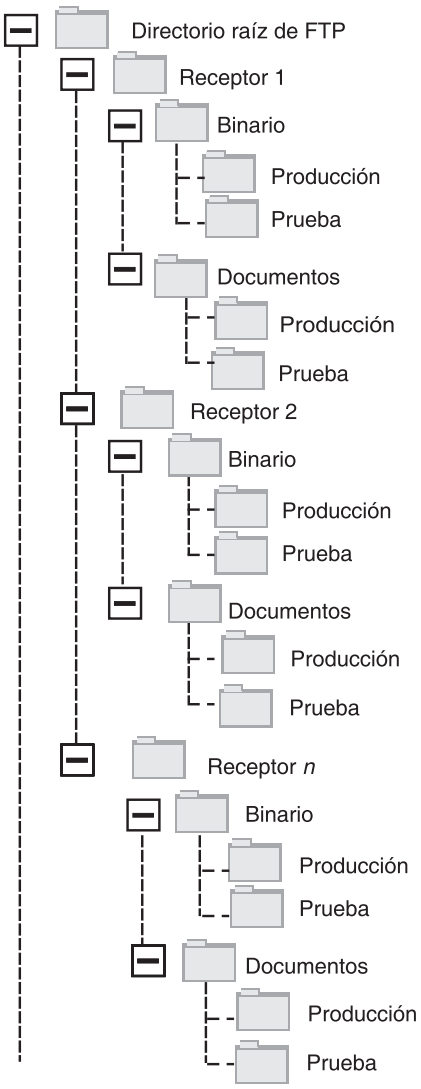


Figura 15. Estructura de directorio FTP

Cada directorio de socio contiene un directorio Binary y un directorio Documents. Tanto el directorio Binary como el Documents contienen un directorio Production y un directorio Test.

El directorio Documents se utiliza cuando un socio envía un documento XML que contiene información completa sobre el direccionamiento (utilizando FTP) al concentrador. Ello precisa de la creación de una definición de XML personalizada. Además, los documentos de intercambio electrónico de datos (EDI) pueden enviarse utilizando este directorio.

El directorio Binary se utiliza cuando un socio envía cualquier otro documento (utilizando FTP) al concentrador.

Para cada socio que utilice FTP para enviar o recibir documentos, cree las siguientes carpetas en el directorio raíz del servidor FTP:

1. Cree una carpeta para el socio.

   Nota: el nombre de la carpeta debe coincidir con el nombre especificado para **Nombre de inicio de sesión de empresa** cuando cree el socio. La creación de socios se describe en el apartado "Creación de perfiles de socio" en la página 25.
2. Cree subcarpetas bajo la carpeta del socio llamadas `Binary` y `Documents`.
3. Cree subcarpetas bajo las carpetas Binary y Documents llamadas `Production` y `Test`.

Proceso de archivos que se envían a través de FTP

Es importante comprender cómo procesa el servidor FTP los archivos binarios y XML.

Archivos binarios

Los archivos binarios tienen una estructura de nombre de archivo obligatoria, ya que el gestor de archivos no gestiona los archivos en absoluto.

La estructura de nombre de archivos es: *<ID_A_socio>.<Nombre_archivo_exclusivo>*

Cuando el componente Receptor detecta un archivo binario, lo graba en el almacenamiento compartido y lo pasa al gestor de documentos para su procesamiento.

El nombre del directorio en el que el archivo ha sido detectado se utiliza para evaluar el nombre de socio de origen y la primera parte del nombre de archivo se utiliza para evaluar el nombre de socio de destino. La posición del directorio en la estructura de directorios se utiliza para evaluar si la transacción es una transacción de tipo producción o prueba.

Por ejemplo, se detecta un archivo denominado 123456789.abcdefg1234567 en el directorio `\ftproot\partnerTwo\binary\production`. El Gestor de documentos conoce la siguiente información:

- El `Nombre de socio de origen` es `partnerTwo` (porque el archivo se ha encontrado en la parte partnerTwo del árbol de directorios).
- El `Nombre de socio de destino` es `partnerOne` (porque la primera parte del nombre de archivo es 123456789, que es el ID de DUNS de partnerOne).

  Nota: aquí y en toda esta publicación, los números DUNS sólo se proporcionan como ejemplos. WebSphere Partner Gateway requiere <To_PartnerID> para coincidir con el DUNS del socio destinatario. En caso de que el ID de Duns no se encuentre, la búsqueda del canal fallará.
- El tipo de transacción es Producción.

El Gestor de documentos busca una conexión de socio de producción que vaya del socioDos al socioUno para:

- Paquete: Ninguno (N/D)
- Protocolo: Binario (1.0)
- Tipo de documento: Binario (1.0)

A continuación, el Gestor de documentos procesará el archivo.

Los archivos binarios también se puede transferir a través del FTP mediante el manejador de preproceso genérico o el manejador FileNamePartnerId. Consulte el apartado "Modificación del punto de configuración de preproceso" en la página 79 para obtener más información.

archivos XML

Un archivo XML que está direccionado utilizando las especificaciones XML personalizadas no tiene requisitos de nombre de archivo ya que el archivo es inspeccionado por el Gestor de documentos y la información de direccionamiento se extrae del mismo documento.

Cuando el componente Receptor detecta un archivo XML, se escribe en el almacenamiento compartido y se pasa al Gestor de documentos para su proceso.

El Gestor de documentos compara el archivo XML con los formatos XML que hayan sido definidos y selecciona el formato XML requerido. (La configuración de los formatos XML se describe en el apartado "Proceso de documentos de XML personalizado" en la página 159.) El nombre de socio de origen, el nombre de socio de destino y la información de direccionamiento se extraen del archivo XML.

La posición del directorio en la estructura de directorios se utiliza para evaluar si la transacción es una transacción de tipo producción o prueba.

El Gestor de documentos utiliza entonces esta información para localizar la conexión de socio correcta antes de procesar el archivo.

Configuración adicional del servidor FTP

Acerca de esta tarea

Después de crear la estructura de directorio requerida, configure el servidor FTP para cada uno de los socios en la comunidad del concentrador. La forma en que configure el servidor FTP depende del servidor que esté utilizando. Consulte la documentación del servidor FTP y realice las tareas siguientes:

Procedimiento

1. Añada un nuevo grupo (por ejemplo, Socios).
2. Añada un usuario al grupo recién creado para cada socio que envíe o reciba documentos a través de FTP.
3. Para cada socio, configure el servidor FTP para que correlacione el socio de entrada con la estructura de directorio que haya creado para el socio en el apartado anterior " Configuración de la estructura de directorios necesaria en el servidor FTP" en la página 36. Para obtener más información, consulte la documentación del servidor FTP

Consideraciones de seguridad para el servidor FTPS

Si está utilizando un servidor FTPS para recibir documentos de entrada, las consideraciones de seguridad para las sesiones SSL son gestionadas exclusivamente por el servidor FTPS y el cliente que está utilizando el socio. No existe una configuración de seguridad específica para WebSphere Partner Gateway destinada a los documentos FTPS entrantes. WebSphere Partner Gateway recupera los documentos del receptor FTP (que se describe en el apartado " Configuración de un receptor FTP" en la página 64) una vez el servidor ha negociado satisfactoriamente los canales seguros y recibido el documento. Consulte la documentación del servidor FTPS para determinar qué certificados son necesarios (y dónde lo son) para configurar satisfactoriamente un canal seguro con el que pueda contactar el socio.

Para la autenticación de servidor, proporcione a los socios el certificado del componente Receptor. Si el certificado se emite mediante una autoridad certificadora (CA), proporcione también la cadena de certificados de CA. Si la Autenticación de cliente está soportada por el servidor FTPS, los certificados de la Autenticación de cliente deberán especificarse en el servidor FTPS. Consulte la documentación del servidor FTPS para obtener información sobre la especificación de la Autenticación de cliente y los certificados de Autenticación de cliente.

Configuración del concentrador para el protocolo de transporte JMS

En este apartado se describe cómo configurar el concentrador para que utilice el transporte JMS. Si va a utilizar el transporte JMS para enviar documentos desde el concentrador o para recibir documentos en este, siga los procedimientos descritos en este apartado. Si no va a utilizar el transporte JMS, ignore este apartado.

Nota: los procedimientos de este apartado describen cómo utilizar la implementación de JMS de WebSphere MQ para configurar el entorno JMS. Los procedimientos también describen cómo configurar colas locales. Si desea configurar colas de transmisión y remotas, consulte la documentación de WebSphere MQ.

Aunque este apartado es específico de WebSphere MQ, otros proveedores JMS necesitarán el uso de procedimientos similares. Para WebSphere Platform Messaging, consulte el apartado "Configuración de JMS cuando WebSphere Partner Gateway está instalado en WebSphere Application Server" en el Capítulo 5, o bien "Integración de WebSphere Process Server con JMS como transporte" en la publicación Guía de integración de *WebSphere Partner Gateway*.

En posteriores apartados del documento, aprenderá cómo configurar los receptores o destinos JMS (o ambos). Estas tareas se describen en los apartados " Configuración de un receptor JMS" en la página 67 y "Configuración de un destino JMS" en la página 232.

Creación de un directorio para JMS

Acerca de esta tarea

En primer lugar debe crea un directorio para JMS. Por ejemplo, supongamos que deseara crear un directorio denominado JMS en el directorio c:\temp de una instalación Windows. Estos son los pasos que debe seguir:

Procedimiento

1. Abra el Explorador de Windows.
2. Abra el directorio C:\temp.
3. Cree una nueva carpeta llamada JMS.

Modificación de la configuración JMS predeterminada

Acerca de esta tarea

En este apartado, se actualiza el archivo JMSAdmin.config, que forma parte de la instalación de WebSphere MQ, para cambiar el URL del proveedor y de la fábrica de contexto.

1. Vaya al directorio `Java\bin` de WebSphere MQ. Por ejemplo, en una instalación Windows, debe ir a: C:\IBM\MQ\Java\bin
2. Abra el archivo JMSAdmin.config con un editor de texto plano, como el Bloc de notas de Windows o vi.
3. Añada el carácter # al inicio de las líneas siguientes:

   ```
   INITIAL_CONTEXT_FACTORY=com.sun.jndi.ldap.LdapCtxFactory
   PROVIDER_URL=ldap://polaris/o=ibm,c=us
   ```

4. Elimine el carácter # del inicio de las líneas siguientes:

   ```
   #INITIAL_CONTEXT_FACTORY=com.sun.jndi.fscontext.RefFSContextFactory
   #PROVIDER_URL=file:/C:/JNDI-Directory
   ```

5. Cambie la línea `PROVIDER_URL=file:/C:/JNDI-Directory` para que indique el nombre del directorio JMS que haya configurado en el apartado " Creación de un directorio para JMS" en la página 39. Por ejemplo, si configura el directorio `c:/temp/JMS`, la línea se parecería a la siguiente:

   ```
   PROVIDER_URL=file:/c:/temp/JMS
   ```

6. Guarde el archivo.

Creación de colas y del canal

En este apartado, WebSphere MQ se utiliza para crear colas que se emplearán para enviar y recibir documentos y el canal para esta comunicación. Se supone que se ha creado un gestor de colas. El nombre del gestor de colas debe indicarse donde aparece <*nombre_gestor_colas*> en los pasos siguientes. También se da por supuesto que se ha iniciado un receptor para este gestor de colas en el puerto TCP 1414.

1. Abra un indicador de línea de mandatos.
2. Especifique el mandato siguiente para iniciar el servidor de mandatos de WebSphere MQ:

   ```
   strmqcsv <nombre_gestor_colas>
   ```

3. Especifique el mandato siguiente para iniciar el entorno de mandatos de WebSphere MQ:

   ```
   runmqsc <nombre_gestor_colas>
   ```

4. Especifique el mandato siguiente para crear una cola WebSphere MQ que se utilizará para los documentos entrantes enviados al concentrador:

   ```
   def ql(<nombre_cola>)
   ```

   Por ejemplo, para crear una cola denominada JMSIN, debe especificar:

   ```
   def ql(JMSIN)
   ```

5. Especifique el mandato siguiente para crear una cola WebSphere MQ que se utilizará para los documentos enviados desde el concentrador:

   ```
   def ql(<nombre_cola>)
   ```

   Por ejemplo, para crear una cola denominada JMSOUT, debe especificar:

```
def ql(JMSOUT)
```

6. Especifique el siguiente mandato para crear un canal de WebSphere MQ que se utilizará para los documentos entrantes y salientes enviados al concentrador:

   ```
   def channel(<nombre_canal>) CHLTYPE(SVRCONN)
   ```

   Por ejemplo, para crear un canal denominado canal.java, debe especificar:

   ```
   def channel(canal.java) CHLTYPE(SVRCONN)
   ```

7. Especifique el mandato siguiente para salir del entorno de mandatos de WebSphere MQ:

   ```
   end
   ```

Adición de un tiempo de ejecución Java al entorno

Acerca de esta tarea

Especifique el siguiente mandato para añadir un tiempo de ejecución de Java™(TM) a la vía de acceso del sistema:

```
set PATH=<ProductDir>\_jvm\jre\bin
```

donde *DirProducto* se refiere al directorio en el que se ha instalado WebSphere Partner Gateway.

Definición de la configuración JMS

Acerca de esta tarea

Para definir la configuración de JMS, realice los pasos siguientes:

1. Vaya al directorio Java de WebSphere MQ (directorio *<vía_acceso_directorio_instalación_Websphere_MQ>*\java\bin)
2. Inicie la aplicación JMSAdmin especificando el mandato siguiente:

   ```
   JMSAdmin
   ```

3. Defina un nuevo contexto JMS especificando los mandatos siguientes desde el indicador InitCtx>:

   ```
   define ctx(<nombre_contexto>)
   change ctx(<nombre_contexto>)
   ```

   Por ejemplo, si el *nombre_contexto* es JMS, los mandatos son parecidos al siguiente:

   ```
   define ctx(JMS)
   change ctx(JMS)
   ```

4. Desde el indicador InitCtx/jms>, especifique la siguiente configuración de JMS:

   ```
   define qcf(nombre_fábrica_conexiones)
       tran(CLIENT)
       host(<su_dirección_IP>)
       port(1414)
       chan(java.channel)
       qmgr(<nombre_gestor_colas>)
   define q(<nombre>) queue(<nombre_cola>) qmgr(<nombre_gestor_colas>)
   define q(<nombre>) queue(<nombre_cola>) qmgr(<nombre_gestor_colas>)
   end
   ```

   Nota:

   - Si MQ y WebSphere Partner Gateway están instalados en dos máquinas diferentes, seleccione el tipo de transporte como CLIENT.

- Si MQ y WebSphere Partner Gateway están instalados en la misma máquina, el tipo de transporte debe ser BINDINGS.

En los pasos anteriores se ha creado el archivo .bindings, que se encuentra en una subcarpeta de la carpeta especificada en el paso 5 en la página 40. El nombre de la subcarpeta es el nombre especificado para el contexto JMS.

A modo de ejemplo mostramos la siguiente sesión JMSAdmin que se utiliza para definir la fábrica de conexiones de cola como `Hub`, con la dirección IP `sample.ibm.com` donde reside el gestor de colas MQ (<*nombre_gestor_colas*> de `sample.queue.manager`). El ejemplo utiliza los nombres de cola de JMS y el nombre de canal que se creó en el apartado "Creación de colas y del canal" en la página 40. Observe que la entrada del usuario sigue a la solicitud del >.

```
InitCtx> define ctx(jms)
InitCtx> change ctx(jms)
InitCtx/jms> define qcf(Hub)
    tran(CLIENT)
    host(sample.ibm.com)
    port(1414)
    chan(java.channel)
    qmgr(sample.queue.manager)
InitCtx/jms> define q(inQ) queue(JMSIN) qmgr(sample.queue.manager)
InitCtx/jms> define q(outQ) queue(JMSOUT) qmgr(sample.queue.manager)
InitCtx/jms>end
```

En este ejemplo, el archivo .bindings estaría ubicado en el siguiente directorio: `c:/temp/JMS/JMS`, donde `c:/temp/JMS` es PROVIDER_URL y `JMS` es el nombre de contexto.

Configuración de bibliotecas de tiempo de ejecución

Para el Receptor JMS o el Destino JMS, existen varios archivos jar de WebSphere MQ que deben ser visibles para WebSphere Partner Gateway. Estos archivos jar se hacen visibles al colocarlos en la vía de acceso de clases. Si, para acceder a MQ, utiliza la modalidad MQ Binding, las bibliotecas nativas de MQ también deben encontrarse en la vía de acceso. Consulte la documentación de WebSphere MQ para obtener más información sobre loas archivos jar de MQ y las bibliotecas nativas de JMS.

Existen varias formas de añadir los archivos jar a la vía de acceso de clases de Websphere Partner Gateway. Una de ellas es colocarlos en el directorio de salidas de usuario y otra es asociarlos mediante bibliotecas compartidas de WebSphere Application Server.

Método de directorio de salidas de usuario:

Para utilizar este método, coloque los archivos jar especificados en el directorio de Salidas de usuario apropiado:

- Para el Receptor JMS, colóquelos en el directorio <Raíz-instalación-WPG>/receiver/lib/userexits
- Para el Destino JMS, colóquelos en el directorio <Raíz-instalación-WPG>/router/lib/userexits

Método de bibliotecas compartidas de WebSphere Application Server

Acerca de esta tarea

Para utilizar este método, cree una variable de biblioteca compartida y, a continuación, asocie la variable con el Receptor o Aplicación de gestor de

documentos tal como se muestra brevemente en los siguientes pasos. Consulte la documentación de WebSphere Application Server para obtener más información sobre este procedimiento.

1. Inicie la sesión en la consola administrativa de WebSphere Application Server.
2. Cree la variable Bibliotecas compartidas completando lo siguiente:
   a. Vaya a **Entorno** > **Bibliotecas compartidas**.
   b. Seleccione un **Ámbito** (probablemente un nodo) y pulse **Nuevo**.
   c. Escriba el nombre de la variable (por ejemplo, MQ_LIBRARIES), complete las entradas de la vía de acceso de clases para los archivos jar de MQ y pulse **Aceptar**.
3. Asocie la variable de biblioteca compartida que creó con los componentes de WebSphere Partner Gateway completando lo siguiente:
   a. Vaya a **Aplicaciones** > **Aplicaciones de empresa**.
   b. Seleccione **BCGReceiver** (para receptores JMS) o **BCGDocMgr** (para destinos JMS).
   c. Seleccione **Referencias de biblioteca compartida**.
   d. Seleccione la aplicación y pulse **Bibliotecas compartidas de referencia**.
   e. En la Lista disponible, seleccione la variable de biblioteca compartida que creó (por ejemplo, MQ_LIBRARIES) y mueva la variable a la Lista seleccionada. A continuación, pulse **Aceptar**.

Configuración del receptor y la pasarela JMS con MQ externo

Acerca de esta tarea

A continuación se encuentran los pasos para crear un puente de comunicación entre WebSphere Partner Gateway y MQ a través de la consola administrativa de WebSphere Application Server:

1. Cree la Fábrica de conexiones de la cola JMS.
   a. Inicie la sesión en la consola administrativa de WebSphere Application Server.
   b. Vaya a **Recursos > JMS > Fábricas de conexión de cola**.
   c. Seleccione un **Ámbito** y pulse **Nuevo.**
      - Para la configuración de pasarela, seleccione el ámbito del servidor/nodo del gestor de documentos. (El ámbito de nodo es útil en caso de clústeres. Para la modalidad simple, seleccione un ámbito de servidor.)
      - Para la configuración del receptor, seleccione el ámbito del servidor/nodo del receptor. (El ámbito de nodo es útil en caso de clústeres. Para la modalidad simple, seleccione un ámbito de servidor.)
   d. Seleccione la opción **Proveedor de mensajería de WebSphere MQ** y pulse **Aceptar**.
   e. Introduzca el **Nombre** y **Nombre JNDI**. Estos son los valores necesarios.
   f. Introduzca los valores apropiados para el **Gestor de colas**, **Host** (IP de la máquina donde se está ejecutando el gestor de colas), **Puerto**, **Canal** y **Tipo de transporte**. El resto de los campos son opcionales.

      Nota:
      - Si MQ y WebSphere Partner Gateway están instalados en dos máquinas diferentes, seleccione el tipo de transporte como CLIENT.
      - Si MQ y WebSphere Partner Gateway están instalados en la misma máquina, el tipo de transporte debe ser BINDINGS.

Para obtener más detalles, consulte el InfoCenter de WebSphere Application Server InfoCenter en el sitio siguiente: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multipla...

2. Cree la cola JMS.
   a. Inicie sesión en la consola administrativa de WebSphere Application Server.
   b. Vaya a **Recursos > JMS > Colas**.
   c. Seleccione un **Ámbito** y pulse **Nuevo.**
      - Para la configuración de pasarela, seleccione el ámbito del servidor/nodo del gestor de documentos. (El ámbito de nodo es útil en caso de clústeres. Para la modalidad simple, seleccione un ámbito de servidor.)
      - Para la configuración del receptor, seleccione el ámbito del servidor/nodo del receptor. (El ámbito de nodo es útil en caso de clústeres. Para la modalidad simple, seleccione un ámbito de servidor.)
   d. Introduzca el **Nombre** y **Nombre JNDI**. Estos son los valores necesarios.
   e. Introduzca los valores apropiados para el **Gestor de colas**, **Host** (IP de la máquina donde se está ejecutando el gestor de colas), **Puerto**, **Canal** y **Tipo de transporte**. El resto de los campos son opcionales.
   f. Reinicie los servidores que han experimentado cambios, por ejemplo DocumentManager/Receiver/bcgserver en el caso de instalación distribuida simple.
3. Configure la pasarela JMS en WebSphere Partner Gateway.
   a. Inicie la sesión en la consola administrativa de WebSphere Partner Gateway.
   b. Pulse **Administración de cuentas > Perfiles > Destinos**.
   c. Pulse **Crear**.
   d. Introduzca el **Nombre de destino**. Se trata de un campo obligatorio.
   e. Seleccione **JMS** en el campo de transporte.
   f. Introduzca valores para los campos obligatorios siguientes:
      - Dirección: especifique la dirección de destino proporcionando el nombre de host apropiado y puerto de la Fábrica de conexión de colas u objetos de cola, que se crearon en WebSphere Application Server. La dirección debe estar en formato corbaloc:iiop: <hostname>: <bootstrapportnumber> , donde:
        – corbaloc:iiop - indica el protocolo utilizado para la comunicación entre el cliente (WebSphere Partner Gateway) y la búsqueda del servidor (WebSphere Application Server).
        – <nombre_host> - el nombre de host o la dirección IP de la máquina donde está instalado WebSphere Application Server, para el que la fábrica de conexión de cola y los objetos de cola se crearon.
        – <bootstrapportnumber> - el número de puerto de bootstrap del servidor donde la fábrica de conexión de cola y los objetos de cola están enlazados juntos. Para obtener el número de puerto de bootstrap, puede iniciar sesión en la consola administrativa de WebSphere Application Server, ir a **Servidores > Servidor de aplicaciones> <sever name> puertos** y comprobar la dirección de bootstrap. En el caso de modalidad distribuida, los números de puertos son diferentes para Receptor y Pasarela. Acceda al servidor correspondiente (bcgreceiver para Receptor y bcgdocmgr para Pasarela) para obtener el número de puerto de bootstrap correcto.
      - Nombre de la fábrica JMS: el nombre JNDI proporcionado por la fábrica de conexión de cola de JMS.

- Nombre de la cola JMS: el nombre JNDI proporcionado por la cola JMS.
- Nombre de la fábrica JNDI JMS: es la fábrica que se utiliza para la comunicación JNDI. Utilizando WebSphere Application Server, puede especificar el valor como com.ibm.websphere.naming.WsnInitialContextFactory.

4. Configure el receptor JMS en WebSphere Partner Gateway.
   a. Inicie la sesión en la consola administrativa de WebSphere Partner Gateway.
   b. Pulse **Administración del concentrador > Configuración del concentrador > Receptores**.
   c. Pulse **Crear destinatario**.
   d. Introduzca el **Nombre del receptor**. Se trata de un campo obligatorio.
   e. Seleccione **JMS** en el campo de transporte.
   f. Introduzca valores apropiados para los campos requeridos como se describen en el paso:3f en la página 44.

Configuración de la compresión RNIF

Los mensajes de empresa de RosettaNet y sus archivos adjuntos se comprimen y se empaquetan mediante el sobre S/MIME para transferir documentos grandes. Asimismo, se proporciona soporte de descompresión para los mensajes de empresa de RosettaNet. Se proporciona una opción para comprimir la carga ya sea sola o junto con archivos adjuntos. Para mejorar el rendimiento, comprima el contenido de servicio y sus ardchivos adjuntos antes del cifrado, firma o codificación de transferencia según la Especificación técnica recomendada de RosettaNet 2.0. Bajo el canal de WebSphere Partner Gateway de RosettaNet correspondiente, seleccione la compresión de atributo de objeto de direccionamiento para que tenga uno de los siguientes valores:

- Ninguno
- Carga
- Carga y archivo adjunto

Además de la opción de compresión seleccionada, también puede seleccionar atributos de criterios de filtro adicionales como **Tipo de contenido de compresión** y **Tamaño de compresión**. Puede seleccionar la carga o los archivos adjuntos para comprimir en la agrupación de archivos adjuntos mediante los criterios de filtro. El **Tipo de contenido de compresión** espera “Todo” o los tipos MIME válidos separados mediante comas. Si selecciona la opción **Carga** en la compresión base, la carga se comprimirá independientemente dle valor especificado en el atributo de objeto de direccionamiento **Tipo de contenido de compresión**. Sólo se seleccionan archivos adjuntos para comprimir en función de los tipos de ocntenido especificados. El atributo de objeto de direccionamiento **Tamaño de compresión** espera “Todo” o un límite de tamaño válido. El límite de tamaño válido indica el tamaño mínimo aceptable para la compresión.

Cuando se envía un documento comprimido de RosettaNet, la descompresión S/MIME se realiza sobre el contenido de servicio y sus archivos adjuntos.

Utilización de scripts de FTP para receptores y destinos de FTP Scripting

El transporte FTP Scripting permite enviar datos a cualquier servicio FTP, incluida una red de valor añadido (VAN). Las operaciones en el servidor FTP se controlan mediante un archivo script que incluye mandatos FTP.

Este script se especifica cuando se crea el receptor o destino de FTP Scripting. WebSphere Partner Gateway sustituye los valores reales especificados cuando se crea el receptor o destino para las posiciones en el script FTP.

Las operaciones definidas en el script de entrada se convierten en acciones en el servidor FTP. El script de entrada consta de un grupo de mandatos FTP soportados. Los parámetros para estos mandatos pueden tener el formato de una variable, que se rellena en el tiempo de ejecución.

Para obtener más información acerca de la creación de un script FTP para un receptor de FTP Scripting, consulte el apartado " Configuración de un receptor de FTP Scripting" en la página 70. Para obtener más información acerca de la creación de un script FTP para un destino de FTP Scripting, consulte el apartado "Configuración de un destino de FTP Scripting" en la página 239.

Utilización de correlaciones desde Data Interchange Services Client

Para realizar las acciones de validación, transformación y desensobrado EDI, o para realizar transformaciones entre ROD, XML y EDI, es necesario importar las correlaciones asociadas de Data Interchange Services Client. Data Interchange Services es un programa que se instala aparte y que normalmente reside en un sistema distinto del sistema en el que se ejecuta WebSphere Partner Gateway.

El especialista en correlaciones de Data Interchange Services crea correlaciones que describen cómo deben transformarse y validarse documentos concretos.

Para crear cualquier correlación, es necesaria la definición del documento de origen y el de destino. WDI suministra las definiciones de los documentos de origen a EDI, mientras que para ROD y XML deber crearla mediante el cliente DIS. Para EDI, importe el archivo .eif, el archivo estándar, en el cliente DIS. En el caso de ROD, cree el estándar mediante el cliente DIS. Importe DTD/XSD para crear el estándar para XML. Se puede compilar la correlación estándar y de transformación por separado.

Por ejemplo, puede que tenga un pedido de compra creado por una aplicación de fondo que desea transformar y enviar a un socio externo como un pedido de compra X12 EDI estándar (850). El especialista de correlaciones de Data Interchange Services escribirá una correlación que indica cómo transformar cada campo o segmento de datos del programa en formato X12. La correlación se exportará directamente a WebSphere Partner Gateway, o se exportará a un archivo, que luego se importará mediante un script de mandatos.

En el apartado " Importación manual de correlaciones" en la página 208 encontrará información detallada sobre cómo importar correlaciones desde Data Interchange Services Client.

Nota: El cliente DIS tiene su propia base de datos. Después de completar una correlación en un cliente DIS, expórtela como un archivo .EIF. Importe este archivo .EIF desde la consola de WebSphere Partner Gateway. Almacenará la información en la base de datos de WebSphere Partner Gateway.

Finalización de las tareas de configuración posteriores a la instalación

Después de instalar WebSphere Partner Gateway, es necesario configurarlo. Normalmente, esta configuración conlleva la utilización de la consola administrativa de WebSphere Partner Gateway para configurar el concentrador. En función de los requisitos de la comunidad comercial, es posible que también deba configurar la infraestructura de WebSphere Application Server que aloja los componentes de WebSphere Partner Gateway. A continuación se muestra una lista de dichas tareas junto con los enlaces a las instrucciones detalladas para realizar dicha tarea.

- "Cambio de la complejidad criptográfica" en la página 261
- "SSL con configuración de Autenticación de Cliente" en la página 263

Capítulo 5. Inicio del servidor y visualización de la Consola de comunidad

En este capítulo se muestra cómo iniciar el servidor WebSphere Partner Gateway y visualizar la Consola de comunidad. Incluye los siguientes temas:

- "Inicio de los componentes de WebSphere Partner Gateway"
- " Inicio de sesión en la Consola de comunidad" en la página 51

Para obtener información sobre cómo iniciar los Clústeres desde la consola administrativa de WebSphere Application Server Network Deployment consulte el Apartado 1. "Gestión de las aplicaciones de componentes de WebSphere Partner Gateway" de la publicación *Guía de administración de WebSphere Partner Gateway*.

Inicio de los componentes de WebSphere Partner Gateway

Acerca de esta tarea

Para iniciar el servidor, debe iniciar cada uno de los tres componentes de WebSphere Partner Gateway: la consola, el Gestor de documentos y el receptor.

En la modalidad simple, todos los componentes de WebSphere Partner Gateway se instalan en la misma instancia de WebSphere Application Server. Todos los componentes se inician y detienen mediante scripts y mediante la consola administrativa de WebSphere Application Server. Si desea iniciar los componentes de WebSphere Partner Gateway en un sistema de modalidad simple, ejecute el script:

```
<DIR INSTALACIÓN>/bin/bcgStartServer.sh
```

Si desea detener los componentes de WebSphere Partner Gateway en un sistema de modalidad simple, ejecute el script:

```
<DIR INSTALACIÓN>/bin/bcgStopServer.sh
```

Nota: No existe la necesidad de especificar un nombre de servidor al realizar la instalación en la modalidad simple. Cuando se realiza la instalación en la modalidad simple, el nombre de servidor es siempre server1.

Nota: Si se ejecuta el instalador cuando hay poco espacio en el directorio **temp** y el producto no se instale correctamente, incremente el espacio en el directorio **temp** y desinstale y vuelva a instalar el producto.

1. Escriba http://<nombre_máquina o dirección_IP>:58080/console. El navegador visualizará la página de bienvenida. Inicie una sesión en WebSphere Partner Gateway con la siguiente información:
   - En el campo **Nombre de usuario**, escriba:
     `hubadmin`
   - En el campo **Contraseña**, escriba:
     `Pa55word`
   - En el campo **Nombre de inicio de sesión de empresa**, escriba:
     `Operador`

   Pulse **Iniciar sesión**.

2. Cuando inicie una sesión por primera vez, debe crear una nueva contraseña. Escriba una nueva contraseña y, a continuación, escriba la nueva contraseña una segunda vez en el campo **Verificar**.
3. Pulse **Guardar**. El sistema muestra la pantalla de entrada inicial de la Consola de comunidad.

Cuando se instala la aplicación WebSphere Partner Gateway, de forma predeterminada se instalan las aplicaciones Primeros pasos e IVT (Installation Verification Test). Permanecerán instaladas mientras esté instalado un componente de WebSphere Partner Gateway en la máquina. La página Primeros pasos llena los datos de componentes instalados para ejecutar la prueba de verificación de cada componente por separado.

La aplicación Primeros pasos se puede invocar con el mandato **bcgFirstSteps.sh**, que se encuentra disponible en la carpeta <dir_instalación>/FirstSteps/bin.

Desde la página Primeros pasos de la consola, se puede conmutar entre las opciones de inicio y detención de todos los componentes instalados. Por ejemplo, si el concentrador está en ejecución, aparecerá listada la opción para detenerlo. De lo contrario, aparecerá la opción para iniciarlo. En la siguiente lista se muestran las opciones de iniciar o detener los componentes en base a sus topologías:

- La opción para iniciar y detener WebSphere Process Gateway está disponible en topologías simples y distribuidas simples.
- La opción para iniciar y detener MAS está disponible en topologías distribuidas simples y distribuidas completas.
- La opción para iniciar y detener el gestor de despliegue está disponible en topologías distribuidas simples y distribuidas completas.

  Nota: Esta opción únicamente estará disponible si se instaló el gestor de despliegue mediante el instalador de WebSphere Partner Gateway.
- La opción para iniciar o detener la consola, el receptor y el direccionador están disponibles en una topología distribuida completa.
- La opción para iniciar o detener la gestión de FTP está disponible en todas las topologías.

Las opciones anteriores están disponibles para las topologías que se indican siempre que estén instaladas en dicha máquina. Es necesario verificar los registros del servidor para asegurarse que la acción se ha completado de forma satisfactoria. También existe la posibilidad de consultar la ventana de la línea de mandatos para comprobar el estado. Al pulsar el enlace **Iniciar WPG** en el panel Primeros pasos, se emite el mandato de inicio en el indicador de mandatos del sistema operativo de disco. El panel de Primeros pasos no notificará si el mandato se ha completado de forma satisfactoria (o si no lo ha hecho).

Cuando se invoca a la prueba de verificación de instalación (IVT), verifica la validez de los componentes de WebSphere Partner Gateway que se han instalado en la máquina. Otra posibilidad es invocar a la prueba de verificación desde la línea de mandatos con el mandato **LaunchIVT.sh**. Este mandato se encuentra en la carpeta <dir_instalación>/FirstSteps/ivt/bin. Después de completar la verificación, IVT genera un informe con los detalles de todos los componentes instalados de WebSphere Partner Gateway. Además, limpia los archivos temporales que se crearon durante esta operación y detiene todos los nodos/servidores iniciados para esta operación. Para indicar la anomalía de un componente, se generan los archivos de registro necesarios en la carpeta <dir_instalación>/FirstSteps/ivt/logs.

Nota: En una topología distribuida, IVT no verificará los componentes instalados en las distintas máquinas.

Cuando se intentan subir certificados con una criptografía más segura que la criptografía predeterminada, es posible que no se puedan subir los certificados.

Inicio de sesión en la Consola de comunidad

Acerca de esta tarea

En esta apartado se describen los pasos para visualizar e iniciar sesión en la consola de comunidad. La resolución de pantalla recomendada es 1024x768.

Nota: La consola de comunidad WebSphere Partner Gateway necesita soporte para cookies para encenderse y mantener la información de sesión. No se almacena información personal en la cookie y caduca cuando se cierra el navegador.

1. Abra un navegador web e introduzca la siguiente URL para mostrar la consola:

   http://<*hostname*>.<*domain*>:58080/console (no segura)

   https://<*hostname*>.<*domain*>:58443/console (segura)

   Donde<*hostname*> y <*domain*> son el nombre y la ubicación del sistema que aloja el componente de la consola de comunidad.

   Nota: Estos URL asume que se usa los números de puerto predeterminados. Si cambia los números de puerto predeterminados, sustituya los números predeterminados con los valores que haya especificado.

En la mayoría de casos, el administrador del concentrador le envía el nombre de usuario, contraseña inicial y el nombre de inicio de sesión de la empresa que utilizará para iniciar sesión en la consola de comunidad. Necesitará esta información para los procedimientos siguientes. Si no ha recibido esta información, póngase en contacto con el administrador del concentrador.

Para iniciar sesión en la consola de comunidad (estas instrucciones se aplican tanto a los socios internos como a los externos):

1. Especifique el **Nombre de usuario** para su empresa.
2. Especifique la **Contraseña** para su empresa.
3. Introduzca el **Nombre de inicio de sesión de la empresa**, por ejemplo, IBM.
4. Pulse **Iniciar sesión**. Cuando inicie sesión por primera vez, debe crear una contraseña nueva.
5. Introduzca una contraseña nueva, a continuación introdúzcala de nuevo en el cuadro de texto Verificar.
6. Pulse **Guardar**. El sistema muestra la pantalla de entrada inicial de la consola.

Nota: Si se configura WebSphere Partner Gateway mediante LDAP, deberá introducir el nombre de usuario de LDAP y la contraseña. El nombre de inicio de sesión de la empresa no es relevante en este caso, ya que no se le pedirá que introduzca dicha información. Además, el sistema no le pedirá que cambie la contraseña.

Capítulo 6. Configuración de la Consola de comunidad

Este capítulo describe cómo configurar la Consola de comunidad para especificar lo que ven los socios, cómo inician sesión en la consola y qué acceso tienen en las distintas tareas de consola. Este capítulo incluye los siguientes temas:

- "Especificación de la información de personalización de la consola y del entorno local"
- "Establecimiento de la política de contraseñas" en la página 55
- "Configuración de permisos" en la página 56
- "Cómo establecer el valor de tiempo de espera de la consola" en la página 57

No debe realizar ninguna de estas tareas si desea utilizar los valores predeterminados suministrados por WebSphere Partner Gateway.

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado la sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Especificación de la información de personalización de la consola y del entorno local

Acerca de esta tarea

De manera predeterminada, las páginas de la consola de comunidad aparecen en inglés. IBM facilita traducciones del contenido en otros idiomas como un conjunto de archivos que pueden subirse. Otros elementos de la consola que proporciona IBM para diferentes entornos locales son los gráficos del mensaje de cabecera. Si lo desea, puede subir sus propios gráficos de logotipos. También puede subir su propia hoja de estilo personalizada usada para formatear el texto en las páginas.

Para realizar estas tareas deberá utilizar la página de Subida del entorno local. Para visualizar la página de Subida del entorno local:

1. Pulse **Administración del concentrador > Configuración de consola > Configuración de entorno local**.
2. Pulse **Crear**.
3. Seleccione un entorno local de la lista **Entornos locales**.

La consola muestra la página Subida de entorno local.

En la página Subida de entorno local puede seleccionar la realización de las tareas siguientes:

- Personalice la consola subiendo un mensaje de cabecera o un logotipo exclusivos (o ambos).
- Suba los archivos que proporciona IBM para poder localizar el contenido de los elementos de la consola.

Personalización de consola

Acerca de esta tarea

Puede personalizar el aspecto de la Consola de comunidad cambiando las imágenes de personalización. La información de personalización de la Consola de comunidad consiste en la importación de dos imágenes: el fondo de cabecera y el logotipo de empresa.

- Se recomienda fondo de cabecera se extiende por la parte superior de la Consola de comunidad.
- Se recomienda logotipo de empresa aparece en la parte superior derecha de la Consola de comunidad.

Las imágenes deben ser archivos con el formato .JPG y deben ajustarse a ciertas especificaciones, para que quepan en la ventana de la Consola de comunidad.

- Para ver las especificaciones necesarias para la cabecera y el logotipo, pulse **Especificaciones de imagen** en la ventana Subida de entorno local.
- Para ver ejemplos de una imagen de cabecera o logotipo, desplácese a la parte de **Imágenes de ejemplo** de la página y pulse **sample_headerback.jpg** o **sample_logo.jpg**.
- Para descargar ejemplos de cabecera y logotipo y usarlos como plantilla para crear sus propios logotipo y cabecera, pulse **Imágenes de ejemplo (fondo de cabecera y logotipo de empresa)**.

Una vez que haya creado la cabecera o el logotipo (o ambos), realice los pasos siguientes:

1. Para subir la cabecera personalizada, realice una de las tareas siguientes:
   - En el campo **Mensaje de cabecera**, escriba la vía de acceso y el nombre del archivo de imagen que desea utilizar como cabecera/mensaje de cabecera.
   - Pulse **Examinar** para ir al archivo .jpg que contiene el mensaje de cabecera y selecciónelo.
2. Para subir el logotipo personalizado, realice uno de los pasos siguientes:
   - En el campo **Logotipo**, escriba la vía de acceso y el nombre del archivo que desea utilizar como logotipo de empresa.
   - Pulse **Examinar** para ir al archivo .jpg que contiene el logotipo y selecciónelo.
3. Pulse **Subir**.

Nota: cuando sustituya el fondo de cabecera y el logotipo de empresa, debe reiniciar la Consola de comunidad para que los cambios surtan efecto.

Cambio de la hoja de estilo

Acerca de esta tarea

Si desea especificar una hoja de estilo distinta del valor predeterminado (por ejemplo, si desea colores diferentes o fonts de distinto tamaño), realice las siguientes tareas:

1. Realice una de las siguientes tareas:
   - En el campo **CSS**, escriba la vía de acceso y el nombre del archivo que contiene la hoja de estilo personalizada.
   - Pulse **Examinar** para ir al archivo que contiene la hoja de estilo y selecciónelo.
2. Pulse **Subir**.

Localización de datos en la consola

Acerca de esta tarea

Si recibe paquetes compuestos de recursos o archivos de entorno local de IBM, puede utilizar la página de Subida de entorno local para subirlos. Los paquetes compuestos de recursos incluyen la información siguiente:

- **Etiquetas de consola**, que contienen cadenas de texto que representan todo el texto de la interfaz
- **Descripciones de sucesos**, que contienen cadenas de texto que se utilizan para mostrar los detalles del suceso (por ejemplo, "Se ha realizado un intento de crear una conexión duplicada")
- **Nombres de suceso**, que contiene cadenas de texto que representan los nombres de sucesos (por ejemplo, "La conexión ya existe")
- **Descripciones de sucesos EDI**, que contienen cadenas de texto que se utilizan para mostrar los detalles de sucesos EDI (por ejemplo, "Error de reconciliación de acuse de recibo funcional. No se ha encontrado ningún ID de actividad para las transacciones encontradas en el acuse de recibo de EDI. ")
- **Nombres de sucesos EDI**, que contienen cadenas de texto que representan nombres de sucesos EDI (por ejemplo, "Error de reconciliación de acuse de recibo funcional")
- **Texto de suceso ampliado**, que contienen cadenas de texto que proporcionan información sobre sucesos (por ejemplo, la causa del suceso y la información para la resolución de problemas)

Para subir un paquete de recursos u otro archivo de entorno local:

1. Para cada paquete o archivo de recursos, realice alguna de las tareas siguientes:
   - Escriba la vía de acceso y el nombre del archivo.
   - Pulse **Examinar** para ir al archivo y selecciónelo.
2. Cuando termine de subir los archivos, pulse **Subir**.

Establecimiento de la política de contraseñas

Puede establecer una política de contraseñas para la comunidad del concentrador, si desea utilizar unos valores distintos a los definidos de forma predeterminada (por el sistema). La política de contraseñas se aplica a todos los usuarios que inician sesión en la Consola de comunidad.

Puede cambiar los elementos siguientes de la política de contraseñas:

- Longitud mínima, que representa el número mínimo de caracteres que debe utilizar el socio para la contraseña. El valor predeterminado es 8 caracteres.
- Tiempo de caducidad, que representa el número de días que faltan para que caduque la contraseña. El valor predeterminado es de 30 días.
- Singularidad, que especifica el número de contraseñas que deben contenerse en un archivo de historial. Un socio no puede utilizar una contraseña antigua si existe en el archivo de historial. El valor predeterminado es 10 contraseñas.
- Caracteres especiales, que, si se seleccionan, indican que las contraseñas deben contener al menos tres de los tipos de caracteres especiales siguientes:
  - Caracteres en mayúsculas
  - Caracteres en minúsculas
  - Caracteres numéricos
  - Caracteres especiales

Este valor permite unos requisitos de seguridad más estrictos cuando las contraseñas se componen de caracteres ingleses (ASCII). El valor predeterminado es Desactivado. Se recomienda que tenga desactivados los caracteres especiales cuando las contraseñas se compongan de caracteres internacionales. Los juegos de caracteres distintos del inglés podrían no contener los tres tipos necesarios de los cuatro tipos de caracteres.

Los caracteres especiales que el sistema soporta son: '#', '@', '$', '&', '+'.

- Comprobación de variación de nombre, que si se selecciona, impide el uso de contraseñas que contengan una variación fácilmente deducible del nombre real o del de inicio de sesión del usuario. Este campo está seleccionado de forma predeterminada.

Para cambiar los valores predeterminados:

1. Pulse **Administración del concentrador > Configuración de consola > Política de contraseña**. Aparece la página Política de contraseña.
2. Pulse el icono **Editar**.
3. Cambie cualquiera de los valores predeterminados a aquellos que desee utilizar para la política de contraseñas.
4. Pulse **Guardar**.

Configuración de permisos

Los permisos representan privilegios que debe poseer un usuario para acceder a los distintos módulos de la consola.

Cómo se otorgan los permisos a los usuarios

Antes de configurar los permisos, resulta útil entender cómo se conceden a los usuarios individuales. Los tres tipos de entidades en la comunidad del concentrador (el administrador del concentrador, el socio interno y los socios externos) pueden tener un usuario Administrador. Cuando cree un Socio interno o un socio, cree también el usuario Administrador para dicha entidad.

Nota: En el caso del socio Operador del concentrador, se crean en el momento de la instalación dos usuarios administrativos: un usuario Admin y el usuario hubadmin.

Cuando cree el socio (como se define en el apartado “Creación de perfiles de socio” en la página 25), proporcionará al socio la información de inicio de sesión (como el nombre a utilizar para iniciar la sesión y la contraseña). Una vez el socio inicia sesión, el socio crea usuarios adicionales dentro de la organización. El socio también crea grupos y asigna usuarios a dichos grupos. Por ejemplo, una organización puede querer tener un grupo para las personas que supervisen el volumen de los documentos. El socio crearía un grupo Volumen y le añadiría usuarios.

Nota: Como el usuario administrador del concentrador (hubadmin), también puede definir los usuarios y grupos de un socio.

El usuario Administrador del socio asignaría entonces permisos a dicho grupo de usuarios. Por ejemplo, el usuario Administrador podría decidir que el grupo Volumen sólo debe ver los informes de Análisis de documentos y Volumen de documentos. En ese caso, el usuario Administrador habilitaría el módulo de informes de documentos pero inhabilitaría el resto de módulos para el grupo Volumen con ayuda de la página de Detalles del grupo.

El valor que el Administrador del concentrador define en la página de Permisos determina si un módulo aparece o no en la página de Detalles del grupo.

Algunos módulos están restringidos a determinados miembros de la comunidad del concentrador (por ejemplo, los administradores del concentrador, como hubadmin). Además, incluso si se habilita uno de estos módulos para que sea utilizado por un socio, el módulo no aparecerá en la página Detalles de grupo del socio.

Habilitación o inhabilitación de permisos

Acerca de esta tarea

Desde la página Lista de permisos, puede determinar qué permisos están disponibles para su asignación a grupos de usuarios habilitando o inhabilitando los permisos. Sin embargo, no puede definir permisos nuevos.

Para cambiar los permisos predeterminados:

1. Pulse **Administración del concentrador > Configuración de consola > Permisos**. Aparece la Lista de permisos.
2. Si desea cambiar los valores predeterminados, lleve a cabo los siguientes pasos:
   a. Pulse sobre el valor actual (**Habilitado** o **Inhabilitado**) para cambiar el valor.
   b. Cuando se le solicite que confirme el cambio, pulse el botón **Aceptar**.

Cómo establecer el valor de tiempo de espera de la consola

El valor de tiempo de espera de sesión predeterminado de 30 minutos podría no ser aceptable en las siguientes situaciones:

- Los usuarios en entornos seguros podrían necesitar periodos de tiempo de espera de sesión más breves para lograr una mayor seguridad. Esto también podría aplicarse siempre que dejasen sus máquinas y olvidasen de cerrar la sesión desde la consola.
- Los usuarios podrían requerir periodos de tiempo de espera de sesión más extensos si deben responder de una forma más lenta por razones de accesibilidad que los usuarios habituales.

Siga los siguientes pasos para establecer el valor de tiempo de espera para la consola de WebSphere Partner Gateway:

1. Abra la consola de WebSphere Application Server.
2. Vaya a **Servidores** > **Servidores de aplicaciones** > **bcgserver** > **Valores de contenedor web** > **Contenedor web**> **Gestión de sesión**.
3. En la página **Gestión de sesión**, seleccione **Establecer tiempo de espera** en la sección **Tiempo de espera de sesión**.
4. Especifique el valor en minutos. El valor predeterminado es 30 minutos.
5. Pulse **Aplicar**.

Capítulo 7. Definición de receptores

Este capítulo describe cómo configurar receptores en WebSphere Partner Gateway. Incluye los siguientes temas:

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado la sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Visión general de receptores

Como se describe en el apartado "Visión general del proceso de documentos" en la página 12, el *receptor* es responsable de aceptar documentos entrantes de un transporte determinado. Una instancia de receptor se configura para un despliegue determinado.

Los documentos recibidos en un receptor del concentrador pueden proceder de socios externos (para la eventual entrega al socio interno) o de una aplicación de fondo del socio interno (para su eventual entrega a socios externos).

La Figura 16 en la página 60 muestra un servidor de WebSphere Partner Gateway con cuatro receptores configurados. Dos de los receptores (HTTP/S y FTP/S) son para documentos procedentes de socios. Estos dos receptores representan un URI de HTTP y un directorio FTP. La información acerca de estos receptores se proporciona a los socios para indicar dónde deben enviar los documentos. Los otros dos receptores (JMS y el directorio de archivos) son para documentos que se originan a partir de la aplicación de fondo del socio interno. Estos receptores representan una cola y un directorio.

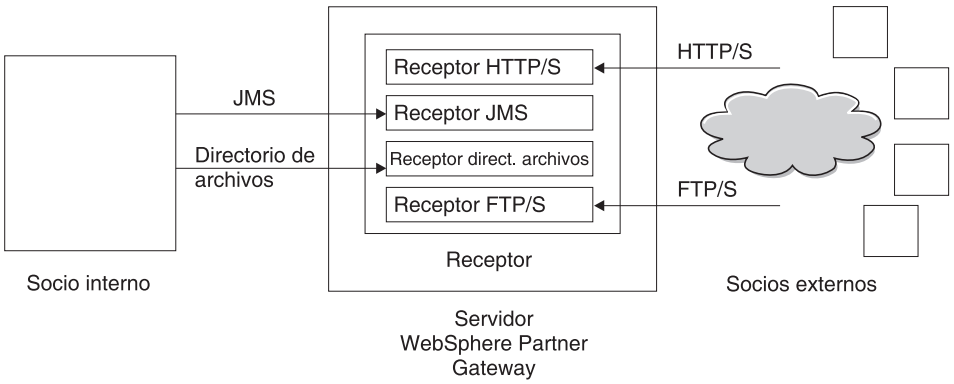


Figura 16. Transportes y receptores asociados

Configure, al menos, un receptor para cada tipo de transporte mediante el que se enviarán los documentos al concentrador. Por ejemplo, tendrá un receptor HTTP para recibir cualquier documento enviado a través de un transporte HTTP y HTTPS. Si los socios externos enviarán documentos mediante FTP, debe configurar un receptor FTP.

Si tiene algún requisito especial para algunos documentos que haya recibido, es posible que necesite configurar más de un receptor para un transporte determinado. En este caso, puede comunicar a los socios dichos requisitos y pedirles que envíen dichos documentos a direcciones específicas para que pueda realizarse el proceso del receptor correcto.

El componente Receptor detecta cuando llega un mensaje a uno de los receptores. Algunos receptores detectan mensajes sondeando sus transportes a intervalos regulares o en base a una planificación para determinar si han llegado nuevos mensajes. Los receptores de WebSphere Partner Gateway basados en sondeo son: JMS, FTP, SMTP, File y FTP Scripting. El receptor HTTP/S se basa en llamadas de retorno, lo cual quiere decir que recibe una notificación del transporte cuando llegan los mensajes. Los transportes definidos por el usuario pueden basarse en sondeos o en llamadas de retorno.

Subida de manejadores definidos por el usuario

Acerca de esta tarea

Los puntos de configuración pueden modificarse para receptores especificando un manejador para el receptor. El manejador lo puede proporcionar WebSphere Partner Gateway o puede ser un manejador definido por el usuario. En este apartado se describe cómo subir un manejador definido por el usuario. Utilice este apartado únicamente para manejadores definidos por el usuario. Los manejadores proporcionados por WebSphere Partner Gateway ya están disponibles.

Para subir un manejador, lleve a cabo los siguientes pasos:

1. En el menú principal, pulse **Administración del concentrador > Configuración del concentrador > Manejadores**.
2. Pulse **Destinatario**.

   Aparecerá la lista de manejadores actualmente definidos para los receptores. Observe que los manejadores suministrados por WebSphere Partner Gateway tienen el ID de proveedor **Producto**.
3. En la página Lista de manejadores, pulse **Importar**.

4. En la página Importar manejador, especifique la vía de acceso al archivo XML que describe el manejador o utilice **Examinar** para buscar dicho archivo XML.

Después de haber subido un manejador, puede utilizarlo para personalizar los puntos de configuración de los receptores.

Manejadores de preproceso genéricos

El manejador de configuración de preproceso está disponible en todos los tipos de receptores, pero no es aplicable a receptores SMTP. La tabla siguiente describe los atributos que puede establecer para un manejador de preproceso genérico:

Tabla 2. Manejador de preproceso genérico

Atributos	**Descripción**
Nombre De empaquetado	Este atributo indica el empaquetado asociado con el documento. Este valor debe coincidir con el paquete especificado en la definición del documento.
Versión De empaquetado	Este atributo indica la versión del empaquetado especificado en **Nombre de empaquetado**. Por ejemplo, si el documento tiene el paquete Ninguno, este valor será N/D.
Nombre De protocolo	Este atributo indica el protocolo asociado con el documento. Este valor debe coincidir con el protocolo especificado en la definición del documento.
Versión De protocolo	Este atributo indica la versión del protocolo especificado en **Nombre de protocolo**.
Código De proceso	Este atributo indica el proceso (tipo de documento) asociado con este documento. Este valor debe coincidir con el tipo de documento en la definición del documento.
Versión De proceso	Este atributo indica la versión del proceso especificado en **Código de proceso**.
METADICTIONARY	Este atributo indica el nombre del diccionario para el que está asociada la definición del documento. Este valor debe coincidir con el protocolo especificado en el campo Nombre de protocolo.
METADOCUMENT	Este atributo indica el nombre de la definición del documento asociado con este documento. Este valor debe coincidir con el proceso especificado en el campo Código de proceso.
METASYNTAX	Este atributo indica la sintaxis del documento que se procesará en este receptor; los valores permitidos son ediIchg(intercambio EDI) / xml / rod (archivo sin formato).
ENCODING	Este atributo indica la codificación de caracteres del documento. El valor predeterminado es ASCII.
BCG_BATCHDOCS	Este atributo está establecido en **ON** si quiere que los documentos se procesen en un lote.
SenderId, ReceiverId	Este atributo indica el ID del receptor, el ID del remitente, que son los ID de empresa de los participantes como están configurados en sus perfiles.

Configuración de valores de transporte global

Acerca de esta tarea

Establezca los atributos de transporte global que se aplican a los receptores de FTP Scripting. Si no está definiendo receptores de FTP Scripting, este apartado no es pertinente.

1. Pulse **Administración de concentrador > Configuración de concentrador > Receptores** para visualizar la lista de receptores.
2. Pulse el enlace **Atributos globales de transporte**.
3. Si los valores predeterminados son adecuados para la configuración, pulse **Cancelar**. En caso contrario, continúe con los restantes pasos en este apartado.
4. Pulse el icono **Editar** situado junto a **Atributos globales listados por categoría**.
5. Revise y, si es necesario, cambie los valores de **Transporte FTP Scripting** y **FTP Scripting - Receptores y destinos**.

   El transporte FTP Scripting utiliza un mecanismo que impide que más de una instancia de FTP Scripting acceda al mismo receptor al mismo tiempo. Cuando un transporte FTP Scripting está preparado para enviar documentos, solicita este bloqueo. Se proporcionan valores predeterminados, como el tiempo que debe esperar una instancia de receptor para obtener el bloqueo y cuántas veces intenta recuperarlo si el bloqueo está siendo utilizado. Puede utilizar estos valores predeterminados o cambiarlos. Para cambiar uno o varios de los valores, escriba el nuevo valor o los nuevos valores. Puede cambiar:

   - Valores de **Transporte FTP Scripting**
     - **Recuento de reintento de bloqueo**, que indica cuántas veces intentará el receptor obtener un bloqueo si el bloqueo está siendo utilizado en la actualidad. El valor predeterminado es 3.
     - **Intervalo de reintento de bloqueo (segundos)**, que indica el periodo de tiempo que transcurrirá entre intentos para obtener el bloqueo. El valor predeterminado es 260 segundos.
   - Valores de **FTP Scripting - Receptores y destinos**
     - **Tiempo máximo de bloqueo (segundos)**, que indica cuánto tiempo puede el destino retener el bloqueo. El valor predeterminado es 240 segundos.
     - **Cola máxima de bloqueo (segundos)**, que indica cuánto tiempo esperará el receptor en una cola para obtener el bloqueo. El valor predeterminado es 740 segundos.
6. Pulse **Guardar**.

Configuración de un receptor HTTP/S

Acerca de esta tarea

El componente Receptor tiene un servlet bcgreceiver predefinido que se utiliza para recibir mensajes de HTTP/S POST. Cree uno o más receptores HTTP para acceder a los mensajes recibidos por el servlet.

Los siguientes pasos describen qué necesita especificar para un receptor HTTP/S.

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** para mostrar la página Lista de receptor.
2. En la página Lista de receptores, pulse **Crear receptor**.

Detalles del receptor

Acerca de esta tarea

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

Procedimiento

1. Escriba un nombre para el receptor. Por ejemplo, puede llamar al receptor HttpReceiver1. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptores.
2. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está listo para recibir documentos. Un receptor que está inhabilitado no puede aceptar documentos.
3. Si lo desea, especifique una descripción del receptor.
4. Seleccione **HTTP/S** en la lista **Transporte**.

Configuración del receptor

Acerca de esta tarea

En el apartado **Configuración del receptor**, lleve a cabo los siguientes pasos:

1. Si lo desea, especifique la modalidad de operación. La modalidad de operación define la naturaleza de la transmisión. Por ejemplo, si desea probar un intercambio de documentos antes de ponerlo en producción, especifique **Probar**. El valor predeterminado es **Producción**.
2. Escriba el URI del receptor HTTP/S. El nombre debe empezar por **bcgreceiver**. Por ejemplo, puede escribir /bcgreceiver/Receiver. Los documentos que llegan al servidor mediante HTTP/S se recibirán en /bcgreceiver/Receiver.
3. Para autenticar un receptor HTTP/S mediante el atributo header, establezca el distintivo **Habilitar autenticación básica** en true. El valor predeterminado es false.
4. Revise y, si es necesario, cambie los valores de **Transporte HTTP/S**. Puede cambiar:
   - **Tiempo de espera síncrono máximo (segundos)**, para indicar el número de segundos que una conexión síncrona puede permanecer abierta. El valor predeterminado es de 300 segundos.
   - **Número máximo de conexiones síncronas simultáneas**, que indica la cantidad de conexiones síncronas que aceptará el sistema. El valor predeterminado es 100 conexiones.

Nota: Puede editar los valores de **Direccionamiento síncrono**.

Manejadores

Si va a recibir archivos que contienen varios intercambios EDI o documentos XML o ROD que es necesario dividir, configure el manejador de divisor correspondiente en el punto de configuración de preproceso.

Si va a enviar o a recibir determinados tipos de documentos de empresa (RosettaNet, cXML, SOAP y AS2) a través de un intercambio síncrono, especifique un manejador para el protocolo asociado en el punto de configuración de comprobación síncrona.

También puede modificar los puntos de configuración de postproceso para el receptor.

Para modificar un punto de configuración, vaya al apartado " Modificación de puntos de configuración" en la página 77. De lo contrario, pulse **Guardar**.

Configuración de un receptor FTP

Acerca de esta tarea

Un receptor FTP sondea el servidor FTP a un intervalo determinado para buscar nuevos documentos.

Los siguientes pasos describen qué es necesario especificar para un receptor FTP.

Procedimiento

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** para mostrar la página Lista de receptor.
2. En la página Lista de receptores, pulse **Crear receptor**.

Resultados

Detalles del receptor

Acerca de esta tarea

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

Procedimiento

1. Escriba un nombre para el receptor. Por ejemplo, puede llamar al receptor FTPReceiver1. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptores.
2. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está preparado para aceptar documentos. Un receptor que está inhabilitado no puede aceptar documentos.
3. Si lo desea, especifique una descripción del receptor.
4. Seleccione **Directorio FTP** en la lista **Transporte**.

Configuración del receptor

Acerca de esta tarea

En el apartado **Configuración del receptor**, lleve a cabo los siguientes pasos:

1. En el campo del **directorio raíz FTP**, especifique el directorio raíz en el servidor FTP. El Gestor de documentos sondeará automáticamente los subdirectorios del socio dentro del directorio raíz de FTP para buscar el direccionamiento de documentos. Se trata de un campo obligatorio. Consulte el apartado "Configuración del servidor FTP para la recepción de documentos" en la página 35 para obtener información sobre cómo configurar el directorio para un servidor FTP.

   Nota: Escriba la vía de acceso de directorio que finaliza en el directorio raíz FTP. No incluya los subdirectorios del socio.
2. Si lo desea, especifique un valor para **Intervalo no cambiado de archivo** para indicar el número de segundos que debe permanecer sin modificación el tamaño del archivo antes de que el Gestor de documentos recupere el documento para su procesado. Este periodo de intervalo sin modificar

garantiza que un documento haya completado su transmisión (y que no esté aún en tránsito) cuando el Gestor de documentos lo recupera. El valor predeterminado es 3 segundos.

3. Si lo desea, especifique un valor para **Número de hebras**, para indicar el número de documentos que el Gestor de documentos puede procesar simultáneamente. Se recomienda utilizar el valor predeterminado 1.
4. Si lo desea, especifique un valor en **Extensiones de archivo a excluir** para indicar los tipos de documentos que debe omitir el Gestor de documentos (no procesar) si encuentra los documentos en el directorio FTP. Por ejemplo, si desea que el Gestor de documentos omita los archivos de hojas de cálculo, debe especificar su extensión. Después de escribir la extensión, pulse **Añadir**. A continuación, la extensión se añade a la lista de extensiones de archivos que deben omitirse. De manera predeterminada, no se excluye ningún tipo de archivo.

   Nota: no utilice un punto antes de la extensión del nombre de archivo (por ejemplo: .exe o . txt). Utilice sólo caracteres que denotan la extensión de archivos.

Manejadores

Si va a recibir archivos que contienen varios intercambios EDI o documentos XML o ROD que es necesario dividir, configure el manejador de divisor correspondiente en el punto de configuración de preproceso.

Para modificar el punto de configuración de preproceso, vaya al apartado " Modificación de puntos de configuración" en la página 77. De lo contrario, pulse **Guardar**.

Configuración de un receptor SMTP (POP3)

Acerca de esta tarea

Un receptor SMTP sondea el servidor de correo POP3 (de acuerdo con la planificación que especifique) en busca de nuevos documentos.

Los siguientes pasos describen qué necesita especificar para un receptor SMTP (POP3).

Procedimiento

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** para mostrar la página Lista de receptores.
2. En la página Lista de receptores, pulse **Crear receptor**.

Resultados

Detalles del receptor

Acerca de esta tarea

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

Procedimiento

1. Escriba un nombre para el receptor. Por ejemplo, puede llamar al receptor POP3Receiver1. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptores.

2. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está preparado para aceptar documentos. Un receptor que está inhabilitado no puede aceptar documentos.
3. Si lo desea, especifique una descripción del receptor.
4. Seleccione **POP3** en la lista **Transporte**.

Configuración del receptor

Acerca de esta tarea

En el apartado **Configuración del receptor** de la página, lleve a cabo los siguientes pasos:

Procedimiento

1. Si lo desea, inicie el modo de operación. El modo de operación define la naturaleza de la transmisión. Por ejemplo, si desea probar un intercambio de documentos antes de ponerlo en producción, especifique **Probar**. El valor predeterminado es **Producción**.
2. Especifique la ubicación del servidor POP3 a la cual se entrega el correo. Por ejemplo, puede especificar una dirección IP.
3. Si lo desea, especifique un número de puerto. Si no especifica ningún valor, se utilizará 110.
4. Especifique el ID de usuario y la contraseña necesarios para acceder al servidor de correo, si éstos son obligatorios.
5. **Número de hebras** está en modalidad de sólo lectura. Indica el número de documentos que el Gestor de documentos puede procesar de forma simultánea.

Planificación

Acerca de esta tarea

En el apartado **Planificación** de la página, realice los pasos siguientes:

1. Seleccione **Planificación basada en intervalos** o **Planificación basada en calendario**.
2. Realice uno de los conjuntos de pasos siguientes:
   - Si selecciona **Planificación basada en intervalos**, seleccione el número de segundos que deben transcurrir antes de volver a sondear al servidor POP3 (o acepte el valor predeterminado). Si selecciona el valor predeterminado, el servidor POP3 se sondea cada 5 segundos.
   - Si selecciona **Planificación basada en calendario**, elija el tipo de planificación (**Planificación diaria**, **Planificación semanal** o **Planificación personalizada**).
     - Si selecciona **Planificación diaria**, seleccione la hora del día (hora y minutos) en que debe sondearse el POP3.
     - Si elige **Planificación semanal**, seleccione uno o varios días de la semana además de la hora del día.
     - Si elige **Planificación personalizada**, seleccione la hora del día y luego **Rango** o **Días selectivos** para la semana y el mes. Con **Rango**, indique la fecha de inicio y la fecha de finalización. (Por ejemplo, puede pulsar **Lunes** y **Viernes** si desea que el servidor se sondee a una determinada hora únicamente los días laborables). Con **Días selectivos** puede elegir los días concretos de la semana y del mes.

Manejadores

Si va a recibir archivos que contienen varios intercambios EDI o documentos XML o ROD que es necesario dividir, configure el manejador de divisor correspondiente en el punto de configuración de preproceso.

Para modificar el punto de configuración de preproceso, vaya al apartado " Modificación de puntos de configuración" en la página 77. De lo contrario, pulse **Guardar**.

Configuración de un receptor JMS

Acerca de esta tarea

Un receptor JMS sondea una cola JMS (de acuerdo con la planificación que especifique) en busca de nuevos documentos.

Los siguientes pasos describen qué es necesario especificar para un receptor JMS.

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** para mostrar la página Lista de receptor.
2. En la página Lista de receptores, pulse **Crear receptor**.

Nota: Para obtener información sobre cómo configurar las bibliotecas de tiempo de ejecución para que los archivos jar de MQ necesarios sean visibles para WebSphere Partner Gateway, consulte el apartado "Configuración de bibliotecas de tiempo de ejecución" en la página 42.

Detalles del receptor

Acerca de esta tarea

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

1. Escriba un nombre para el receptor. Por ejemplo, puede llamar al receptor JMSReceiver1. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptor.
2. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está preparado para aceptar documentos. Un receptor que está inhabilitado no puede aceptar documentos.
3. Si lo desea, especifique una descripción del receptor.
4. Seleccione **JMS** en la lista **Transporte**.

Configuración del receptor

Acerca de esta tarea

En el apartado **Configuración del receptor** de la página, lleve a cabo los siguientes pasos:

1. Si lo desea, indique el **Tipo de funcionamiento**. El tipo de operación define la naturaleza de la transmisión. Por ejemplo, si desea probar un intercambio de documentos antes de ponerlo en producción, especifique **Probar**. El valor predeterminado es *Producción*.
2. Especifique el **URL del proveedor JMS**. Este valor debe coincidir con el valor especificado (la vía de acceso al archivo de enlaces) al configurar WebSphere

Partner Gateway para JMS (paso 5 en la página 40). También puede especificar la subcarpeta para el contexto JMS como parte del URL del proveedor JMS.

Por ejemplo, sin el contexto JMS, debería indicar `c:/temp/JMS`. Con el contexto JMS, debería indicar `c:/temp/JMS/JMS`.

3. Especifique el **ID de usuario** y la **Contraseña** que se necesitan para acceder a la cola JMS, si es necesario.
4. Especifique un valor para **Nombre de cola JMS**. Se trata de un campo obligatorio. Este nombre debe coincidir con el especificado con el mandato `define q` al crear el archivo de enlaces (paso 4 en la página 41).

   Si ha especificado la subcarpeta para el contexto JMS en el paso 2 en la página 67, indique aquí sólo el nombre de cola (por ejemplo, `inQ`). Si no ha especificado la subcarpeta para el contexto JMS en el URL del proveedor JMS, especifique la subcarpeta antes del nombre de fábrica (por ejemplo, `JMS/inQ`).
5. Especifique un valor para **Nombre de fábrica JMS**. Se trata de un campo obligatorio. Este nombre debe coincidir con el especificado con el mandato `define qcf` al crear el archivo de enlaces (paso 4 en la página 41).

   Si ha especificado la subcarpeta para el contexto JMS en el paso 2 en la página 67, indique aquí sólo el nombre de fábrica (por ejemplo, `Hub`). Si no ha especificado la subcarpeta para el contexto JMS en el URL del proveedor JMS, especifique la subcarpeta antes del nombre de fábrica (por ejemplo, `JMS/Hub`).
6. Si lo desea, especifique el **Paquete de URL del proveedor**.
7. Introduzca el **Nombre de fábrica JNDI**. Se trata de un campo obligatorio. El valor de com.sun.jndi.fscontext.RefFSContextFactory es probablemente el que se utilizará si se establece la configuración de JMS para WebSphere MQ tal como se describe en el apartado "Configuración del concentrador para el protocolo de transporte JMS" en la página 39.
8. Especifique el **Nombre de usuario JMS** y la **Contraseña JMS**.
9. Si lo desea, especifique un valor para **Tiempo de espera**, para indicar el número de segundos que el receptor supervisará la cola JMS en busca de documentos. Este campo es opcional.
10. Si lo desea, especifique un valor para **Número de hebras**, para indicar el número de documentos que el Gestor de documentos procesará simultáneamente. Se recomienda utilizar el valor predeterminado 1.

Por ejemplo, si desease configurar un receptor JMS para que coincidiese con el ejemplo de configuración de JMS en el apartado "Configuración del concentrador para el protocolo de transporte JMS" en la página 39, debería hacer lo siguiente:

1. Especifique el valor de **JMSReceiver** en el recuadro **Nombre del receptor**.
2. Introduzca uno de los valores siguientes en el recuadro **URL del proveedor de JMS**:
   - **file:///C:/TEMP/JMS/JMS** en el caso de Windows.
   - **file:///opt/temp** en UNIX.
3. Especifique el valor **inQ** en el recuadro **Nombre de cola JMS**.
4. Especifique el valor **Hub** en el recuadro **Nombre de fábrica JMS**.

Manejadores

Si va a recibir archivos que contienen varios intercambios EDI o documentos XML o ROD que es necesario dividir, configure el manejador de divisor correspondiente en el punto de configuración de preproceso.

Para modificar puntos de configuración para este receptor, vaya al apartado " Modificación de puntos de configuración" en la página 77. De lo contrario, pulse **Guardar**.

Configuración de un receptor del directorio de archivos

Acerca de esta tarea

Un receptor del Directorio de archivos sondea un directorio según un intervalo establecido donde buscar documentos nuevos.

Los pasos siguientes describen qué necesita especificar para un receptor del directorio de archivos.

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** para mostrar la página Lista de receptor.
2. En la página Lista de receptores, pulse **Crear receptor**.

Detalles del receptor

Acerca de esta tarea

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

1. Escriba un nombre para el receptor. Por ejemplo, puede llamar al receptor FileReceiver1. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptor.
2. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está preparado para aceptar documentos. Un receptor que está inhabilitado no puede aceptar documentos.
3. Si lo desea, especifique una descripción del receptor.
4. Seleccione **Directorio de archivos** en la lista **Transporte**.

Configuración del receptor

Acerca de esta tarea

En el apartado **Configuración del receptor** de la página, lleve a cabo los siguientes pasos:

1. Especifique un valor para **Vía de acceso raíz de documento** para indicar dónde se recibirán los documentos.

   Si el directorio raíz no existe, se creará un directorio nuevo para el receptor. Pero, si el directorio raíz ya existe, el receptor utilizará el directorio existente. Esto es sólo aplicable a partir de WebSphere Partner Gateway 6.1.1.

   El prefijo `file://` es opcional.

   Por ejemplo, si desea especificar el directorio `c:\wpg\receivers\file1` como Vía de acceso raíz de documento, especifique `c:\wpg\receivers\file1` o `file://c:\wpg\receivers\file1`.
2. Si lo desea, especifique un valor para **Intervalo de sondeo** para indicar con qué frecuencia debe sondearse el directorio en busca de nuevos documentos. Si no especifica ningún valor, el directorio se sondeará cada 5 segundos.
3. Si lo desea, especifique un valor para **Intervalo no cambiado de archivo** para indicar el número de segundos que debe permanecer sin modificación el tamaño del archivo antes de que el Gestor de documentos recupere el documento para su procesado. Este periodo de intervalo sin modificar

garantiza que un documento haya completado su transmisión (y que no esté aún en tránsito) cuando el Gestor de documentos lo recupera. El valor predeterminado es 3 segundos.

4. Si lo desea, especifique un valor para **Número de hebras**, para indicar el número de documentos que el Gestor de documentos puede procesar simultáneamente. Se recomienda utilizar el valor predeterminado 1.

Manejadores

Si va a recibir archivos que contienen varios intercambios EDI o documentos XML o ROD que es necesario dividir, configure el manejador de divisor correspondiente en el punto de configuración de preproceso.

Para modificar el punto de configuración de preproceso, vaya al apartado " Modificación de puntos de configuración" en la página 77. De lo contrario, pulse **Guardar**.

Configuración de un receptor de FTP Scripting

Acerca de esta tarea

Un receptor de FTP Scripting es un receptor de sondeo que se ejecuta de acuerdo con la planificación que haya establecido. El comportamiento de un receptor de FTP Scripting se controla mediante un script de mandatos FTP.

A diferencia del receptor FTP, que sondea un directorio en el servidor FTP, el receptor de FTP Scripting sondea los directorios en otro servidor (por ejemplo, una VAN).

Nota:

1. Si la base de datos está inactiva y el bloqueo de usuarios está establecido en "Sí", es posible que el receptor de FTP Scripting no funcione ya que no puede obtener el bloqueo de la base de datos.
2. El socio necesita asegurarse de que el documento está completo para que el receptor de FTP Scripting lo reciba. Esto se puede conseguir haciendo que el servidor de FTP mantenga el documento bloqueado hasta que esté completo o haciendo que el socio grabe el documento en un directorio temporal y, a continuación, mueva el documento completado al directorio que utiliza el receptor de FTP Scripting.

Creación de scripts FTP

Acerca de esta tarea

Los servidores FTP pueden tener requisitos específicos para los mandatos que aceptarán. Para utilizar un receptor de FTP Scripting, cree un archivo que incluya todos los mandatos FTP necesarios para el servidor FTP al que se está conectando. (Esta información se debe recibir del administrador del servidor FTP.)

1. Cree un script para los receptores, para indicar las acciones que desea realizar. En el siguiente script se muestra un ejemplo de cómo conectarse al servidor FTP especificado (con el nombre y la contraseña especificados), pasar al directorio especificado en el servidor FTP y recibir todos los archivos que están en ese directorio:

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
cd %BCGOPTION1%
mget *
quit
```

Los indicadores de posición (por ejemplo, %BCGSERVERIP%) son sustituidos cuando el receptor es puesto en funcionamiento por los valores especificados cuando se crea una instancia específica de un receptor de FTP Scripting. %BCGOPTION% en este ejemplo es el nombre del directorio en el mandato `cd`. Los parámetros de script y sus campos de receptor de FTP Scripting asociados aparecen en la Tabla 3:

Tabla 3. Cómo correlacionar los parámetros de script con las entradas de campo del receptor de FTP Scripting

Parámetro de script	**Entrada de campo del receptor de FTP Scripting**
%BCGSERVERIP%	IP de servidor
%BCGUSERID%	ID de usuario
%BCGPASSWORD%	Contraseña
%BCGOPTIONx%	Opción*x*, en **Atributos definidos por el usuario**

2. Guarde el archivo.

Mandatos de FTP Scripting

Al crear el script puede utilizar los siguientes mandatos:

- ascii, binary, passive, epsv

  Estos mandatos no se envían al servidor FTP. Modifican la modalidad de transferencia (ascii, binary o passive) al servidor FTP.

- cd

  Este mandato le lleva al directorio especificado.

- delete

  Este mandato suprime un archivo del servidor FTP.

- get

  Este mandato acepta un solo argumento: el nombre del archivo que se debe recuperar en el sistema remoto. El archivo solicitado se transferirá al sistema WebSphere Partner Gateway. Utilice este mandato sólo si selecciona un único archivo y el nombre es conocido; si no, se debe utilizar el mandato `mget` con caracteres comodín.

- getdel

  Este mandato es el mismo que el mandato `get`, excepto en que el archivo se suprime del sistema remoto cuando WebSphere Partner Gateway obtiene el archivo para procesarlo.

- mget

  Este mandato acepta un solo argumento, que describe un grupo de archivos que deben recuperarse. La descripción puede incluir los caracteres comodín estándar ('*' y '?'). A continuación, se recuperan uno o varios archivos del sistema remoto.

- mgetdel

  Este mandato acepta un solo argumento, que describe un grupo de archivos que deben recuperarse y luego suprimirse del servidor FTP. La descripción puede

incluir los caracteres comodín estándar (* y ?). Se recuperan los archivos y, a continuación, se suprimen del sistema remoto.

- mkdir

  Este mandato crea un directorio en el servidor FTP.

- mputren

  Este mandato es una combinación de los mandatos mput y rename. Por ejemplo, el mandato **mputren * *.tmp /destino/*** copia el archivo del destino al servidor FTP con la extensión **.tmp**. Después de que se complete el proceso de descarga de documentos, el archivo se redenominará y copiará en el directorio **/destino** en el directorio raíz del FTP.

- open

  Este mandato acepta tres parámetros: la dirección IP del servidor FTP, el nombre de usuario y una contraseña. Estos parámetros se correlacionan con las variables %BCGSERVERIP%, %BCGUSERID% y %BCGPASSWORD%.

  Por lo tanto, la primera línea del script del receptor de FTP Scripting debería ser:

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```

- quit

  Este mandato finaliza una conexión existente con un servidor FTP.

- quote

  Este mandato indica que todo lo que siga a QUOTE debe enviarse al sistema remoto como mandato. Esto permite enviar a un servidor FTP remoto mandatos que es posible que no estén definidos en el protocolo FTP estándar.

- rename

  Este mandato cambia el nombre de un archivo en el servidor FTP.

- rmdir

  Este mandato suprime un directorio del servidor FTP.

- site

  Este mandato puede utilizarse para emitir mandatos específicos del sitio al sistema remoto. El sistema remoto determina si el contenido de este mandato es válido.

Detalles del receptor

Acerca de esta tarea

Los siguientes pasos describen qué es necesario especificar para un receptor de FTP Scripting.

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** para mostrar la página Lista de receptor.
2. En la página Lista de receptores, pulse **Crear receptor**.

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

1. Escriba un nombre para el receptor. Por ejemplo, puede llamar al receptor FTPScriptingReceiver1. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptor.
2. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está preparado para aceptar documentos. Un receptor que está inhabilitado no puede aceptar documentos.
3. Si lo desea, especifique una descripción del receptor.
4. Seleccione **FTP Scripting** en la lista Transporte.

Configuración del receptor

Acerca de esta tarea

En el apartado **Configuración del receptor** de la página, lleve a cabo los siguientes pasos:

Procedimiento

1. Si lo desea, indique **Modalidad de funcionamiento**. El tipo de operación define la naturaleza de la transmisión. Por ejemplo, si desea probar un intercambio de documentos antes de ponerlo en producción, especifique **Probar**. El valor predeterminado es **Producción**.
2. Escriba la dirección **IP de servidor** FTP al que se está conectando. El valor aquí especificado sustituirá al valor %BCGSERVERIP% cuando se ejecute el script FTP.
3. Especifique el **ID de usuario** y la **Contraseña** que utilice para acceder al servidor. Los valores aquí especificados sustituirán a %BCGUSERID% y %BCGPASSWORD% cuando se ejecuta el script FTP.
4. Con la **Modalidad FTPS**, seleccione *Sí* o *No* para indicar si el receptor funcionará en modalidad SSL (Secure Sockets Layer). Si responde afirmativamente, necesitará intercambiar certificados con los socios tal como se describe en el apartado Capítulo 13, "Habilitación de la seguridad para intercambios de documentos", en la página 251.
5. Suba el archivo script realizando los siguientes pasos:
   a. Pulse **Subir archivo de script**.
   b. Escriba el nombre del archivo que contiene el script para procesar documentos o utilice **Examinar** para desplazarse hasta el archivo.
   c. Seleccione el **Tipo de codificación del archivo de script**.
   d. Pulse **Cargar archivo** para cargar el archivo de script en el recuadro de texto **Archivo de script cargado actualmente**.
   e. Si el archivo de script es el que desea utilizar, pulse **Guardar**.
   f. Pulse **Cerrar ventana**.
6. En **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico.
7. En el campo **Bloquear usuario**, indique si el receptor solicitará un bloqueo, para que ninguna otra instancia de un receptor de FTP Scripting pueda acceder al mismo directorio FTP al mismo tiempo.

Resultados

Nota: los valores **Atributos globales de FTP Scripting** ya están rellenados y no se pueden editar en esta página. Para modificarlos, utilice la página Atributos de transporte global, como se describe en el apartado " Configuración de valores de transporte global" en la página 62.

Atributos definidos por el usuario

Acerca de esta tarea

Si desea especificar atributos adicionales, realice los pasos siguientes. El valor que especifique para la opción sustituirá al valor %BCGOPTION*x*% cuando se ejecute el script FTP (donde *x* corresponde al número de la opción).

1. Pulse **Nuevo**.

2. Escriba un valor junto a la **Opción 1**.
3. Si va a especificar atributos adicionales, vuelva a pulsar **Nuevo** y escriba un valor.
4. Repita el paso 3 tantas veces como sea necesario para definir todos los atributos.

Por ejemplo, suponga que el script FTP es parecido al siguiente:

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mget *
          quit
```

En este caso %BCGOPTION% sería un nombre de directorio.

Planificación

Indique si desea la planificación basada en intervalos o la planificación basada en agenda.

- Si selecciona **Planificación basada en intervalos**, seleccione el número de segundos que deben transcurrir antes de sondear el servidor FTP (o acepte el valor predeterminado).
- Si selecciona **Planificación basada en calendario**, elija el tipo de planificación (**Planificación diaria**, **Planificación semanal** o **Planificación personalizada**).
  - Si selecciona **Planificación diaria**, especifique la hora del día a la que debe sondearse el servidor FTP.
  - Si elige **Planificación semanal**, seleccione uno o varios días de la semana además de la hora del día.
  - Si elige **Planificación personalizada**, seleccione la hora del día y luego **Rango** o **Días selectivos** para la semana y el mes. Con **Rango**, indique la fecha de inicio y la fecha de finalización. (Por ejemplo, puede pulsar **Lunes** y **Viernes** si desea que el servidor se sondee a una determinada hora únicamente los días laborables). Con **Días selectivos** puede elegir los días concretos de la semana y del mes.

Manejadores

Si va a recibir archivos que contienen varios intercambios EDI o documentos XML o ROD que es necesario dividir, configure el manejador de divisor correspondiente en el punto de configuración de preproceso.

Para modificar el punto de configuración de preproceso, vaya al apartado " Modificación de puntos de configuración" en la página 77. De lo contrario, pulse **Guardar**.

Configuración de un receptor SFTP

Acerca de esta tarea

Esta sección proporciona información detallada para usar SFTP (SSH-FTP) como protocolo para transferir documentos empresariales. Proporciona la confidencialidad, la autenticación y la integridad del mensaje para los datos.

El receptor SFTP sondea el El servidor SFTP recupera archivos del servidor SFTP y los almacena en el directorio local. El directorio que se sondea en el servidor SFTP se denomina directorio de sucesos remoto. El directorio en el que se almacenan los

archivos recuperados se denomina directorio de sucesos local. Los siguientes pasos describen qué es necesario especificar para un receptor SFTP.

Los siguientes pasos describen qué es necesario especificar para un receptor SFTP.

1. Pulse **Administración del concentrador > Configuración del concentrador > Receptores** para mostrar la página Lista de receptores.
2. En la página Lista de receptores, pulse **Crear receptor**.

Creación del receptor SFTP en los sistemas habilitados para seguridad administrativa de WAS

Acerca de esta tarea

WebSphere Partner Gateway V6.2.1 facilita la creación del receptor SFTP en los sistemas habilitados para seguridad administrativa de WAS. Este tema detalla una tarea para crear un receptor SFTP en un sistema habilitado para seguridad administrativa de WAS:

1. En la consola WebSphere Partner Gateway, vaya a **Administración del sistema** > **Administración de la consola** > **Seguridad administrativa de WAS**.
2. En esta pantalla, establezca el valor del atributo **bcg.RMIConnector.security.enabled** a true. Observe que el valor de este atributo es "false" por defecto.
3. Establezca los demás atributos de la pantalla como ilustrados en el siguiente procedimiento:
   a. **bcg.RMIConnector.security.enabled**: Establezca este atributo a "true" sólo si tiene habilitada la opción **Seguridad administrativa de WAS** . Si no establece esta propiedad a "true", no podrá crear el receptor SFTP.
   b. **bcg.RMIConnector.security.enabled**: Si este atributo está establecido en "true", es obligatorio establecer los siguientes atributos:
      - **bcg.RMIConnector.host.name**: Entre el nombre de host o dirección IP del gestor de despliegue.
      - **bcg.RMIConnector.portNumber**: Proporcione el BOOTSTRAP PORT del gestor de despliegue.
      - **bcg.RMIConnector.admin.userId**: Establezca este atributo para el ID de usuario que se utiliza para la seguridad administrativa de WAS.
      - **bcg.RMIConnector.admin.password**: Establezca este atributo para la contraseña que se utiliza para la seguridad administrativa de WAS.
4. Pulse **Guardar**.

Detalles del receptor

Acerca de esta tarea

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

Procedimiento

1. Escriba un nombre para el receptor. Por ejemplo, puede llamar al receptor SFTPReceiver1. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptores.
2. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está preparado para aceptar documentos. Un receptor que está inhabilitado no puede aceptar documentos.
3. Si lo desea, especifique una descripción del receptor.

4. Seleccione **SFTP** en la lista **Transporte**.

Configuración del receptor

Acerca de esta tarea

En el apartado **Detalles del receptor**, lleve a cabo los siguientes pasos:

Procedimiento

1. Entre en **Modalidad de operación**. Seleccione un elemento de la lista desplegable o pulse **Nuevo** para crear una modalidad.
2. En el campo **SFTP Host IP**, especifique el nombre de host del servidor SFTP. Se aceptarán un máximo de 100 caracteres. También puede introducir direcciones de IP, IPv4 y direcciones IPv6.
3. Introduzca el valor del **Número de puerto**.El valor predeterminado es 22.
4. El **Directorio de sucesos remotos** es el directorio desde el que el adaptador descarga archivos de suceso desde el sitio STFP.
5. En **Tipo de autenticación**, seleccione el **Nombre de usuario / Contraseña** o la autenticación de **Clave privada**.
6. Especifique el **Id de usuario** y la **Contraseña** del nombre de usuario/contraseña. Si el tipo de autenticación corresponde a una autenticación de clave privada, especifique el nombre de usuario, el archivo de clave privada y la frase de paso. El archivo de clave privada debe utilizar el formato OpenSSH.
7. En **Intervalo de sondeo SFTP**, especifique el cantidad de tiempo en milisegundos. Se trata de la cantidad de tiempo que el adaptador espera mientras sondea el directorio de sucesos locales. Esta cantidad de tiempo y la cantidad de tiempo para procesar los documentos en el directorio de sucesos local se denomina ciclo de sondeo.
8. **Cantidad de sondeos** es el número de sucesos (documentos) que el receptor procesa durante cada ciclo de sondeo.
9. **Intervalo de reintentos** es la cantidad de tiempo en milisegundos que el adaptador espera entre intentos para establecer una conexión nueva después de un error durante las operaciones entrantes.
10. **Límite de reintentos** es el número de veces que el adaptador intenta restablecer una conexión entrante después de un error.
11. **Codificación EIS** es la codificación del servidor FTP. Utilice este valor para establecer la codificación de la conexión de control al servidor FTP.
12. Se puede **Habilitar autenticación de servidor** para autenticar el servidor con el que se está estableciendo la conexión. Si se ha habilitado la autenticación de servidor, especifique la vía de acceso del archivo de claves de host. El archivo de claves de host debe utilizar el formato OpenSSH.
13. Si es necesario, configure los manejadores.
14. Pulse **Guardar** para guardar la configuración.

Manejadores

Si va a recibir archivos que contienen varios intercambios EDI o documentos XML o ROD que es necesario dividir, configure el manejador de divisor correspondiente en el punto de configuración de preproceso.

Para modificar el punto de configuración de preproceso, vaya al apartado " Modificación de puntos de configuración". De lo contrario, pulse **Guardar**.

Configuración de un receptor para un transporte definido por el usuario

Acerca de esta tarea

Si está definiendo un receptor para un transporte definido por el usuario, los nombres de campo así como otras informaciones se definen dentro del archivo que describe el transporte.

Realice los siguientes pasos

1. Pulse **Administración del concentrador > Configuración del concentrador > Receptor**.
2. Pulse **Gestionar tipos de transporte**.
3. Especifique el nombre de un archivo XML que defina el transporte (o utilice **Examinar** para ir hasta el archivo).
4. Pulse **Subir**.

   Nota: desde la lista Receptores, puede también es posible borrar un tipo de transporte definido por el usuario. No es posible borrar un transporte proporcionado por WebSphere Partner Gateway. Además, no puede suprimir un transporte definido por el usuario después de haber sido utilizado para crear un receptor.
5. Pulse **Crear destinatario**.
6. Escriba un nombre para el receptor. Se trata de un campo obligatorio. El nombre que especifique aquí aparecerá en la lista Receptor.
7. Si lo desea, indique el estado del receptor. **Habilitado** es el valor predeterminado. Un receptor que está habilitado está preparado para aceptar documentos. Un receptor que está inhabilitado no puede aceptar documentos.
8. Si lo desea, especifique una descripción del receptor.
9. Seleccione el transporte definido por el usuario en la lista.
10. Rellene los campos (que serán exclusivos para cada transporte definido por el usuario).
11. Si desea modificar puntos de configuración para este receptor, vaya al apartado " Modificación de puntos de configuración". De lo contrario, pulse **Guardar**.

Modificación de puntos de configuración

El número de puntos de configuración disponibles y el número de manejadores asociados para dichos puntos de configuración varían dependiendo del tipo de receptor que esté configurando. Por ejemplo, el punto de configuración de comprobación síncrona sólo está disponible con receptores HTTP/S y JMS.

Para determinados protocolos empresariales (RosettaNet, cXML, SOAP y AS2) implicados en intercambios síncronos, debe especificar un manejador para dicho protocolo en el punto de comprobación síncrona. También puede modificar la manera en que los receptores procesan documentos aplicando un manejador definido por el usuario que se haya subido (o un proceso proporcionado por el producto) a los puntos de preproceso y postproceso del receptor.

Para aplicar un manejador escrito por el usuario a estos puntos de configuración, deberá primero subir el manejador, tal como se describe en el apartado " Subida de manejadores definidos por el usuario" en la página 60. Puede también utilizar un manejador proporcionado por el producto, que ya está disponible y que no es necesario subir.

Preproceso

El manejador de configuración de preproceso está disponible en todos los tipos de destino, pero es aplicable a receptores SMTP.

Atributos de preproceso

En la Tabla 4 se describen los atributos que se pueden establecer para un manejador de preproceso y lista los manejadores de divisor al que se aplican los atributos.

Los atributos de ROD utilizados como ejemplos en esta tabla corresponden a los utilizados en el apartado " Ejemplo de ROD a EDI" en la página 368. En el ejemplo, los atributos de ROD están contenidos en la correlación S_DT_ROD_TO_EDI.eif, que incluye la siguiente definición de documento:

- Paquete: Ninguno (versión N/D)
- Protocolo: ROD_TO_EDI_DICT (versión ALL)
- Tipo de documento: DTROD-TO-EDI_ROD (versión ALL)

El metadiccionario y el metadocumento ROD asociados a este flujo son ROD_TO_EDI_DICT y DTROD-TO-EDI_ROD.

Tabla 4. Atributos del manejador de divisor

Atributo	Descripción	Manejador de divisor
Codificación	Codificación de caracteres del documento. El valor predeterminado es ASCII.	ROD Genérico XML EDI
BATCHDOCS	Cuando BCG_BATCHDOCS está activo, el divisor añade varios ID de lote a los documentos después de dividirlos. Si los documentos se transforman en transacciones EDI que se deben ensobrar, el ensobrador utiliza los ID de lote para asegurarse de que las transacciones se ponen en el mismo intercambio EDI (si es posible) antes de entregarse. Tenga en cuenta que el ensobrador debe tener el atributo de proceso por lotes establecido en **Activado** (el valor predeterminado). Consulte el apartado "Modalidad de proceso por lotes" en la página 192.	ROD Genérico XML
Nombre De empaquetado	El paquete asociado al documento. Este valor debe coincidir con el paquete especificado en la definición del documento. Por ejemplo, para un documento con un paquete Ninguno, este valor debe ser **Ninguno**.	ROD Genérico
Versión De empaquetado	Versión del paquete especificado en Nombre De empaquetado. Por ejemplo, si el documento tiene el paquete Ninguno, este valor sería **N/D**.	ROD Genérico
Nombre De protocolo	El protocolo asociado al documento. Este valor debe coincidir con el protocolo especificado en la definición del documento. Por ejemplo, para un documento ROD, este valor podría ser **ROD-TO-EDI_DICT**.	ROD Genérico

Tabla 4. Atributos del manejador de divisor (continuación)

Atributo	Descripción	Manejador de divisor
Versión De protocolo	La versión del protocolo que se ha especificado en Nombre De protocolo. Por ejemplo, para el protocolo ROD-TO-EDI_DICT, el valor sería **ALL**.	ROD Genérico
Código De proceso	El proceso (tipo de documento) asociado a este documento. Este valor debe coincidir con el tipo de documento en la definición del documento. Por ejemplo, para un documento ROD, este valor podría ser DTROD-TO-EDI_ROD.	ROD Genérico
Versión De proceso	Versión del proceso especificado en Código De proceso. Por ejemplo, para DTROD-TO-EDI_ROD, este valor sería **ALL**.	ROD Genérico
Metadiccionario	El metadiccionario proporciona información que permite a WebSphere Partner Gateway interpretar los datos. Por ejemplo, para un documento ROD, este valor podría ser **ROD-TO-EDI_DICT**.	ROD Genérico
Metadocumento	El metadocumento proporciona información que permite a WebSphere Partner Gateway interpretar los datos. Por ejemplo, para un documento ROD, este valor podría ser **DTROD-TO-EDI_ROD**.	ROD Genérico
Metasintaxis	La metasintaxis describe el formato del documento que se divide. El valor predeterminado es **ROD**.	ROD Genérico
SenderId	El ID del socio de envío.	Genérico
ReceiverId	El ID del socio receptor.	Genérico

Notas:

1. Sólo se da soporte a un tipo de documento ROD por instancia de receptor.
2. Si un receptor tiene más de un manejador de divisor configurado (por ejemplo, si tiene manejadores de divisores ROD, XML y EDI configurados), el divisor ROD debe ser el último en la **Lista configurada**.

Modificación del punto de configuración de preproceso

Acerca de esta tarea

Para modificar el punto de configuración de preproceso, realice los siguientes pasos:

1. Seleccione **preproceso** en la lista **Manejadores de puntos de configuración**.

   De forma predeterminada se proporcionan cinco manejadores de preproceso, que se muestran en la **Lista disponible**.

   - com.ibm.bcg.edi.receiver.preprocesshandler.EDISplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler
   - com.ibm.bcg.edi.receiver.preprocesshandler.GenericDocumentFlowHandler
   - com.ibm.bcg.server.receiver.preprocesshandler.FileNamePartnerId

   Nota: los manejadores de preproceso no se aplican a receptores de SMTP.
2. Si va a recibir varios intercambios EDI, o documentos XML o ROD que es necesario dividir, asegúrese de seleccionar el manejador de divisor adecuado. Para configurar el paso de preproceso:

a. Seleccione un manejador en la **Lista disponible** y pulse **Añadir**. Tenga en cuenta que el manejador pasa de la **Lista disponible** a la **Lista configurada**, como se muestra en la Figura 17:

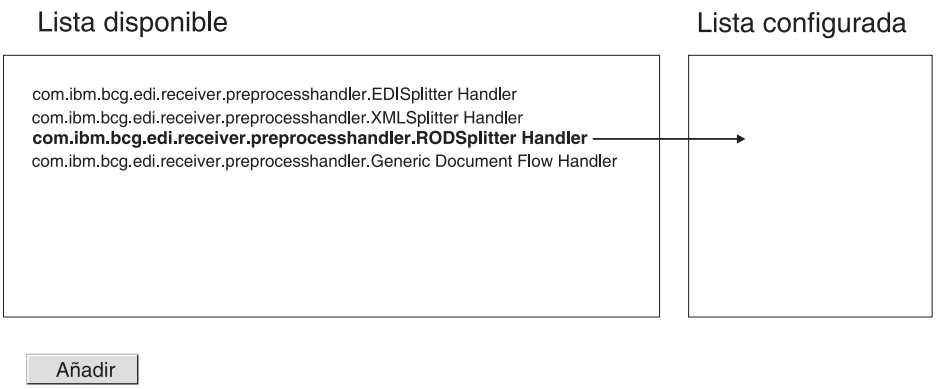


Figura 17. Configuración del paso de preproceso para un receptor

b. Repita este paso para cada manejador que desea añadir a la lista configurada.

   Recuerde que para los receptores, los manejadores se invocan en el orden en el que aparecen en la **Lista configurada**. El primer manejador correspondiente procesa la solicitud y no se invocan los siguientes manejadores en la lista.

c. Configure el manejador seleccionándolo y pulsando **Configurar**:
   - Si ha añadido EDISplitterHandler, puede modificar su atributo Codificación. El valor predeterminado es ASCII.
   - Si ha añadido XMLSplitterHandler, puede modificar su atributo BCGBATCHDOCs. El valor predeterminado es **Activado**. Consulte el apartado "Atributos de preproceso" en la página 78 para obtener información sobre este atributo.
   - Si ha añadido RODSplitterHandler, puede especificar valores para 11 atributos. Codificación, BATCHDOCS y Metasintaxis tiene valores predeterminados. Para los demás atributos, debe escribir un valor para Nombre De empaquetado, Versión De empaquetado, Nombre De protocolo, Versión De protocolo, Código De Proceso, Versión De Proceso, Metadiccionario y Metadocumento. Consulte el apartado "Atributos de preproceso" en la página 78 para obtener información sobre estos atributos.
   - Si ha añadido GenericDocumentFlowHandler, puede especificar valores para 13 atributos. Codificación y BATCHDOCS tienen valores predeterminados. Los atributos SenderId y ReceiverId están configurados previamente para GenericDocumentFlowHandler sin ningún valor predeterminado. Para los demás atributos, debe escribir un valor para Nombre De empaquetado, Versión De empaquetado, Nombre De protocolo, Versión De protocolo, Código De Proceso, Versión De Proceso, Metadiccionario, Metadocumento y Metasintaxis. Consulte el apartado "Atributos de preproceso" en la página 78 para obtener información sobre estos atributos.
   - Si ha añadido FileNamePartnerId, no esperará ningún parámetro de configuración. Esperará que el archivo recibido siga este convenio de denominación:

     ```
     <cualquiercadena>bcgrcv<ID de receptor>bcgsdr<ID de remitente>bcgend<cualquiercadena>
     ```

donde

ID de receptor ,ID de remitente
: Son los ID de empresa de los socios tal y como están configurados en sus perfiles.

bcgrcv, bcgsdr
: Son constantes de cadenas que señalan el comienzo de los ID del receptor y del remitente.

bcgend
: Es una constante de cadena que determina el final de una cadena de convenio de denominación requerida

anystring
: es cualquier carácter alfanumérico elegido por el usuario

Este manejador sólo puede ser configurado para receptores de FTP Scripting o de directorio de archivos. Para recibir archivos binarios a través de FTP Scripting o de directorio de archivos, puede configurar este manejador para el receptor.

Comprobación síncrona

Acerca de esta tarea

El punto de configuración de comprobación síncrona sólo está disponible para receptores HTTP/S y JMS.

Para especificar un manejador para un protocolo empresarial incluido en un intercambio síncrono, realice los siguientes pasos:

1. Seleccione **Comprobación síncrona** en la lista **Manejadores de puntos de configuración**.

   Se proporcionan seis manejadores de comprobación síncrona (valor predeterminado) para un receptor HTTP/S. Estos manejadores se muestran en la **Lista disponible**:

   - com.ibm.bcg.server.sync.As2SyncHdlr
   - com.ibm.bcg.server.sync.CxmlSyncHdlr
   - com.ibm.bcg.server.sync.RnifSyncHdlr
   - com.ibm.bcg.server.sync.SoapSyncHdlr
   - com.ibm.bcg.server.sync.DefaultAsynchronousSyncCheckHandler
   - com.ibm.bcg.server.sync.DefaultSynchronousSyncCheckHandler
   - com.ibm.bcg.server.sync.EBMSSyncCheckHandler

   Por ejemplo, si está configurando un receptor HTTP/S, la Lista disponible se parecerá a la siguiente:

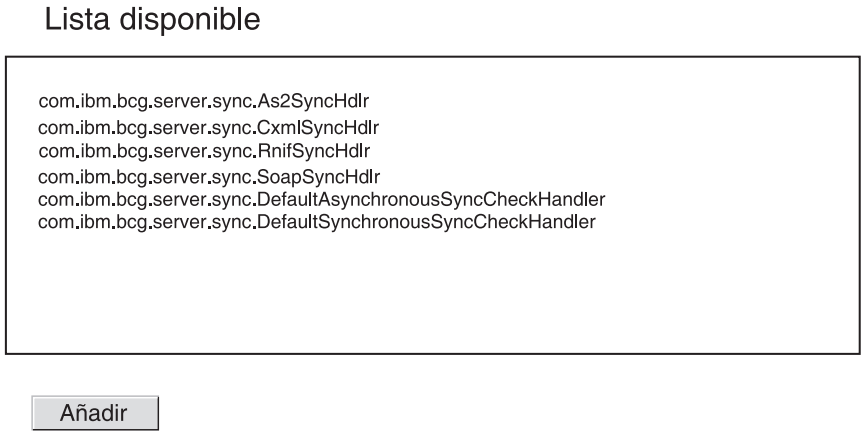


Figura 18. Lista de manejadores disponibles para un punto de configuración de comprobación síncrona HTTP/S

Tal como puede verse en el convenio de denominación, los primeros cuatro manejadores son específicos de los cuatro tipos de documentos que pueden utilizarse para transacciones síncronas. Cualquier solicitud que utilice DefaultAsynchronousSyncCheckHandler se considerará una solicitud asíncrona. Cualquier solicitud que utilice DefaultSynchronousSyncCheckHandler se considerará una solicitud síncrona.

Puede utilizar DefaultAsynchronousSyncCheckHandler y DefaultSynchronousSyncCheckHandler con otros receptores (como con un receptor JMS).

2. Si va a recibir documentos síncronos en este receptor, lleve a cabo los siguientes pasos:
   a. Seleccione uno o varios manejadores en la **Lista disponible** y pulse **Añadir**.
   b. Repita este paso para añadir otros manejadores a la lista. Recuerde que para los receptores, los manejadores se invocan en el orden en el que aparecen en la **Lista configurada**. El primer manejador disponible procesa la solicitud y los siguientes manejadores de la lista no se invocan.

   En receptores HTTP y HTTPS, es recomendable listar el manejador de comprobación síncrona específico (por ejemplo, com.ibm.bcg.server.sync.As2SyncHdlr para las transacciones AS2) antes de listar los manejadores de comprobación síncrona predeterminada.

Postproceso

Acerca de esta tarea

No se proporciona ningún manejador predeterminado para el paso de postproceso y, por lo tanto, no se lista ningún manejador predeterminado en la **Lista disponible**. Puede, no obstante, subir un manejador para este punto de configuración para todos los tipos de receptores que den soporte a la comunicación síncrona. Los tipos de manejadores disponibles para el paso de postproceso son:

- RECEIVER.SYNCRESPONSEPROCESS.JMS
- RECEIVER.SYNCRESPONSEPROCESS.HttpS

Añada un manejador de postproceso subiendo un manejador que se ajuste a uno de estos tipos de manejador. Utilice la opción **Importar** de la página Lista de manejadores para subir un manejador definido por el usuario. Cuando se sube un

manejador de receptor definido por el usuario, se añadirá el manejador a la lista de manejadores. También aparece en la Lista disponible para el tipo de punto de configuración al que pertenece.

Para modificar el punto de configuración de postproceso, realice los pasos siguientes:

1. Seleccione **Postproceso** en la lista **Manejadores de puntos de configuración**.
2. Seleccione un manejador definido por el usuario en la **Lista disponible** y pulse **Añadir**. Tenga en cuenta que el manejador pasa de la **Lista disponible** a la **Lista configurada**.

Modificación de la lista configurada

Acerca de esta tarea

Si necesita cambiar el orden de los manejadores, suprimir un manejador o configurar atributos para el manejador, realice el paso adecuado:

- Elimine un manejador seleccionándolo en la **Lista configurada** y pulsando **Eliminar**. El manejador pasa a la **Lista disponible**.
- Cambie el orden en el que se utiliza el manejador seleccionando el manejador y pulsando **Mover arriba** o **Mover abajo**.
- Configure el manejador seleccionándolo en la **Lista configurada** y pulsando **Configurar**. Aparecerá la lista de los atributos que pueden configurarse.

Capítulo 8. Configuración de pasos de flujos de trabajo fijos y acciones

En este capítulo se describen las tareas opcionales que puede realizar para configurar acciones y flujos de trabajo entrantes y salientes fijos. Si no necesita cambiar el comportamiento proporcionado por el producto de los flujos de trabajo o acciones, ignore este capítulo.

Este capítulo incluye los siguientes temas:

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado la sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Subida de manejadores

Acerca de esta tarea

Si desea modificar algunos componentes, antes de crear o configurar dichos componentes deberá subir los manejadores de dichos componentes. Sólo deberá subir los manejadores definidos por el usuario para los componentes que los necesiten. Por ejemplo, si añade su propio paso de validación, deberá subir dicho manejador de la página Acciones de **Manejadores** (como se describe en los pasos 1 a 4 en la página 86).

Nota: tal como se menciona en el apartado "Configuración de componentes de proceso de documentos con manejadores" en la página 14, sólo se subirán los manejadores definidos por el usuario. Los manejadores proporcionados por WebSphere Partner Gateway ya están disponibles.

Puede modificar acciones y flujos de trabajo fijos y crear nuevas acciones. Estos componentes se modifican mediante los manejadores que se les asocian.

Nota: puede listar los tipos de manejadores válidos para acciones y flujos de trabajo fijos pulsando **Administrador de concentrador > Configuración del concentrador > Manejadores > Acción > Tipos de manejadores** o **Administración del concentrador > Configuración del concentrador > Manejadores > Flujo de trabajo fijo > Tipos de manejadores**. Utilice esta lista para confirmar que el tipo de su manejador es válido antes de subirlo. Debe presentar uno de los tipos permitidos; de lo contrario, no podrá subirlo satisfactoriamente.

Para subir un manejador, lleve a cabo los siguientes pasos:

1. En el menú principal, pulse **Administración del concentrador > Configuración del concentrador > Manejadores**.
2. Seleccione el tipo de manejador (**Acción** o **Flujo de trabajo fijo**).

Aparece la lista de manejadores definida actualmente para ese componente determinado. Observe que los manejadores suministrados por WebSphere Partner Gateway aparecen en la lista. Su ID de proveedor es **Producto**.

3. En la página Lista de manejadores, pulse **Importar**.
4. En la página Importar manejador, especifique la vía de acceso al archivo XML que describe el manejador o utilice **Examinar** para buscar dicho archivo XML.
5. Pulse **Subir**.

Una vez que se ha subido un manejador, puede utilizarlo para crear nuevas acciones y nuevos flujos de trabajo.

Nota: puede actualizar los manejadores definidos por el usuario subiendo el archivo XML modificado. Por ejemplo, para un manejador de acción debería pulsar **Administración del concentrador > Configuración del concentrador > Manejadores > Acción** e **Importar**.

No es posible modificar o borrar los manejadores facilitados por WebSphere Partner Gateway.

Configuración de flujos de trabajo fijos

Acerca de esta tarea

En el Capítulo 2, "Introducción a la configuración del concentrador", en la página 5 se describen los dos pasos de flujos de trabajo entrantes fijos que puede configurar, uno para desempaquetar un protocolo y otro para analizar el protocolo. Para los flujos de trabajo salientes, hay un solo paso, para empaquetar el protocolo.

Si se dispone a utilizar un manejador definido por el usuario para configurar un flujo de trabajo, suba el manejador tal como se describe en el apartado " Subida de manejadores" en la página 85.

Para configurar un flujo de trabajo fijo, realice los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Flujo de trabajo fijo**.
2. Pulse **Entrante** o bien **Saliente**.
3. Pulse el icono **Ver detalles** situado junto al nombre del paso que desea configurar.

   Aparece un listado con el paso, junto con una lista de manejadores ya configurados para dicho paso. Consulte los apartados "Flujos de trabajo entrantes" en la página 87 y "Flujo de trabajo saliente" en la página 87 para obtener una lista de manejadores predeterminados.
4. Pulse el icono **Editar** para editar la lista de manejadores.
5. Realice una de las siguientes tareas para cada paso que desee modificar.
   a. Añada un manejador seleccionándolo en la **Lista disponible** y pulsando **Añadir**. (Un manejador aparece en la **Lista disponible** si ha subido un manejador definido por el usuario o si anteriormente se ha eliminado un manejador de la **Lista configurada**). El manejador pasa a la **Lista configurada**.
   b. Elimine un manejador seleccionándolo en la **Lista configurada** y pulsando **Eliminar**. El manejador pasa a la **Lista disponible**.
   c. Cambie el orden en el que se invocan los manejadores seleccionando el manejador y pulsando **Mover arriba** o **Mover abajo**.

Los manejadores se invocan en el orden en el que aparecen en la **Lista configurada**. El primer manejador disponible que puede procesar la solicitud es el que se encarga de ella. Si tiene previsto recibir una gran cantidad de documentos de un determinado tipo (por ejemplo, documentos ROD), puede mover el manejador asociado con dicho tipo de documento (en este ejemplo, com.ibm.bcg.edi.business.process.RODScannerHandler) al principio de la lista.

6. Pulse **Guardar**.

Flujos de trabajo entrantes

En este apartado se muestran los manejadores configurados para los flujos de trabajo entrantes.

Manejadores de desempaquetado de protocolos

De forma predeterminada, el paso de desempaquetado de protocolo tiene los siguientes manejadores configurados:

- com.ibm.bcg.ediint.ASUnpackagingHandler
- com.ibm.bcg.server.pkg.NullUnpackagingHandler
- com.ibm.bcg.server.pkg.MIMEMultipartUnpackagingHandler
- com.ibm.bcg.eai.EAIUnpackagingHandler

Manejadores de proceso de protocolos

De forma predeterminada, el paso de proceso de protocolo tiene los siguientes manejadores configurados:

- com.ibm.bcg.server.RNOChannelParseHandler
- com.ibm.bcg.server.RNSignalChannelParseHandler
- com.ibm.bcg.server.RNSCChannelParseHandler
- com.ibm.bcg.server.BinaryChannelParseHandler
- com.ibm.bcg.cxml.cXMLChannelParseHandler
- com.ibm.bcg.soap.SOAPChannelParseHandler
- com.ibm.bcg.server.XMLRouterBizProcessHandler
- com.ibm.bcg.edi.EDIRouterBizProcessHandler
- com.ibm.bcg.edi.business.process.RODScannerHandler
- com.ibm.bcg.edi.business.process.NetworkAckHandler
- com.ibm.bcg.server.EBMSProtocolParseHandler
- com.ibm.bcg.server.BackendChannelParseHandler

El atributo "Content-Types" está asociado con BinaryChannelParseHandler, XMLRouterBizHandler, EDIRouterBizProcessHandler y cXMLChannelParseHandler. Estos manejadores se pre-rellenan con la lista predeterminada de tipos de contenido. Si el documento recibido tiene una cabecera de tipo de contenido que está configurado para cualquiera de los manejadores anteriormente mencionados, se aplicará dicho manejador.

Flujo de trabajo saliente

De forma predeterminada, el paso de empaquetado de protocolo tiene los siguientes manejadores configurados:

- com.ibm.bcg.server.pkg.NullPackagingHandler
- com.ibm.bcg.ediint.ASPackagingHandler
- com.ibm.bcg.edi.server.EDITransactionHandler

- com.ibm.bcg.rosettanet.pkg.RNOPPackagingHandler
- com.ibm.bcg.server.pkg.RNPassThruPackagingHandler
- com.ibm.bcg.cxml.cXMLPackagingHandler
- com.ibm.bcg.soap.SOAPPackagingHandler
- com.ibm.bcg.eai.EAIPackagingHandler

Configuración de acciones

En el apartado Capítulo 2, “Introducción a la configuración del concentrador”, en la página 5 se indica que las acciones pueden estar formadas por uno o más pasos. WebSphere Partner Gateway proporciona varias acciones predeterminadas. Puede añadir elementos a la lista de acciones subiendo uno o varios manejadores de acción (pasos de la acción), que posteriormente podrán utilizarse en una acción. También pueden crearse acciones nuevas, tal como se describe en el apartado “Creación de acciones” en la página 105.

Nota: no es posible modificar las acciones que facilita WebSphere Partner Gateway, aunque sí puede copiar una de ellas y modificarla, tal como se describe en el apartado “Copiar una acción” en la página 106.

Si se dispone a utilizar un manejador definido por el usuario para configurar una acción, suba el manejador, tal como se describe en el apartado “ Subida de manejadores” en la página 85.

Acciones proporcionadas con el producto

Este apartado proporciona detalles sobre las acciones proporcionadas con el producto de Websphere Partner Gateway referentes a su propósito y cualquier configuración necesaria para utilizarlas. El apartado Capítulo 9, “Configuración de tipos de documento”, en la página 107 proporciona más detalles acerca de cuándo utilizar algunas de estas acciones.

Algunas acciones tienen la palabra Bidireccional en su nombre. Aquí *Bidireccional* quiere decir que los formatos de origen o destino pueden cambiarse y que puede seguir utilizándose la acción. Por ejemplo, para la acción “Conversión bidireccional RosettaNet y XML con validación”, el documento de origen puede ser de RosettaNet y el documento de destino XML, o el documento de origen puede ser XML y el documento de destino RosettaNet.

Las siguientes son las distintas acciones proporcionadas con Websphere Partner Gateway:

- “Paso a través” en la página 89
- “Cancelación del socio interno de proceso de RosettaNet” en la página 90
- “Paso a través de RosettaNet con registro cronológico de procesos” en la página 90
- “Traducción bidireccional de RosettaNet y Contenido de servicio de Rosettanet con validación” en la página 91
- “Traducción bidireccional de RosettaNet y Contenido de servicio de Rosettanet sin validación de contenido” en la página 93
- “Traducción bidireccional de XML personalizado de socio interno a RosettaNet con comprobación duplicada y validación de contenido” en la página 93
- “Traducción bidireccional de RosettaNet y XML con validación” en la página 92
- “Traducción bidireccional de XML personalizado con validación” en la página 94

Paso a través

Esta acción se utiliza cuando no es necesario realizar ningún proceso especial, como la validación o la transformación, en el documento. El documento origen se envía a la ubicación de destino tal cual.

Configuración

No necesita ninguna.

Modificación

Esta acción pude ser copiada en una nueva acción. Es posible añadir nuevos pasos antes de los pasos anteriores. Por ejemplo, un paso de validación personalizado que valide el documento de origen u otro tipo de proceso personalizado.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.passthrough.No_op** - utilizado para indicar que el tipo de contenido del documento de destino no debe derivar del contenido del documento.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Cancelación del socio interno de proceso de RosettaNet

Propósito

Esta acción está dirigida a la cancelación de un proceso RosettaNet RNIF por parte del socio interno (programa de fondo). Cuando la aplicación de fondo (socio interno) envía un documento de suceso XML con el código de suceso 800/801, se creará, en este paso, un documento 0A1 para enviarlo al socio externo y se cancelará el correspondiente proceso PIP.

Configuración

El proceso RNIF que está siendo cancelado debe haber sido ya configurado en WebSphere Partner Gateway y WebSphere Partner Gateway debe haber recibido ya el documento RosettaNet que ha iniciado el proceso que está siendo cancelado.

Modificación

Esta acción no puede ser modificada o copiada ya que esta acción es específica de la cancelación del proceso PIP de RosettaNet.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la clase de desempaquetado correcta para RNIF o asume que el documento no es RNIF y no se lleva a cabo ningún empaquetado.
2. **com.ibm.bcg.validation.ValidationFactory** - valida el documento RN de origen para el contenido de servicio RNIF correcto.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Paso a través de RosettaNet con registro cronológico de procesos

Esta acción se utiliza cuando el documento RNIF de origen de RosettaNet se pasa a través de WebSphere Partner Gateway. Utilice este paso cuando el contenido de servicio de documento RNIF no se extrae o transforma. Incluso aunque este es un paso a través aún se realiza el proceso RNIF con los acuses de recibo generados.

Configuración

No requiere ninguna

Modificación

Esta acción puede ser copiada o modificada. Es posible añadir nuevos pasos antes de los pasos existentes para añadir procesos adicionales personalizados.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.rosettanet.passthru.ProcessLoggingFactory** - este paso establece los metadatos del documento RosettaNet en el objeto de documento de empresa (BDO).
2. **com.ibm.bcg.passthrough.No_op** - utilizado para indicar que el tipo de contenido del documento de destino no debe derivar del contenido del documento.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Traducción bidireccional de RosettaNet y Contenido de servicio de Rosettanet con validación

Esta acción se utiliza para documentos RNIF RosettaNet. Cuando se recibe un documento RNIF del socio externo, la carga (RNSC - contenido de servicio RosettaNet) será extraída del documento empaquetado RNIF para enviarla a la aplicación de fondo (socio interno). Se producirá la validación en el documento RNIF incluyendo el RNSC. Cuando proceda de la aplicación de fondo (socio interno), el documento RNSC se validará.

Configuración

Es necesario haber cargado el paquete PIP de RosettaNet para el documento RosettaNet.

Modificación

Esta acción no puede ser copiada ni modificada.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la clase de desempaquetado correcta para RNIF o asume que el documento no es RNIF y no se lleva a cabo ningún empaquetado.
2. **com.ibm.bcg.validation.ValidationFactory** - realiza una validación y utiliza los siguientes BusinessProcesses para validar documentos RNIF 1.1, RNIF 2.0 y RNSC. - RNSignal0A1Validation (validación de señales RNIF generadas por WebSphere Partner Gateway o de mensajes 0A1) - ValidationNoOp (esto únicamente devuelve el BusinessDocument sin llevar a cabo ningún proceso, se llamaría cuando WBIC vuelve a intentar las señales RNIF o mensajes 0A1) - RN11Validation (esto es para validar el mensaje RNIF 1.1) - RN20Validation (esto es para validar el mensaje RNIF 2.0) - RNSCValidation (esto es para validar el suceso XML u el mensaje RNSC).
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - utilizado para extraer el RNSC del documento RNIF o para crear la información de RNIF para el RNSC.

4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - utilizado para procesar documentos 0A1 de RosettaNet para actualizar el motor de estado de RosettaNet.
5. **com.ibm.bcg.outbound.OutboundDocFactor**y - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Traducción bidireccional de RosettaNet y XML con validación

Esta acción se utiliza para los documentos RNIF de RosettaNet que necesitan ser transformados en un documento XML personalizado o viceversa. Cuando se recibe un documento RNIF del socio externo, la carga (RNSC - contenido de servicio RNIF) será extraída del paquete RNIF, validada y transformada en un documento XML con los documentos de destino transformados validados para enviarlos a la aplicación de fondo (Socio interno). Cuando proceda de la aplicación de fondo (socio interno) se validará el XML, transformado en el RNSC que se valida.

Configuración

- Es necesario haber cargado el paquete PIP de RosettaNet para el documento RosettaNet.
- Requiere que el mapa de correlación (XML SCHEMA) se configure en el documento XML de origen o de destino
- Es necesario configurar una correlación de transformación XSLT para esta acción

Modificación

Esta acción no puede ser copiada ni modificada.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la clase de desempaquetado correcta para RNIF o asume que el documento no es RNIF y no se lleva a cabo ningún empaquetado.
2. **com.ibm.bcg.validation.ValidationFactory** – para validar el RNIF de origen o documento XML.
3. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – transforma el RNSC en / a partir del XML.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - valida el documento XML transformado resultante.
5. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - utilizado para procesar documentos 0A1 de RosettaNet para actualizar el motor de estado de RosettaNet.
6. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Traducción bidireccional de RosettaNet y Contenido de servicio de Rosettanet sin validación de contenido

Esta acción se utiliza para documentos RosettaNet (RNIF). Cuando se recibe un documento RNIF de un socio externo, se extrae la carga (RNSC - RNIF Service Content) del empaquetado RNIF. La carga extraída se valida y transforma en un documento XML antes de enviarla a la aplicación de fondo (socio interno). Cuando la aplicación de fondo (socio interno) recibe un documento XML, se llevan a cabo los siguientes pasos en dicha aplicación:

1. Comprobación de identificadores duplicados
2. Validación
3. Transformación en RNSC
4. Validación de RNSC

Configuración

Es necesario haber cargado el paquete PIP de RosettaNet para el documento RosettaNet.

Modificación

Esta acción no puede ser copiada ni modificada.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la clase de desempaquetado correcta para RNIF o asume que el documento no es RNIF y no se lleva a cabo ningún empaquetado.
2. **com.ibm.bcg.validation.ValidationWithoutContentFactory** – realizará una validación menos en el RNSC.
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - utilizado para extraer el RNSC del documento RNIF o para crear la información de RNIF para el RNSC.
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - utilizado para procesar documentos 0A1 de RosettaNet para actualizar el motor de estado de RosettaNet.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Traducción bidireccional de XML personalizado de socio interno a RosettaNet con comprobación duplicada y validación de contenido

Esta acción se utiliza para los documentos RNIF de RosettaNet que necesitan ser transformados en un documento XML personalizado o viceversa. Cuando se recibe un documento RNIF del socio externo, la carga (RNSC - contenido de servicio RNIF) será extraída del paquete RNIF, validada y transformada en un documento XML para enviarla a la aplicación de fondo (Socio interno). Cuando proceda de una aplicación de fondo (Socio interno), se efectuará una comprobación de ID

duplicado sobre el XML y, a continuación, se validará el XML, se transformará en RNSC y se realizará la validación. Todo esto de forma similar a la acción "Conversión bidireccional de RosettaNet y XML con validación" pero con una comprobación de duplicados adicional, ejecutada en el XML de origen.

Configuración

- El formato XML del documento de origen necesita que la comprobación de claves duplicadas esté configurada
- Es necesario haber cargado el paquete PIP de RosettaNet para el documento RosettaNet.
- Requiere que el mapa de correlación (XML SCHEMA) se configure en el documento XML de origen o de destino
- Es necesario configurar una correlación de transformación XSLT para esta acción

Modificación

Esta acción no puede ser copiada ni modificada, ya que es específica de un documento RNIF.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - con un XML personalizado recibido realiza una comprobación de ID duplicado.
2. **com.ibm.bcg.server.pkg.UnPackagingFactory** - determina la clase de desempaquetado correcta para RNIF o asume que el documento no es RNIF y no se lleva a cabo ningún empaquetado.
3. **com.ibm.bcg.validation.ValidationFactory** – para validarel RNIF de origen o documento XML.
4. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – transforma el RNSC en / a partir del XML.
5. **com.ibm.bcg.validation.OutboundValidationFactory** - valida el documento XML transformado resultante.
6. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - utilizado para procesar documentos 0A1 de RosettaNet para actualizar el motor de estado de RosettaNet.
7. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Traducción bidireccional de XML personalizado con validación

Esta acción se utiliza con documentos XML personalizados procedentes de un socio externo o de los socios internos. El documento de origen se valida, se transforma en el documento de destino y se valida el documento de destino.

Configuración

- Requiere que la correlación de validación (XML SCHEMA) esté configurada en el documento de origen
- Es necesario configurar una correlación de transformación XSLT para esta acción

- Requiere que la correlación de validación (XML SCHEMA) esté configurada en el documento de destino

Modificación

Esta acción puede ser copiada o modificada. Los pasos de transformación o de validación pueden ser sustituidos con pasos de Usuarios definidos o pasos definidos por el usuario adicionales añadidos.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.validation.ValidationFactory** – este paso valida el documento XML personalizado recibido.
2. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** – realiza la transformación.
3. **com.ibm.bcg.validation.OutboundValidationFactory** - valida el documento XML transformado resultante.
4. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Traducción bidireccional de XML personalizado con comprobación duplicada y validación

Esta acción se utiliza con documentos XML personalizados. Puede utilizarse para documentos procedentes el socio externo o del socio interno. Se realiza la comprobación de ID duplicado en el documento origen, validación en el documento origen, transformación del documento de origen en el documento de destino y la validación del documento de destino. Esta acción es similar a la "Conversión bidireccional de XML personalizado con validación" excepto por el paso de comprobación de duplicados adicional.

Configuración

- El formato XML del documento de origen necesita que la comprobación de claves duplicadas esté configurada
- Requiere que la correlación de validación (XML SCHEMA) esté configurada en el documento de origen
- Es necesario configurar una correlación de transformación XSLT para esta acción
- Requiere que la correlación de validación (XML SCHEMA) esté configurada en el documento de destino

Modificación

Esta acción puede ser copiada o modificada. Los pasos que pueden ser sustituidos con pasos definidos por el usuario son ValidationFactory, XSLTTranslationFactory y OutboundValidationFactory o pasos definidos por el usuario adicionales añadidos.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - comprueba un documento duplicado basado en el ID de documento.
2. **com.ibm.bcg.validation.ValidationFactory** - este paso valida el documento XML personalizado recibido.
3. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** - este paso transforma el documento XML personalizado recibido al formato XML de destino.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - este paso valida el documento XML de destino del paso de transformación anterior.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Paso a través de XML personalizado con comprobación duplicada y validación

Propósito

Esta acción se utiliza con documentos XML personalizados. Puede utilizarse para documentos procedentes de un socio externo o del socio interno. Se realiza la comprobación de ID duplicado y la validación del documento de origen. Esta acción es similar a la "Paso a través de XML personalizado con comprobación de duplicados" excepto en que se ejecuta una comprobación de validación de documento de origen adicional.

Configuración

- El formato XML del documento de origen necesita que se configuren las claves de comprobación duplicadas.
- Requiere que se configure la correlación de validación (XML SCHEMA) en el documento XML de origen.

Modificación

Esta acción puede ser copiada o modificada. Los pasos que pueden sustituirse con pasos definidos por el usuario son ValidationFactory o pasos definidos por el usuario adicionales.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - comprueba un documento duplicado basado en el ID de documento. El formato XML de este documento de origen debe tener la configuración de ID duplicado.
2. **com.ibm.bcg.validation.ValidationFactor**y - este paso valida el documento XML personalizado de origen.
3. **com.ibm.bcg.passthrough.No_op** - utilizado para indicar que el tipo de contenido del documento de destino no debe derivar del contenido del documento.

4. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Paso a través de XML personalizado con comprobación duplicada

Esta acción se utiliza con documentos XML personalizados. Puede utilizarse para documentos procedentes de un socio externo o del socio interno. Se realiza la comprobación de ID duplicados en el documento de origen.

Configuración

El formato XML del documento de origen necesita que se configuren las claves de comprobación duplicadas.

Modificación

Esta acción no puede copiarse a una nueva acción, ya que la posible modificación sería añadir un paso de validación, el cual ya está definido en la acción "Paso a través de XML personalizado con comprobación duplicada y validación".

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - comprueba un documento duplicado basado en el ID de documento. El formato XML de este documento de origen debe tener la configuración de ID duplicado.
2. **com.ibm.bcg.passthrough.No_op** - utilizado para indicar que el tipo de contenido del documento de destino no debe derivar del contenido del documento.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Paso a través de XML personalizado con validación

Esta acción se utiliza con los documentos XML personalizados procedentes de un socio externo o del socio interno. Se efectúa la validación en el documento de origen.

Configuración

Requiere que la correlación de validación (XML SCHEMA) esté configurada en el documento XML de origen.

Modificación

Esta acción puede ser copiada o modificada. ValidationFactory puede ser sustituido por un paso definido por el usuario o por pasos definidos por el usuario adicionales añadidos.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.validation.ValidationFactory** - este paso valida el documento XML personalizado de origen.
2. **com.ibm.bcg.passthrough.No_op** - utilizado para indicar que el tipo de contenido del documento de destino no debe derivar del contenido del documento.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Desensobrar EDI

Esta acción se utiliza con intercambios EDI procedentes de un socio externo. El intercambio EDI será desensobrado (y las transacciones EDI extraídas); dichas transacciones EDI serán reintroducidas en WebSphere Partner Gateway para su proceso individual. El documento de intercambio EDI no se procesa más dentro de WebSphere Partner Gateway.

Configuración

Configuración opcional en las definiciones de documento.

Modificación

Esta acción no puede ser copiada ni modificada

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.edi.business.process.EDIDenvFactory** – realiza el desensobrado de intercambio EDI.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Validación de EDI y conversión de EDI

Esta acción se utiliza para las transacciones EDI que han sido desensobradas desde un intercambio EDI por la acción Desensobrar EDI. Estas proceden de un Socio interno. Los documentos de transacción EDI serán validados y, a continuación, transformados.

Configuración

- Configuración opcional en las definiciones de documento
- Correlaciones de validación opcionales para la transacción EDI de origen desde el cliente DIS o desde el estudio de diseño WTX.

- Correlaciones de transformación desde el cliente DIS o desde el estudio de diseño de WTX.
- Connexión del participante desde cualquier paquete / EDI - Cualquier / De cualquier a ninguno / EDI - Cualquier / Cualquier debe instalarse con la acción definida como Desensobrar EDI.

Modificación

Esta acción puede ser copiada y modificada para añadir pasos de salida de usuario adicionales.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.edi.business.process.EDISourceValidationFactory** – Valida la transacción EDI. Este paso también emitirá el FA de EDI después de procesar todas las transacciones EDI desde el intercambio EDI.
2. **com.ibm.bcg.edi.business.process.EDITranslatorFactory** – Transforma la transacción EDI en el documento de destino.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Conversión de XML y validación de EDI

Propósito

Esta acción se utiliza con los documentos XML personalizados del socio interno. El documento XML de origen se transforma en una transacción EDI y se valida. A continuación se envía al programa de fondo o a un socio externo. Los formatos XML se utilizan para identificar la información de direccionamiento.

Configuración

- Configuración opcional en las definiciones de documento.
- Correlaciones de validación opcionales para la transacción EDI de destino desde el cliente DIS.
- Correlaciones de transformación desde el cliente DIS o desde el estudio de diseño de WDI.

Modificación

Esta acción puede ser copiada y modificada para eliminar EDITargetValidationFactory o para añadir pasos de salida de usuario adicionales.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.edi.business.process.XMLTranslatorFactory** – Transforma el documento XML de origen en la transacción EDI de destino.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – Valida la transacción EDI de destino.

3. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Conversión de ROD (FlatFile) y validación de EDI

Esta acción se utiliza para documentos orientados a registros (ROD/Archivo plano) procedentes del socio interno. El documento ROD de origen será transformado en una transacción EDI y validado.

Configuración

- Configuración opcional en las definiciones de documento.
- Correlaciones de validación opcionales para la transacción EDI de destino desde el cliente DIS.
- El estándar de ROD debería definirse en el cliente DIS y compilarse mediante una correlación de transformación edummy.
- El divisor ROD y el procesador de documentos genéricos deben añadirse por manejador de proceso en el receptor. Esto es para conocer el formato y el documento del diccionario.

Modificación

Esta acción puede ser copiada y modificada para eliminar EDITargetValidationFactory o para añadir pasos de salida de usuario adicionales.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.edi.business.process.RODTranslatorFactory** – transforma el documento ROD de origen en la transacción EDI de destino.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – Valida la transacción EDI de destino.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Dividir y analizar ebMS

Esta acción es para documentos ebMS procedentes de un socio externo. Los archivos adjuntos de carga serán extraídos y reintroducidos en WebSphere Partner Gateway para su proceso individual. El documento ebMS no se procesa más dentro de WebSphere Partner Gateway.

Configuración

No es necesaria ninguna configuración adicional.

Modificación

Esta acción no puede ser copiada ni modificada.

Pasos

Esta acción contiene los siguientes pasos, los cuales son ejecutados de forma secuencial:

1. **com.ibm.bcg.server.EBMSSplitAndParse** – los archivos adjuntos de carga se extraen creando documentos individuales.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza un paso obligatorio de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Validación de intercambio EDI

La validación de intercambio EDI se utiliza durante la integración asíncrona con WTW. Las transacciones individuales se extraen del intercambio desensobrándolo. La acción Desensobrar extraerá cada transacción del intercambio. Cada transación creará un documento que se pasará directamente a la validación

Nota: El atributo "Descartar sobre si hay errores" no se puede utilizar en el contexto de validación de intercambio EDI. Si intenta configurar el valor para utilizar este atributo, se ignorará el valor.

Configuración

- La conexión de participante desde <cualquier paquete> / EDI – xxxx / XXX a Ninguno / EDI – xxxx / XXX debe configurarse con la acción definida como "Validación de intercambio EDI"
- Si lo desea, el usuario de FA puede configurar la correlación FA.
- Debe definirse un canal para que el reconocimiento funcional fluya.

Transformación WTX

EDI, XML y ROD o los archivos planos se transforman mediante WTX.

La transformación de EDI mediante WTX puede ser asíncrona o síncrona. La transformación síncrona se utiliza mayoritariamente cuando una transacción desensobrada y validada se envía a WTX para procesar, pero aquí la transacción se volvería a ensobrar, tal como se requiere para procesar en WTX. Un vez se valida la transacción EDI correctamente, se pasa a la acción de transacción EDI de transformación WTX. En modo asíncrono, las transacciones EDI se transforman en los programas de fondo, donde WTX se despliega en WESB/WMB o lanzador WTX.

Deben tenerse en cuenta los siguientes puntos al utilizar EDI como entrada para transformación:

Importante:

1. Utilice siempre un delimitador de un único carácter.
2. Si utiliza la combinación "/r/n" como delimitador de caracteres y el delimitador de caracteres "/r" se encuentra en la posición de delimitador de segmento de la cabecera de intercambio, se ignorará el delimitador de caracteres "/n".
3. Modifique el árbol de tipo como corresponda.

Configuración para la transformación síncrona

- La conexión de participante de <cualquier paquete> / EDI – xxxx / XXX a None / EDI – xxxx / XXX debería instalarse con la acción definida como Desensobrador EDI.
- La conexión de participante de <N/D> / XXXXXXX/ YYYYY a Ninguna / ZZZZZZ / BBBBBBB debe configurarse con la acción definida como "Validación EDI" y "Transacción EDI de transformación WTX".
- Una correlación de transformación WTX debe asociarse también a este canal.

Configuración para la transformación asíncrona

- La conexión de participante de <cualquier paquete> / EDI – xxxx / XXX a None / EDI – xxxx / XXX debería instalarse con la acción definida como Desensobrador EDI.
- La conexión de participante de la transacción <N/D> / <versión edi>/ a <N/D> / <versión edi > / debe configurarse con la acción definida como Validación de EDI.
- La conexión de participante de <N/D> / <versión de edi> / transacción a <BI> / <intercambio edi> / <ISA> / <UNB> / <UCS> debe configurarse con la acción definida como Validación EDI& EDI RE-ENVELOPE.

Configuración para ROD y XML

- Transformación ROD: la conexión de participante de <cualquier paquete> / <cualquier protocolo (archivo plano)> / <cualquier archivo plano> a <Cualquier> / <ANY> / <Cualquier> formato debe configurarse con la acción definida como "Transformación WTX".
- Transformación XML: la conexión de participante de <cualquier paquete> / <cualquier protocolo> / <cualquier XML> a <Cualquier> / <ANY> / <Cualquier> formato deberían configurarse con la acción definida como "Transformación WTX".

Sobre WTX
Propósito

Cuando se utiliza WTX en modo asíncrono, transforma i produce transacciones EDI después de la transformación WTX. Esto se envía a WebSphere Partner Gateway para ensobrar.

Configuración

- Conexión desde <Programas de fondo> / <Diccionario EDI> / <documento EDI> {EDI Trx} a <N/D> / <EDI X12/EDIFACT> / <EDI ISA/UNB> con la acción Paso a través configure el perfil del ensobrador al final del destino. (Canal-A).
- Conexión desde <ND> / <Intercambio EDI> / <EDI ISA/UNB> a <ANY PACKAGE> / <EDI X12/EDIFACT> / <EDI ISA/UNB> con acción como paso a través. (Canal-B)
-

Reensobrador EDI

El reensobrador se usa para ensobrar transacciones individuales. Toma las cabeceras del ensobrador del sobre origen y envuelve con él las transacciones desensobradas.

Configuración

- Una conexión entre origen como transacción y Destino como Intercambio EDI con el perfil del sobre establecido
- Establezca la acción como Reensobrador EDI

Validación de sobre SOAP

Se validará toda la solicitud de servicio web contra el esquema SOAP1.1 según los estándares del sector. El Sobre SOAP de acción contiene los siguientes pasos, que se ejecutan secuencialmente:

1. **com.ibm.bcg.validation.WebserviceFactory** – Realiza la validación de la solicitud del servicio web y devuelve el manejador WebserviceValidation.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza el proceso necesario de WebSphere Partner Gateway en el documento de destino. Este es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Validación de cuerpo SOAP

Esta característica valida el Cuerpo SOAP o la carga disponible en el Sobre SOAP. La validación de la carga sólo está soportada para las cargas XML del Sobre SOAP. El puntero de ubicación de esquemas estándar del sector del XML de carga se utiliza para la validación basada en esquemas. Opcionalmente, puede asociar el esquema con la conexión de servicios web que corresponda para validar la carga. El esquema que haya asociado explícitamente con la conexión de servicios web tendrá preferencia sobre el esquema colocado en el XML de carga. En caso de que no haya ningún puntero de ubicación de esquema en el XML de carga, asocie un esquema de la conexión de servicios web. Los atributos de objetos de direccionamiento para tanto la solicitud como para la respuesta de servicios web son los siguientes:

- **ResponseValidation** – Establezca el valor de este atributo en “No” en el lado de destino si no desea validar un documento de respuesta. El valor predeterminado de este atributo es “Sí”.
- **ContentValidation** – Este atributo le permite habilitar o inhabilitar la validación de contenido para el XML de carga. De forma predeterminada, la validación de contenido está habilitada. Si la establece en “No”, se efectuará la validación gramatical .

El Cuerpo SOAP de acción contiene los siguientes pasos, que se ejecutan secuencialmente:

1. **com.ibm.bcg.validation.ValidationFactory** – Realiza la validación de la solicitud de servicio web.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza el proceso necesario de WebSphere Partner Gateway en el documento de destino. Éste es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Para actualizar WebSphere Partner Gateway para que incluya la característica de validación de la carga del Sobre SOAP, consulte la Guía del administrador.

Desensobrar SOAP

El Sobre SOAP debe desensobrarse y debe introducirse en el Cuerpo SOAP para su posterior proceso. Los atributos del objeto de direccionamiento para Desensobrar Sobre SOAP son los siguientes:

- **Desensobrar Sobre SOAP** - Sólo da soporte a la comunicación asíncrona. No se devuelve ningún fallo ni ninguna respuesta de SOAP, puesto que se trata de un soporte de perfil básico de servicio web en una sola dirección. En caso de que sea síncrono, Desensobrar Sobre SOAP fallará con el documento y se registrará un suceso de error.
- **Documento de desensobrado de redireccionamiento** - Se trata de un atributo de objeto de direccionamiento enlazado de la acción **Desensobrar Sobre SOAP**. Si este atributo de objeto de direccionamiento se establece en "Sí", la acción **Desensobrar Sobre SOAP** debe introducir el Cuerpo SOAP extraído del Sobre SOAP como un documento nuevo en WebSphere Partner Gateway. Además, debe introducirse el archivo adjunto también como un documento nuevo. Todos los documentos recién introducidos irán al paquete N/D. Para seguir direccionándolos, deberá configurar el canal basado en el paquete N/D para la carga extraída y los documentos adjuntos.
- **ConsumePayload**: este atributo se enlaza con el atributo **Redireccionar documento desensobrado**. Se utiliza para suprimir la carga útil después de la extracción. Si el valor de este atributo y el valor de **Redireccionar documento desensobrado** se establecen en "Sí", la carga útil no se extrae ni direcciona desde el sobre SOAP. Únicamente se direccionan los accesorios. En caso que este atributo se establezca en "No" y **Redireccionar documento desensobrado** se establezca en "Sí", la carga útil y los accesorios se direccionan por separado. El valor predeterminado de este atributo es "No".

La acción Desensobrar Sobre SOAP contiene los siguientes pasos, que se ejecutan secuencialmente:

1. **com.ibm.bcg.validation.SOAPDeEnveloperFactory** – Realiza la validación de la solicitud del servicio web y devuelve el manejador SOAPDeEnveloper.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Siempre necesario. Realiza el proceso necesario de WebSphere Partner Gateway en el documento de destino. Éste es el último paso y lo añade de forma automática la Consola a las acciones existentes o a las acciones recién creadas. Este paso no aparece en la lista de manejadores configurados.

Durante las instancias donde desee desensobrar SOAP con un accesorio y direccionar únicamente accesorios y no la carga útil bajo el cuerpo SOAP, la configuración es la siguiente:

- bcg.soap.ConsumePayload = Y (de manera predeterminada este valor es N)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (de manera predeterminada este valor es Y)

Cuando desee desensobrar SOAP con accesorios y direccionar la carga útil y los accesorios por separado, la configuración es la siguiente:

- bcg.soap.ConsumePayload = N (de manera predeterminada este valor es N)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (de manera predeterminada este valor es Y)

Para actualizar WebSphere Partner Gateway para que incluya la característica de validación de la carga del Sobre SOAP, consulte la *Guía del administrador de WebSphere Partner Gateway*.

Modificación de una acción definida por el usuario

Acerca de esta tarea

Para configurar una acción definida por el usuario, efectúe los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Acciones**.
2. Pulse el icono **Ver detalles** situado junto al nombre de la acción definida por el usuario que desea configurar.

   Aparece un listado de la acción, junto con una lista de manejadores (pasos de la acción) ya configurados para dicha acción.
3. Realice uno de los pasos siguientes para cada acción que desee modificar.
   a. Añada un paso seleccionando el manejador asociado de la **Lista disponible** y pulsando **Añadir**. El manejador pasa a la **Lista configurada**.
   b. Elimine un manejador seleccionándolo en la **Lista configurada** y pulsando **Eliminar**. El manejador pasa a la **Lista disponible**.
   c. Cambie el orden en el que se invocan los manejadores seleccionando el manejador y pulsando **Mover arriba** o **Mover abajo**.
   d. Para que un manejador se procese más de una vez, selecciónelo y pulse **Repetir**.

      Recuerde que se invocan todos los manejadores configurados para una acción y que los pasos que representan los manejadores se realizan en el orden en el que aparecen en la **Lista configurada**.
   e. Configure el manejador seleccionándolo en la **Lista configurada** y pulsando **Configurar**. Aparecerá la lista de los atributos que pueden configurarse.
4. Pulse **Guardar**.

Creación de acciones

Puede crear una acción de los siguientes modos:

- Crear una acción nueva y asociar manejadores a la acción.
- Copiar una acción suministrada con el producto y, si es necesario, modificar los manejadores asociados con ésta.

Creación de una acción nueva

Acerca de esta tarea

Para crear una acción nueva, efectúe los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Acciones**.
2. Pulse **Crear**.
3. Especifique un nombre para la acción. Este campo es necesario.
4. Especifique una descripción opcional de la acción.
5. Indique si se permite el uso de la acción.
6. Para cada paso que se invocará como parte de la acción, añada el manejador asociado seleccionándolo en la **Lista disponible** y pulsando **Añadir**. El manejador pasa a la **Lista configurada**.

   Recuerde que la acción invoca los manejadores en el orden en el que aparecen en la **Lista configurada**. Asegúrese de que coloca los manejadores en el orden correcto. Puede utilizar **Mover arriba** o **Mover abajo** para reorganizar el orden de los manejadores o **Repetir** para lograr que un manejador se procese en más de una ocasión.

7. Configure un manejador seleccionándolo en la **Lista configurada** y pulsando **Configurar**. Aparecerá la lista de los atributos que pueden configurarse.
8. Pulse **Guardar**.

Copiar una acción
Acerca de esta tarea

Para crear una acción copiando una acción existente, efectúe los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Acciones**.
2. En la lista Acciones, pulse el icono **Copiar** situado junto a la acción que desee copiar.
3. Especifique un nombre para la acción. Este campo es necesario.
4. Especifique una descripción opcional de la acción.
5. Indique si se permite el uso de la acción.
6. Tenga en cuenta que uno o varios pasos ya están en la **Lista configurada**. Estos son los pasos asociados con la acción copiada. Por ejemplo, si ha clonado la acción Cancelación del proceso de RosettaNet del socio interno que se proporciona con el producto, podrá ver la siguiente lista de manejadores disponibles y configurados:

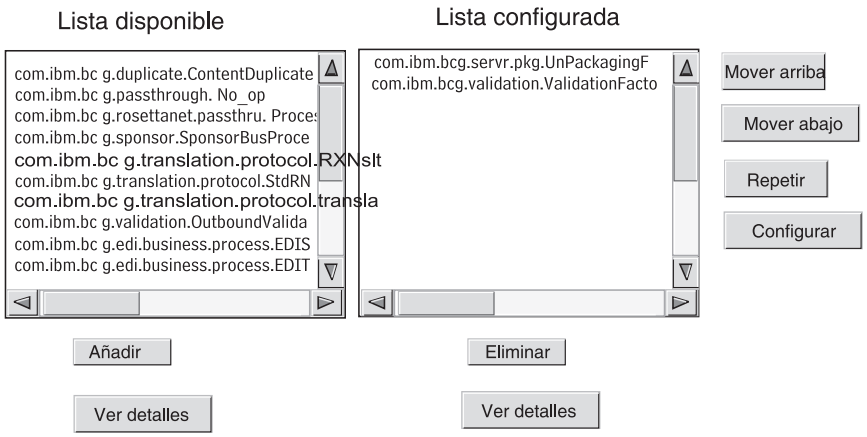


Figura 19. Clonación de una acción

Para modificar la **Lista configurada**, realice uno o varios de los siguientes pasos:

a. Añada un paso seleccionando el manejador asociado de la **Lista disponible** y pulsando **Añadir**. El manejador pasa a la **Lista configurada**.
b. Elimine un paso seleccionando el manejador asociado en la **Lista configurada** y pulsando **Eliminar**. El manejador pasa a la **Lista disponible**.
c. Cambie el orden en el que se invocan los manejadores seleccionando el manejador y pulsando **Mover arriba** o **Mover abajo**.

   Recuerde que se invocan todos los manejadores configurados para una acción y que los pasos asociados con los manejadores se realizan en el orden en el que aparecen en la **Lista configurada**.
d. Configure el paso seleccionándolo en la **Lista configurada** y pulsando **Configurar**. Aparecerá la lista de los atributos que pueden configurarse.

7. Pulse **Guardar.**

Capítulo 9. Configuración de tipos de documento

Este capítulo describe cómo configurar los documentos no EDI que intercambiará con los socios externos y con las aplicaciones de programas de fondo. La configuración de tipos de documento e interacciones para documentos EDI (con la excepción de documentos que se pasan a través) se describe en el apartado Capítulo 10, “Configuración de flujos de documentos EDI”, en la página 173. El apartado Capítulo 10, “Configuración de flujos de documentos EDI”, en la página 173 también describe cómo configurar tipos de documentos e interacciones para documentos XML y de datos orientados a registros (ROD).

Este capítulo incluye los siguientes temas:

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado la sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Visión general de los tipos de documento

Un definición de documento se compone de, como mínimo, un paquete, un protocolo y un tipo de documento. En el caso de algunos protocolos, se puede especificar una actividad, una acción y una señal. Las definiciones de documento especifican el tipo de documento que será procesado por WebSphere Partner Gateway.

El paquete hace referencia a la lógica necesaria para empaquetar un documento de acuerdo con una especificación, como AS2. Un flujo de protocolos es la lógica necesaria para procesar un documento que cumple las normas de un determinado protocolo, como EDI-X12. Un tipo de documento describe el aspecto del documento.

Los siguientes apartados describen brevemente los pasos generales para configurar un tipo de documento entre el socio interno y otro socio.

Paso 1: Asegúrese de que la definición del documento se encuentra disponible

Acerca de esta tarea

Compruebe si existe una definición de documento (las que están definidas con el sistema). Si todavía no existe ningún flujo, debe crearlo subiendo los archivos necesarios o creando manualmente una definición personalizada.

Como parte del establecimiento de la definición de documentos, puede modificar determinados atributos. Los atributos se utilizan para realizar varias funciones de direccionamiento y proceso de documentos, como la validación, la comprobación del cifrado y el recuento de intentos. Los atributos que establezca en el nivel de definición proporcionan un valor global para el paquete, protocolo o tipo de documento asociado. Los atributos que se encuentran disponibles varían dependiendo de la definición del documento. Los atributos para definiciones de documento EDI, por ejemplo, tienen atributos distintos de las definiciones de documento de RosettaNet.

Por ejemplo, si especifica un valor para **Tiempo de acuse de recibo** en el paquete AS, aplica a todos los documentos empaquetados con AS. (**Tiempo de acuse de recibo** especifica el intervalo de tiempo que se debe esperar a que llegue un acuse de recibo MDN (Message Disposition Notification) antes de reenviar la solicitud original). Si establece posteriormente el atributo **Tiempo para el acuse de recibo** en el nivel de funciones B2B, ese valor modifica el configurado en el nivel de definición del documento.

Para aquellos atributos que pueden establecerse en todos los niveles de la definición del documento, los valores establecidos en el nivel de tipo de documento tienen prioridad sobre los establecidos en el nivel del protocolo y los atributos establecidos en el nivel del protocolo tienen precedencia sobre aquellos en el nivel del paquete.

Antes de poder crear interacciones, el tipo de documento debe aparecer en la página Gestionar definiciones de documento. Para gestionar la definición de documentos, consulte el *capítulo Tareas de administración del concentrador de la Guía del administrador de WebSphere Partner Gateway*

Paso 2: Crear interacciones

Acerca de esta tarea

Cree interacciones para los tipos de documentos que han sido definidos. La interacción indica a WebSphere Partner Gateway qué acciones realizar en un documento. Para algunos intercambios, sólo necesitará dos flujos, uno para describir el documento que se ha recibido en el concentrador (desde el socio o desde el socio interno) y uno que describa el documento que se ha enviado desde el concentrador (al socio externo o al socio interno). Sin embargo, si el concentrador envía o recibe un intercambio EDI que se partirá en transacciones individuales o en el que se requieren acuses de recibo, en realidad el usuario creará varias interacciones para realizar el intercambio. Para gestionar las interacciones, consulte el *capítulo Tareas de administración del concentrador de la Guía del administrador de WebSphere Partner Gateway*

Paso 3: Crear perfiles de socios, destinos y posibilidades B2B

Acerca de esta tarea

Cree perfiles de socios para el socio interno y para los socios externos. Defina destinos (que determinan dónde se enviarán los documentos) y funciones B2B, que especifican los documentos que el socio interno y los socios externos pueden enviar y recibir. La página de funciones B2B lista todos los tipos de documentos que hayan sido definidos.

Puede establecer atributos en el nivel de funciones B2B. Todos los atributos establecidos en este nivel alterarán temporalmente los establecidos en el nivel de

definición de documentos. Por ejemplo, si establece **Tiempo de acuse de recibo** en 30 en el nivel de definición del documento para paquetes AS pero, a continuación, lo establece en 60 en el nivel de funciones B2B, se utilizará el valor de 60. Establecer un atributo en el nivel B2B permite personalizar el atributo a un socio concreto.

Paso 4: Activar conexiones

Acerca de esta tarea

Active las conexiones entre los socios internos y los socios externos. Las conexiones que están disponibles se basan en las interacciones creadas. Las interacciones se basan en las posibilidades B2B. Las interacciones dependen de las definiciones de documento que estén disponibles.

En algunos intercambios, sólo es necesaria una conexión. Por ejemplo, si un socio está enviando un documento binario a una aplicación de fondo del socio interno, sólo necesitará una conexión. Sin embargo, para el intercambio de intercambios EDI en el que el intercambio se desensobra y las transacciones individuales se transforman, se configuran varias conexiones.

Nota: en los intercambios EDI que se pasan tal como están, sólo se requiere una conexión.

Puede establecer atributos en el nivel de conexión. Todos los atributos establecidos en este nivel alterarán temporalmente los establecidos en el nivel de posibilidades B2B. Por ejemplo, si establece el **Tiempo de acuse de recibo** en 60 para el paquete AS2 en el nivel de funciones B2B, pero después lo establece en 120, se utilizará el valor 120. Si establece un valor para un atributo en el nivel de conexión, podrá personalizar más el atributo, dependiendo de los requisitos de direccionamiento de los socios y aplicaciones implicados.

Un flujo de ejemplo

Acerca de esta tarea

De manera predeterminada, hay varios métodos de empaquetamiento habilitados. Para ilustrar el procedimiento general para establecer definiciones de documento, tenga en cuenta el caso en el que existe un acuerdo con un socio externo para recuperar un intercambio EDI que cumpla el estándar EDI-X12. El socio enviará el documento con el empaquetado AS2. Especificará que el intercambio debe enviarse tal como está (sin transformación) a una aplicación de fondo sin empaquetado.

1. En la página Gestionar definiciones de documento, verifique que la definición de documento (que describe el tipo de documento que fluirá en el concentrador desde el socio) está habilitado.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   b. Pulse el icono **Expandir** situado junto a **Paquete: AS**. Observe que **EDI-X12** ya aparece en la lista.
   c. Pulse el icono **Expandir** situado junto a **Protocolo: EDI-X12**. Tenga en cuenta que **Tipo de documento: ISA** ya aparece listado.
2. Con la página Gestionar definición de documentos todavía en pantalla, verifique que la segunda definición del documento (que describe el tipo de documento que fluirá a la aplicación de fondo) está habilitada.

a. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**. Observe que **EDI-X12** ya aparece en la lista.
b. Pulse el icono **Expandir** situado junto a **Protocolo: EDI-X12**. Tenga en cuenta que **Tipo de documento: ISA** ya aparece listado.

3. Cree una interacción que describa si el tipo de documento será un tipo de origen o un tipo de receptor.
   a. Con la página Gestionar definición de documentos aún en pantalla, pulse el enlace **Gestionar interacciones**.
   b. En la columna Origen, expanda **Paquete: AS**, **Protocolo: EDI-X12 (ALL)** y, a continuación, pulse **Tipo de documento: ISA** para que el botón de selección esté seleccionado.
   c. En la columna Destino, expanda **Paquete: Ninguno**, **Protocolo: EDI-X12 (ALL)** y, a continuación, pulse **Tipo de documento: ISA** para que el botón de selección esté seleccionado.
   d. En este ejemplo, no se produce ninguna transformación. Por lo tanto, no seleccione nada en la lista **Correlación de transformación**.
   e. En la **lista Acción**, seleccione **Paso a través**.
   f. Pulse **Guardar**.

En este momento, ha especificado que el concentrador puede aceptar intercambios EDI-X12 (estándar ISA) empaquetados como AS. También ha especificado que el concentrador puede enviar intercambios EDI-X12 (estándar ISA) sin empaquetado. Además, ha especificado que no se va a producir ninguna transformación en el intercambio; simplemente pasará a la aplicación de fondo (una vez que se han eliminado las cabeceras AS).

Tabla 5. Interacciones proporcionadas por el producto para Open PGP

En el lado del remitente, defina esta conexión	En el lado del destinatario, defina esta conexión
Ninguno/EDI-X12/ISA a Ninguno/EDI-X12/ISA	Ninguno/EDI-X12/ISA a Ninguno/EDI-X12/ISA
Integración de programas de fondo/EDI-X12/ISA a Ninguno/EDI-X12/ISA	Ninguno/EDI-X12/ISA a Ninguno/EDI-X12/ISA

Nota: EDI-X12 no está presente en integración de programas de fondo de forma predeterminada, por lo que debe añadir "EDI-X12" al contexto de integración de programas de fondo. Después de añadir "EDI-X12" al contexto de integración de programas de fondo, añada "ISA" al contexto de integración de programas de fondo - EDI-X12.

Aún no ha especificado qué socio puede enviar este tipo de intercambio al concentrador. Defínalo cuando configure el perfil de socio y las funciones B2B del socio. (Defina también un perfil y las funciones B2B para el sistema de fondo del socio interno). Después de realizar estas tareas, debe crear una conexión entre el socio y la aplicación de fondo. La Figura 20 en la página 111 muestra la conexión entre el socio y la aplicación de fondo del socio interno en este ejemplo.

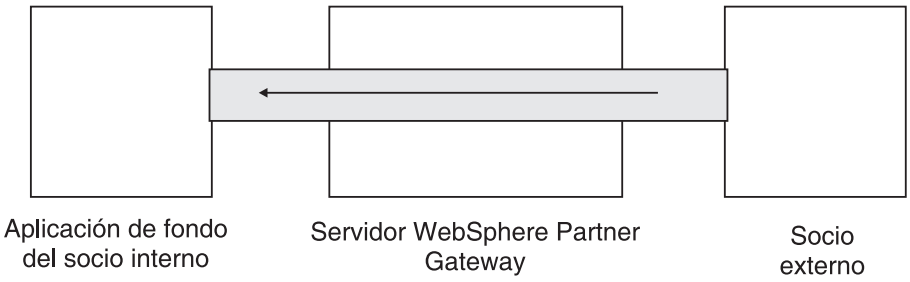


Figura 20. Conexión unidireccional desde el socio al socio interno

Verifique que existe una conexión utilizando la página Gestionar conexiones (**Administración de cuentas > Conexiones > Conexiones de socio**). En la página Gestionar conexiones, seleccione el socio en la lista **Origen**, el socio interno en la lista **Destino** y pulse **Buscar**. Aparecerá la conexión disponible. Si es necesario, puede modificar los atributos y las acciones, tal como se describe en los apartados siguientes.

Hay tres tipos de definiciones de documento: aquellas que proporciona el sistema y que es posible seleccionar desde la consola, aquellas que ya están definidos pero aún no se encuentran en la Consola de comunidad (estas definiciones se suben desde el soporte de instalación de WebSphere Partner Gateway o desde otra ubicación) y aquellas creadas por el propio usuario. Para cada tipo de definición de documento, puede (o a veces debe) especificar atributos o subir correlaciones que definan más en profundidad el tipo de documento.

Documentos binarios

Los documentos binarios son aquellos que se pasan por el concentrador tal cual. Estos documentos se intercambian entre un socio externo y un socio interno mediante una aplicación de fondo. Para crear conexiones entre ellos deberá haber definido previamente los perfiles y funciones business-to-business (B2B) de los socios internos y de los socios externos. Si no se utiliza el socio interno predeterminado, el ID de receptor del socio interno se debe especificar explícitamente. Cuando el documento binario se direcciona mediante el transporte HTTP utilizando autenticación básica, el ID de receptor se puede pasar a través del atributo **X-aux-receiver-id**. Utilizando un protocolo FTP, un socio externo puede enviar documentos binarios al concentrador. El protocolo binario ya está disponible para los paquetes AS, Ninguno e Integración de programas de fondo; por lo tanto, el “Paso 1: Asegúrese de que la definición del documento se encuentra disponible” en la página 107 ya está hecho.

Nota: puede añadir atributos a nivel nivel de Paquete, Protocolo o Tipo de documento para modificar el proceso predeterminado pulsando el icono **Editar valores de atributos**. No se asocia ningún atributo con el protocolo binario o tipo de documento de forma predeterminada.

De forma predeterminada, se proporcionan cuatro interacciones que incluyen documentos binarios para WebSphere Partner Gateway y se proporcionan tres interacciones nuevas para Open PGP. Para dichas interacciones, no es necesario realizar el “Paso 2: Crear interacciones” en la página 108. Se proporcionan interacciones para los siguientes intercambios:

Tabla 6. Interacciones proporcionadas por el producto

Paquete de origen/Protocolo/Tipo de documento	Paquete de destino/Protocolo/Tipo de documento
AS/Binario/Binario	Integración de programas de fondo/Binario/Binario
Integración de programas de fondo/Binario/Binario	AS/Binario/Binario
AS/Binario/Binario	Ninguno/Binario/Binario
Ninguno/Binario/Binario	AS/Binario/Binario

Para OpenPGP, habilite manualmente las siguientes interacciones soportadas desde la consola de WebSphere Partner Gateway:

Tabla 7. Interacciones soportadas de OpenPGP

Paquete de origen/Protocolo/Tipo de documento	Paquete de destino/Protocolo/Tipo de documento
Ninguno/Binario/Binario	Ninguno/Binario/Binario
Integración de programas de fondo/Binario/Binario	Ninguno/Binario/Binario

Para el intercambio de documentos binarios, todavía debe realizar:

- "Paso 3: Crear perfiles de socios, destinos y posibilidades B2B" en la página 108, que se describe en el apartadoCapítulo 3, "Creación y configuración de socios", en la página 25 y Capítulo 11, "Creación de destinos", en la página 223.
- "Paso 4: Activar conexiones" en la página 109, que se describe en el apartado Capítulo 12, "Gestión de conexiones", en la página 247.

Documentos EDI con acción de paso a través

WebSphere Partner Gateway ofrece la posibilidad de desensobrar y transformar los intercambios EDI, un proceso que se describe en el apartado Capítulo 10, "Configuración de flujos de documentos EDI", en la página 173.

La Figura 21 muestra el flujo de un intercambio EDI que está pasando a través de un socio al socio interno.

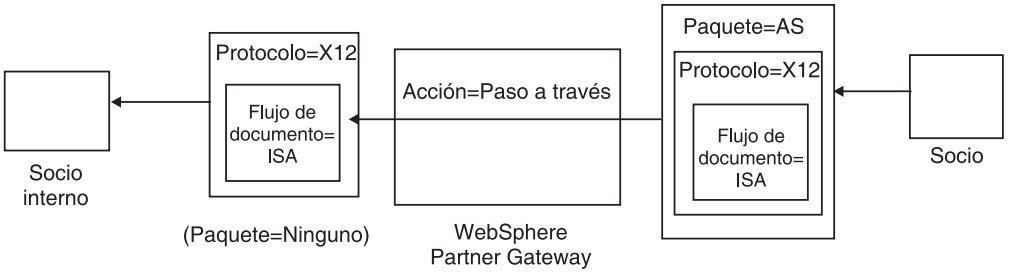


Figura 21. Acción de intercambio EDI entrante con paso a través

En este ejemplo, se han eliminado las cabeceras AS2, aunque aparte de esto el intercambio sigue intacto y fluye a través del sistema hasta el destino del socio interno.

En la transformación síncrona de la transacción EDI mediante WTX (EDI a cualquier), si la transformación tiene más de una salida, basada en el distintivo de redireccionamiento, el hijo pasará directamente al flujo de trabajo saliente o redireccionado en el flujo de entrada fijado para que pase por un nuevo canal. En el caso de Asíncrono, el WTX enviará transacciones EDI a WPG para ensobrarlas. Necesitará establecer conexiones en dos canales - <ninguna> / <Diccionario EDI> / <documento EDI > {EDI Trx} con Paso a través y <ND> / <Intercambio EDI> / <,EDI ISA / UNB> to <Cualquier paquete> / <EDI X12 / <FACT> / <EDI ISA / UNB con acciones como Paso a través.

Creación de definiciones de documento

Acerca de esta tarea

El tipo de documento para los intercambios de paso a través EDI se proporciona (de manera predeterminada) en la página Gestionar definición de documentos, tal como se describe en el apartado "Un flujo de ejemplo" en la página 109. Si desea modificar cualquiera de los atributos que tienen valores predeterminados o establecer un atributo que no tiene ningún valor asignado, puede utilizar la página Gestionar definiciones de documento para realizar esta tarea.

Por ejemplo, suponga que desea cambiar el atributo **Tiempo de acuse de recibo** para un documento EDI empaquetado con AS. Los pasos que debe seguir son los siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse el icono **Editar valores de atributo** situado junto a **Paquete: AS**.
3. Desplácese hasta el apartado de la página titulada **Atributos de contexto de definición de documento**.
4. En la fila **Tiempo de acuse de recibo**, escriba un valor distinto en la columna **Actualizar**.
5. Pulse **Guardar**.

Recuerde que ha cambiado un atributo de paquete en este ejemplo. Los atributos para el protocolo (por ejemplo, EDI-X12) y para el tipo de documento (por ejemplo, ISA) no son relevantes para una acción de Paso a través. Este atributo de paquete se aplica a todos los documentos empaquetados en AS.

Creación de interacciones

Acerca de esta tarea

Para crear la interacción para una acción de intercambio EDI entrante con paso a través, realice los siguientes pasos:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Bajo **Origen**, expanda **Paquete: AS** y **Protocolo: EDI-X12** y, a continuación, seleccione **Tipo de documento: ISA**.
4. Bajo **Destino**, expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y, a continuación, seleccione **Tipo de documento: ISA**.
5. Si lo desea, seleccione una **Correlación de transformación**.
6. En la lista **Acción**, seleccione **Paso a través**.

En los pasos del 1 al 4 se ha habilitado WebSphere Partner Gateway para que acepte un intercambio EDI-X12 empaquetado como AS de un socio de origen, para enviar un intercambio EDI-X12 sin empaquetado al socio de destino y para que el intercambio pase a través del origen hasta el destino.

Si desea definir una interacción que tenga el documento de origen empaquetado como Ninguno/EDI-X12/ISA y el documento de destino empaquetado como AS/EDI-X12/ISA, expanda **Paquete: Ninguno** en el paso 3 (en la columna **Origen**) y expanda **Paquete: AS** en el paso 4 (en la columna **Destino**).

documentos de RosettaNet

RosettaNet es una organización que proporciona estándares abiertos para dar soporte al intercambio de mensajes empresariales entre socios. Para obtener más información sobre RosettaNet, consulte http://www.rosettanet.org. Los estándares incluyen las especificaciones RosettaNet Implementation Framework (RNIF) y Partner Interface Process (PIP). RNIF define el modo en que los socios intercambian mensajes proporcionando una infraestructura de empaquetamiento de mensajes, protocolos de transferencia y seguridad. Se han publicado dos versiones: la 1.1 y la 2.0. Un PIP define un proceso empresarial público y los formatos de mensaje basados en XML que dan soporte al proceso.

WebSphere Partner Gateway da soporte a la mensajería de RosettaNet utilizando RNIF 1.1 y 2.0. Cuando el concentrador recibe un mensaje de PIP, valida y transforma el mensaje para enviarlo al sistema de programas de fondo apropiado. WebSphere Partner Gateway proporciona un protocolo para empaquetar el mensaje transformado en un mensaje RosettaNet Service Content (RNSC) que pueda manejar el sistema de programas de fondo. Consulte la publicación *Guía de integración empresarial de WebSphere Partner Gateway* para obtener información sobre el empaquetado utilizado en estos mensajes para facilitar información de direccionamiento.

El concentrador también puede recibir mensajes RNSC de sistemas de programas de fondo y crear el mensaje PIP correspondiente y enviar el mensaje al socio comercial correspondiente (un socio). El usuario debe proporcionar las definiciones de documento para la versión RNIF y para los PIP que desee utilizar.

Además de facilitar la posibilidad de direccionamiento para mensajes RosettaNet, WebSphere Partner Gateway mantiene un estado para cada mensaje que maneja. Ello le permite reenviar cualquier mensaje que falle hasta que el número de intentos alcance un umbral específico. Se recomienda mecanismo de notificación de sucesos alerta a los sistemas de fondo cuando no es posible enviar un mensaje PIP. Además, el concentrador puede generar automáticamente PIP 0A1 para enviar a los socios apropiados si recibe determinados mensajes de notificación de suceso de los sistemas de programas de fondo. Consulte la publicación *WebSphere Partner Gateway Enterprise Integration Guide* para obtener más información acerca de la notificación de sucesos.

Paquetes de tipo de documento RNIF y PIP

Para dar soporte a la mensajería de RosettaNet, WebSphere Partner Gateway proporciona dos conjuntos de archivos comprimidos denominados paquetes. Se recomienda *paquetes RNIF* constan de definiciones de documento necesarias para dar soporte al protocolo RNIF. Estos paquetes se encuentran en el directorio B2BIntegrate.

Para RNIF V1.1, los paquetes son:

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

Para RNIF V02.00, los paquetes son:

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

EL primer paquete en cada par proporciona las definiciones de documento necesarias para dar soporte a las comunicaciones RosettaNet con los socios y el segundo paquete proporciona las definiciones de documento necesarias para dar soporte a las comunicaciones RosettaNet con los sistemas de fondo.

El segundo conjunto consiste en paquete de tipo de documento PIP. Cada paquete de tipo de documento PIP tiene un directorio Packages que contiene un archivo XML y un directorio GuidelineMaps que contiene archivos XSD. El archivo XML especifica las definiciones de documento que definen cómo WebSphere Partner Gateway maneja el PIP y define los mensajes y señales intercambiados. Los archivos XSD especifican el formato de los mensajes PIP y definen valores aceptables para elementos XML en los mensajes. Los archivos comprimidos para PIP 0A1 también tienen un archivo XML que el concentrador utiliza como plantilla para crear documentos 0A1.

Se recomienda PIP para los que WebSphere Partner Gateway proporciona paquetes de tipo de documento PIP son:

- PIP 0A1 Notificación de anomalía v1.0
- PIP 0A1 Notificación de anomalía V02.00.00
- PIP 2A1 Distribución de información de nuevo producto V02.00.00
- PIP 2A12 Distribución de maestro de productos V01.03.00
- PIP 3A1 Solicitud de oferta V02.00.00
- PIP 3A2 Solicitud de precio y disponibilidad R02.01.00
- PIP 3A4 Solicitud de pedido de compra V02.02.00
- PIP 3A4 Solicitud de pedido de compra V02.00
- PIP 3A5 Consulta del estado del pedido R02.00.00
- PIP 3A6 Distribución del estado del pedido V02.02.00
- PIP 3A7 Notificación de actualización de pedido de compra V02.02.00
- PIP 3A8 Solicitud de modificación de pedido de compra V01.02.00
- PIP 3A8 Notificación de actualización de pedido de compra V01.03.00
- PIP 3A9 Solicitud de cancelación de pedido de compra V01.01.00
- PIP 3B2 Notificación de envío anticipado V01.01.00
- PIP 3B3 Distribución del estado del envío R01.00.00
- PIP 3B11 Notificación de orden de envío R01.00.00A
- PIP 3B12 Solicitud de orden de envío V01.01.00
- PIP 3B13 Notificación de confirmación de orden de envío V01.01.00
- PIP 3B14 Solicitud de cancelación de orden de envío V01.00.00
- PIP 3B18 Notificación de documentación de envío V01.00.00
- PIP 3C1 Devolución de producto V01.00.00
- PIP 3C3 Notificación de factura V01.01.00
- PIP 3C4 Notificación de rechazo de factura V01.00.00

- PIP 3C6 Notificación de información de remesa V01.00.00
- PIP 3C7 Notificación de factura de facturación automática V01.00.00
- PIP 3D8 Distribución de trabajo en curso V01.00.00
- PIP 4A1 Notificación de previsión estratégica V02.00.00
- PIP 4A3 Notificación de pronóstico con liberación por umbral V02.00.00
- PIP 4A4 Notificación de planificación de pronóstico con liberación R02.00.00A
- PIP 4A5 Notificación de respuesta de pronóstico V02.00.00
- PIP 4B2 Notificación de recibo de envío V01.00.00
- PIP 4B3 Notificación de consumo V01.00.00
- PIP 4C1 Distribución de informe de inventario V02.03.00
- PIP 4C1 Distribución de informe de inventario V02.01
- PIP 5C1 Distribución de lista de productos V01.00.00
- PIP 5C2 Solicitud de registro de diseño V01.00.00
- PIP 5C4 Distribución de estado de registro V01.02.00
- PIP 5D1 Solicitud de envío de existencias y autorización de débito V01.00.00
- PIP 6C1 Consulta de derecho de servicio V01.00.00
- PIP 6C2 Solicitud de derecho de garantía V01.00.00
- PIP 7B1 Distribución de trabajo en curso V01.00.00
- PIP 7B5 Notificación de pedido de trabajo de fabricación
- PIP 7B6 Notificación de respuesta de pedido de trabajo de fabricación V01.00.00

Para cada PIP, existen cuatro Paquetes de tipo de documento PIP:

- Para mensajería RNIF 1.1 con socios
- Para mensajería RNIF 1.1 con sistemas de fondo
- Para mensajería RNIF 2.0 con socios
- Para mensajería RNIF 2.0 con sistemas de fondo

Cada paquete de tipo de documento PIP sigue un convenio de denominación determinado que puede utilizar para identificar si el paquete es para mensajes entre WebSphere Partner Gateway y socios o entre WebSphere Partner Gateway y sistemas de fondo. El convenio de denominación también identifica la versión de RNIF, PIP y la versión PIP que soporta el paquete. Para paquetes de tipo de documento PIP utilizados para la mensajería entre WebSphere Partner Gateway y los socios, el formato es:

`BCG_Package_RNIF<versión_RNIF>_<PIP><versión_PIP>.zip`

Para paquetes de tipo de documento PIP utilizados para la mensajería entre WebSphere Partner Gateway y los sistemas de fondo, el formato es:

`BCG_Package_RNSC<versión_integración_programas_fondo>_RNIF<versión_RNIF>_<PIP><versión_PIP>.zip`

Por ejemplo, BCG_Package_RNIF1.1_3A4V02.02.zip es para validar documentos para la Versión 02.02 del PIP 3A4 enviados entre socios y WebSphere Partner Gateway utilizando el protocolo RNIF 1.1. Para que los paquetes de tipo de documento PIP se comuniquen con sistemas de fondo, el nombre del paquete también debe identificar el protocolo utilizando para enviar el contenido RosettaNet a los sistemas de fondo. Consulte la publicación *Guía de integración empresarial de WebSphere Partner Gateway* para obtener información sobre el paquete utilizado para estos mensajes.

Creación de definiciones de documento

Acerca de esta tarea

Para la mensajería RosettaNet, WebSphere Partner Gateway requiere los paquetes RNIF para la versión de RNIF utilizada para enviar los mensajes. Para cada PIP soportado por WebSphere Partner Gateway, son necesarios los dos paquetes de tipo de documento PIP para la versión RNIF. Por ejemplo, para dar soporte a PIP 3A4 en RNIF 2.0, WebSphere Partner Gateway requiere los siguientes paquetes:

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip
- BCG_Package_RNIFV02.00_3A4V02.02.zip
- BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip

El primer paquete da soporte a la mensajería RosettaNet con socios y el segundo paquete da soporte a la mensajería RosettaNet con sistemas de programas de fondo. El tercer y cuarto paquete permiten que WebSphere Partner Gateway pase mensajes 3A4 entre los socios y los sistemas de fondo utilizando RNIF 2.0.

Para subir los paquetes RosettaNet:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse **Subir/descargar paquetes**.
3. Seleccione **No** en **Paquete WSDL**.
4. Pulse **Examinar** y seleccione el paquete RNIF para comunicarse con los socios.

   De manera predeterminada, los paquetes RNIF se encuentran en el directorio B2BIntegrate/Rosettanet del soporte de instalación. Por ejemplo, en el caso de que subiera el paquete de la versión 2.00 de RNIF, debería ir al directorio B2BIntegrate/Rosettanet y seleccionar: Package_RNIF_V0200.zip.
5. Asegúrese de que **Confirmar en base de datos** se establece en **Sí**.
6. Pulse **Subir**.
7. Pulse de nuevo **Examinar** y seleccione el paquete RNIF para comunicarse con las aplicaciones de programas de fondo.

   Por ejemplo, en el caso de que subiera el paquete de la versión 2.00 de RNIF, debería ir al directorio B2BIntegrate/Rosettanet y seleccionar Package_RNSC_1.0_RNIF_V02.00.zip.
8. Pulse **Subir**.

   Los paquetes necesarios para comunicarse con los socios o con el sistema de fondo están ahora instalados en el sistema. Si comprueba la página Gestionar definiciones de documento, verá una entrada para **Paquete: RNIF/Protocolo: RosettaNet**, que representa el empaquetado para comunicarse con los socios, y **Paquete: Integración de fondo/Protocolo: RNSC**, que representa el empaquetado para comunicarse con aplicaciones de fondo.
9. Para cada PIP al que se desee dar soporte, suba el paquete de tipo de documento PIP para el PIP y para la versión RNIF a la que da soporte. Por ejemplo, para subir el PIP 3A6 (Notificación de información de remesa) para que sea enviado a un socio, lleve a cabo los siguientes pasos:
   a. Pulse **Examinar** y seleccione BCG_Package_RNIFV02.00_3C6V02.02 en el directorio B2BIntegrate/RosettaNet.
   b. Asegúrese de que **Confirmar en base de datos** se establece en **Sí**.
   c. Pulse **Subir**.

El PIP 3C6V02.02 aparece ahora como el tipo de documento bajo **Paquete: RNIF/Protocolo: RosettaNet** en la página Gestionar definiciones de documento. También se visualiza una actividad, acción y dos señales. Se incluyen en la subida del PIP.

Para subir el 3A6 PIP que se va a enviar a la aplicación de fondo, efectúe los siguientes pasos:

a. Pulse **Examinar** y seleccione BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip.
b. Asegúrese de que **Confirmar en base de datos** se establece en **Sí**.
c. Pulse **Subir**.

El PIP 3C6V02.02 aparece ahora como el tipo de documento bajo **Paquete: Integración de fondo/Protocolo: RNSC** en la página Gestionar definiciones de documento. Si WebSphere Partner Gateway no proporciona un paquete para el PIP o la versión de PIP que se desea utilizar, puede crear su propio paquete y subirlo. Consulte el apartado "Creación de paquetes de definición de documentos PIP" en la página 377 para obtener más información.

Configuración de valores de atributo

Acerca de esta tarea

Para las definiciones de documento PIP, la mayoría de valores de los atributos ya están definidos y no es necesario configurarlos. Sin embargo, sí es necesario definir los atributos siguientes:

Paquete RNIF (1.0)

- **GlobalSupplyChainCode** - identifique el tipo de la cadena de suministro utilizada por el socio. Los posibles tipos son: componentes electrónicos, tecnología de la información y fabricación de semiconductores. Este atributo no tiene un valor predeterminado.

Paquete RNIF (V02.00)

- **Cifrado**: defina si los PIP deben tener una carga cifrada, un contenedor y una carga cifrados o no debe presentar ningún cifrado. El valor predeterminado es Ninguno.
- **Acuse recibo sínc. necesario** - establézcalo en Sí si el socio desea recibir el acuse de recibo. Establézcalo en No si se solicita un 200.
- **Sinc. soportada**: defina si PIP da soporte a los intercambios de mensajes síncronos. El valor predeterminado es No.

Tenga en cuenta que los PIP para los cuales WebSphere Partner Gateway proporciona paquetes de tipo de documento PIP no son síncronos. Como resultado, no es necesario cambiar los atributos de Acuse recibo sínc. necesario y Sinc. soportada para estos PIP.

Nota: el comportamiento del atributo Acuse recibo sínc. necesario difiere entre PIP unidireccional y bidireccional. Para un PIP bidireccional, cuando Acuse recibo está establecido en No, este valor tiene prioridad sobre un valor de Sí de Sin rechazo. Por ejemplo, supongamos que envía un 3A7 con los valores siguientes:

- SiqReq=Y
- NonRepofRec=Y
- SyncSupported=Y
- SyncAckReq=N

En un PIP bidireccional, recibirá un mensaje de error en el documento entrante. En un PIP unidireccional, sin embargo, podrá ver el documento entrante en la consola y se devolverá un OKB 200 al socio.

Para establecer los atributos, realice los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse los iconos **Expandir** para expandir individualmente un nodo al nivel de definición de documento correspondiente o seleccione **Todos** para expandir todos los nodos de definición de documento visualizados.
3. En la columna **Acciones**, pulse el icono **Editar valores de atributo** para el paquete (por ejemplo, Paquete: RNIF (1.1) o Paquete: RNIF (V02.00)) que desea editar.
4. En el apartado **Atributos de contexto de definición de documento**, vaya a la columna **Actualizar** del atributo que desea definir o escriba el nuevo valor. Repita el mismo procedimiento para cada atributo que desee establecer.
5. Pulse **Guardar**.

Nota: también puede actualizar atributos RosettaNet en el nivel de conexión pulsando **Atributos** para el origen o el destino y, a continuación, especificar o cambiar los valores en la columna **Actualizar**. Consulte el apartado "Especificación o cambio de atributos" en la página 248.

Creación de interacciones

Acerca de esta tarea

El siguiente proceso describe cómo crear una interacción entre un sistema de fondo y un socio. Observe que es preciso crear una interacción para cada PIP que se desea enviar y una para cada PIP que se desea recibir.

Antes de comenzar, asegúrese de haber subido las definiciones de documento RNIF correspondientes y de que los paquetes para el PIP que desea utilizar han sido subidos. Si desea poder generar un PIP 0A1 (Notificación de anomalía), asegúrese de haber subido dicho PIP tal como se describe en el paso 9 en la página 117.

Para crear una interacción para un PIP concreto, realice los siguientes pasos:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda el árbol **Origen** hasta el nivel de **Acción** y expanda el árbol **Destino** hasta el nivel de **Acción**.
4. En los árboles, seleccione las definiciones de documento que desea utilizar para el contexto de origen y para el contexto de destino. Por ejemplo, si el socio es el iniciador de un PIP 3C6 (un PIP de una acción), seleccione las siguientes definiciones de documento:

Tabla 8. PIP 3C6 iniciado por un socio

Origen	Destino
Paquete: RNIF (V02.00)	Paquete: Integración de programas de fondo (1.0)
Protocolo: RosettaNet (V02.00)	Protocolo: RNSC (1.0)

Tabla 8. PIP 3C6 iniciado por un socio (continuación)

Origen	Destino
Tipo de documento: 3C6 (V01.00)	Tipo de documento: 3C6 (V01.00)
Actividad: Notificación de información de remesa	Actividad: Notificación de información de remesa
Acción: acción de notificación de información de remesa	Acción: acción de notificación de información de remesa

Si el sistema de programas de fondo es el iniciador del PIP 3C6, seleccione las siguientes definiciones de documento:

Tabla 9. PIP 3C6 iniciado por un sistema de fondo

Origen	Destino
Paquete: Integración de programas de fondo (1.0)	Paquete: RNIF (V02.00)
Protocolo: RNSC (1.0)	Protocolo: RosettaNet (V02.00)
Tipo de documento: 3C6 (V01.00)	Tipo de documento: 3C6 (V01.00)
Actividad: Notificación de información de remesa	Actividad: Notificación de información de remesa
Acción: acción de notificación de información de remesa	Acción: acción de notificación de información de remesa

Para un PIP de dos acciones como 3A4 iniciado por un socio, seleccione las siguientes definiciones de documento para la primera acción:

Tabla 10. PIP 3A4 iniciado por un socio

Origen	Destino
Paquete: RNIF (V02.00)	Paquete: Integración de programas de fondo (1.0)
Protocolo: RosettaNet (V02.00)	Protocolo: RNSC (1.0)
Tipo de documento: 3A4 (V02.02)	Tipo de documento: 3A4 (V02.02)
Actividad: Solicitud de pedido de compra	Actividad: Solicitud de pedido de compra
Acción: acción de solicitud de pedido de compra	Acción: acción de solicitud de pedido de compra

Si un sistema de fondo inicia el PIP 3A4 de dos acciones, seleccione las siguientes definiciones de documento para la primera acción:

Tabla 11. PIP 3A4 iniciado por un sistema de programas de fondo

Origen	Destino
Paquete: Integración de programas de fondo (1.0)	Paquete: RNIF (V02.00)
Protocolo: RNSC (1.0)	Protocolo: RosettaNet (V02.00)
Tipo de documento: 3A4 (V02.02)	Tipo de documento: 3A4 (V02.02)
Actividad: Solicitud de pedido de compra	Actividad: Solicitud de pedido de compra
Acción: acción de solicitud de pedido de compra	Acción: acción de solicitud de pedido de compra

5. En el campo Acción, seleccione **Traducción bidireccional de RosettaNet y Contenido de servicio de RosettaNet con validación**.

6. Pulse **Guardar**.
7. Si está configurando un PIP de dos acciones, repita los pasos necesarios para crear la interacción para la segunda acción. Por ejemplo, seleccione las siguientes definiciones de documento para la segunda acción para un PIP 3A4 iniciado por un socio. Ésta es la acción en la que el sistema de fondo envía la respuesta.

Tabla 12. PIP 3A4 iniciado por un socio (segunda acción)

Origen	**Destino**
Paquete: Integración de programas de fondo (1.0)	Paquete: RNIF (V02.00)
Protocolo: RNSC (1.0)	Protocolo: RosettaNet (V02.00)
Tipo de documento: 3A4 (V02.02)	Tipo de documento: 3A4 (V02.02)
Actividad: Solicitud de pedido de compra	Actividad: Solicitud de pedido de compra
Acción: Acción de confirmación de pedido de compra	Acción: Acción de confirmación de pedido de compra

Para la segunda acción para un PIP 3A4 iniciado por un sistema de fondo, seleccione las siguientes definiciones de documento:

Tabla 13. PIP 3A4 iniciado por un sistema de fondo (segunda acción)

Origen	**Destino**
Paquete: RNIF (V02.00)	Paquete: Integración de programas de fondo (1.0)
Protocolo: RosettaNet (V02.00)	Protocolo: RNSC (1.0)
Tipo de documento: 3A4 (V02.02)	Tipo de documento: 3A4 (V02.02)
Actividad: Solicitud de pedido de compra	Actividad: Solicitud de pedido de compra
Acción: Acción de confirmación de pedido de compra	Acción: Acción de confirmación de pedido de compra

8. Si desea generar la 0A1 Notificación de anomalía, cree una interacción para XMLEvent.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Expanda el árbol **Origen** al nivel de **Tipo de documento** y expanda el árbol **Destino** al nivel de **Tipo de documento**.
   d. Seleccione las siguientes definiciones de documento:

Tabla 14. Definición de documentos de suceso XML

Origen	**Destino**
Paquete: Integración de programas de fondo (1.0)	Paquete: Integración de programas de fondo (1.0)
Protocolo: XMLEvent (1.0)	Protocolo: XMLEvent (1.0)
Tipo de documento: XMLEvent (1.0)	Tipo de documento: XMLEvent (1.0)

   e. En el campo Acción, seleccione **Paso a través**.
   f. Pulse **Guardar**.
9. Cree una interacción para XMLEvent con 0A1 RNSC.

a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
c. Expanda el árbol **Origen** al nivel de **Tipo de documento** y expanda el árbol **Destino** al nivel de **Actividad**.
d. Seleccione las siguientes definiciones de documento:

Tabla 15. Definición de tipo de documentos de suceso XML a 0A1

Origen	Destino
Paquete: Integración de programas de fondo (1.0)	Paquete: Integración de programas de fondo (1.0)
Protocolo: XMLEvent (1.0)	Protocolo: RNSC (1.0)
Tipo de documento: XMLEvent (1.0)	Tipo de documento: 0A1 (V02.00)
	Actividad: Distribución de notificación de anomalía.

e. En el campo Acción, seleccione **Conversión bidireccional de RosettaNet y XML con validación**.
f. Pulse **Guardar**.

Nota: Para habilitar o inhabilitar XMLEvents, consulte *la sección Habilitación o inhabilitación de XMLEvents de la Guía de integración empresarial*

Visualización de documentos RosettaNet

Acerca de esta tarea

El Visor de RosettaNet muestra información acerca de los documentos de RosettaNet. Puede mostrar documentos sin formato y los sucesos y detalles de proceso de documentos asociados mediante criterios de búsqueda específicos. Esta información es útil si está intentando determinar si un documento se ha entregado satisfactoriamente o para determinar la causa de un problema.

Para mostrar el Visor de RosettaNet, lleve a cabo los siguientes pasos:

1. Pulse **Visores > Visor de RosettaNet**.
2. Seleccione el criterio de búsqueda apropiado de las listas, como se describe en Tabla 16.

Tabla 16. Criterios de búsqueda de RosettaNet

Valor	Descripción
Fecha y hora de inicio	La fecha y hora de inicio del proceso.
Fecha y hora de finalización	La fecha y hora de finalización del proceso.
Socio de origen y de destino	Identifica los socios (sólo socio interno) de origen (inicio) y de destino (recepción).
Socio	Indica si la búsqueda se aplica a todos los socios o sólo a socios internos.
Mi rol es	Indica si la búsqueda es de documentos en los que el socio es el destino o el origen.
ID de empresa de origen	Número de identificación de empresa del socio de origen, por ejemplo, DUNS.
Modalidad de funcionamiento	Producción o prueba. La prueba está disponible sólo en sistemas que tienen soporte para la modalidad de operación de prueba.
Protocolo	Protocolos disponibles para los socios.

Tabla 16. Criterios de búsqueda de RosettaNet (continuación)

Valor	Descripción
Tipo de documento	El proceso empresarial específico.
ID de instancia de proceso	Número de identificación exclusivo asignado para el proceso. Los criterios pueden incluir el comodín asterisco (*).
Ordenar por	Ordena los resultados por: • Fecha y hora de destino • Tipo de documento El valor predeterminado es Indicación de la hora de destino.
Descendente o ascendente	Descendente muestra la indicación de la hora más reciente o el principio del abecedario. Ascendente muestra la hora más antigua o el final del abecedario. El valor predeterminado es Descendente.
Resultados por página	Especifica el número de resultados mostrados por página.

3. Pulse **Buscar**.

Documentos CIDX

CIDX es una asociación comercial y de estándares asentada cuya misión es mejorar la facilidad, velocidad y coste de acometer negocios electrónicos entre compañías químicas y sus socios comerciales. CIDX tiene varias iniciativas que dirigen los estándares de la industria químicas. La iniciativa CIDX de Chem eStandards resulta interesante para el objetivo de este documento. Chem eStandards son los estándares uniformes de intercambio de datos desarrollados específicamente para la compra, venta y entrega de productos químicos. Chem eStandards consta de los siguientes elementos:

- ChemXML o las especificaciones de mensajes de Chem eStandards: v2.0, v2.0.1, v2.0.2, v3.0 y v4.0.
- Especificación Chem eStandards Encelope and Security: v2.0 y v3.0.

Para el empaquetado, CIDX siempre utiliza RNIF 1.1. Es importante tener en cuenta que RNIF 1.1 siempre es asíncrono. Por lo tanto, los intercambios de documentos de CIDX siempre son asíncronos.

CIDX consiste en empaquetados y transacciones mientras que RosettaNet consiste en empaquetados y PIP (procesos de intercambio de socios). CIDX utiliza el empaquetado RNIF 1.1. Las transacciones están definidas por el estándar ChemXML. Cada versión del estándar ChemXML define las transacciones. Todas las transacciones de ChemXML bajo una versión del estándar ChemXML determinada tienen la misma versión que dicho estándar ChemXML. A diferencia de RosettaNet, CIDX no necesita cumplir la definición del proceso. CIDX se centra más con la estructura de la transacción y con el intercambio de mensajes de forma segura.

Continuando con la comparación, RosettaNet es la autoridad administradora del estándar RosettaNet de la misma manera que CIDX es la autoridad administradora del estándar CIDX. RosettaNet define el empaquetado RNIF y los PIP. Los mensajes de RosettaNet pueden utilizar RNIF 1.1 o RNIF 2.0. Los PIP definidos por RosettaNet PIP proporcionan el conjunto de mensajes y la coreografía del proceso. CIDX siempre utiliza RNIF 1.1 como lo define RosettaNet. Ya que CIDX es la entidad administradora, el sobre RNIF necesita ser construido como define la especificación Chem eStandards Envelope and Security. Esta especificación se basa

en la implementación de RosettaNet. CIDX NO utiliza PIP definidos por RosettaNet. En su lugar, CIDX utiliza la especificación de mensajes de Chem eStandards.

Para obtener más información acerca de CIDX, consulte el sitio http://www.cidx.org. Es posible descargar los estándares de CIDX desde esta ubicación: http://www.cidx.org. Chem eStandards Envelope and Security Versión 3.0 puede encontrarse en el sitio http://www.cidx.org/Portals/0/Publications/Envelope_and_Security_v3.0.pdf.

WebSphere Partner Gateway da soporte a los siguientes estándares de Chem eStandards:

- Especificación Chem eStandards Envelope and Security v3.0.
- ChemXML o las especificaciones de mensajes de Chem eStandards v4.0.

Paquetes de tipo de documento RNIF y PIP para CIDX

CIDX utiliza RNIF1.1. Para dar soporte a CIDX, WebSphere Partner Gateway proporciona dos conjuntos de archivos comprimidos denominados paquetes. Se recomienda *paquetes RNIF* constan de definiciones de documento necesarias para dar soporte al protocolo RNIF. Estos paquetes se encuentran en el directorio B2BIntegrate.

Para RNIF V1.1, los paquetes son:

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

El primer paquete proporciona las definiciones de documento necesarias para dar soporte a las comunicaciones de CIDX con los socios y el segundo paquete proporciona las definiciones de documento necesarias para dar soporte a las comunicaciones CIDX con los sistemas de programas de fondo.

El segundo conjunto consiste en paquete de tipo de documento PIP. Cada paquete de tipo de documento PIP tiene un directorio Packages que contiene un archivo XML y un directorio GuidelineMaps que contiene archivos XSD. El archivo XML especifica las definiciones de documento que definen cómo WebSphere Partner Gateway maneja el PIP y define los mensajes y señales intercambiados. Los archivos XSD especifican el formato de los mensajes PIP y definen valores aceptables para elementos XML en los mensajes. Los archivos comprimidos para PIP 0A1 también tienen un archivo XML que el concentrador utiliza como plantilla para crear documentos 0A1.

Para CIDX, WebSphere Partner Gateway proporciona paquetes de tipos de documentos para E41 ChemXML versión 4.0 Order Create y para E42 ChemXML versión 4.0 Order Response.

El convenio de denominación de los paquetes CIDX proporcionados es el mismo que el de los paquetes proporcionados para RosettaNet. Por ejemplo, BCG_Package_RNIF1.1_E414.0.zip es para validar documentos para v4.0 para el PIP E41 enviando entre socios y para WPG utilizando RNIF1.1.

Creación de definiciones de documento

Acerca de esta tarea

Para la mensajería CIDX, WebSphere Partner Gateway requiere los paquetes RNIF para la versión RNIF utilizados para enviar los mensajes. Para cada PIP que WebSphere Partner Gateway da soporte, son necesarios los dos paquetes de tipo de documento PIP para la versión RNIF. Por ejemplo, para dar soporte al PIP E41 en RNIF1.1, WebSphere Partner Gateway necesita los siguientes paquetes:

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip
- BCG_Package_RNIF1.1_E414.0.zip
- BCG_Package_RNSC1.0RNIF1.1_E414.0.zip

El primer paquete da soporte a la mensajería de CIDX con socios y el segundo paquete da soporte a la mensajería de CIDX con sistemas de fondo. El tercer y cuarto paquete permiten que WebSphere Partner Gateway pase mensajes E41 entre los socios y sistemas de fondo.

Para subir los paquetes de CIDX:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse **Subir/descargar paquetes**.
3. Seleccione **No** en **Paquete WSDL**.
4. Pulse **Examinar** y seleccione el paquete RNIF para comunicarse con los socios.

   Los paquetes RNIF se encuentran, de forma predeterminada, en el directorio B2BIntegrate/rosettanet en el soporte de instalación. Por ejemplo, si está subiendo el paquete RNIF versión 2.00, debería ir hasta el directorio B2BIntegrate/Rosettanet y seleccionar: Package_RNIF_V0200.zip.
5. Asegúrese de que **Confirmar en base de datos** se establece en **Sí**.
6. Pulse **Subir**.
7. Pulse de nuevo **Examinar** y seleccione el paquete RNIF para comunicarse con las aplicaciones de programas de fondo.

   Por ejemplo, si está subiendo el paquete RNIF versión 2.00, debería ir hasta el directorio B2BIntegrate/Rosettanet y seleccionar Package_RNSC_1.0_RNIF_V02.00.zip.
8. Pulse **Subir**.

   Los paquetes necesarios para comunicarse con los socios o con el sistema de fondo están ahora instalados en el sistema. Si comprueba la página Gestionar definiciones de documento, verá una entrada para **Paquete: RNIF/Protocolo: RosettaNet**, que representa el empaquetado para la comunicación con los socios y **Paquete: Integración de fondo/protocolo: RNSC**, que representa el empaquetado para comunicarse con las aplicaciones de fondo.
9. Para cada PIP al que desee dar soporte, suba el paquete de tipo de documento PIP del PIP y para la versión de RNIF a la que esté dando soporte.

   Por ejemplo, para subir el PIP de CIDX E41 (Order Create) para que se envíe a un socio, lleve a cabo los siguientes pasos:

   a. Pulse **Examinar** y seleccione **BCG_Package_RNIF1.1_E414.0.zip** en el directorio B2BIntegrate/RosettaNet.
   b. Asegúrese de que **Confirmar en base de datos** se establece en **Sí**.
   c. Pulse **Subir**.

El PIP E41 aparece ahora como tipo de documento por debajo de Paquete: RNIF/Protocolo: RosettaNet en la página Gestionar definiciones de documento. También se visualiza una actividad, acción y dos señales. Se incluyen en la subida del PIP.

Para subir el PIP de E41 para que sea enviado a la aplicación de fondo, lleve a cabo los siguientes pasos:

a. Pulse **Examinar** y seleccione **BCG_Package_RNSC1.0RNIF1.1_E414.0.zip**.
b. Asegúrese de que **Confirmar en base de datos** se establece en **Sí**.
c. Pulse **Subir**.

El PIP E41 aparecerá ahora como el tipo de documento bajo Paquete: Integración de fondo/ Protocolo: RNSC en la página Gestionar definiciones de documento.

Configuración de valores de atributo

Acerca de esta tarea

Para las definiciones de documento RNIF, la mayoría de valores de los atributos ya están definidos y no es necesario configurarlos. Sin embargo, sí es necesario definir los atributos siguientes:

Paquete RNIF (1.1)

- **GlobalSupplyChainCode** - identifique el tipo de la cadena de suministro utilizada por el socio. Los posibles tipos son: componentes electrónicos, tecnología de la información y fabricación de semiconductores. Este atributo no tiene un valor predeterminado.

Para establecer los atributos, realice los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse los iconos **Expandir** para expandir individualmente un nodo al nivel de definición de documento correspondiente o seleccione **Todos** para expandir todos los nodos de definición de documento visualizados.
3. En la columna **Acciones**, pulse el icono **Editar valores de atributo** para el paquete (por ejemplo, Paquete: RNIF (1.1) o Paquete: RNIF (V02.00)) que desea editar.
4. En el apartado **Atributos de contexto de definición de documento**, vaya a la columna **Actualizar** del atributo que desea definir o escriba el nuevo valor. Repita el mismo procedimiento para cada atributo que desee establecer.
5. Pulse **Guardar**.

Nota: también puede actualizar atributos RosettaNet en el nivel de conexión pulsando **Atributos** para el origen o el destino y, a continuación, especificar o cambiar los valores en la columna **Actualizar**. Consulte el apartado "Especificación o cambio de atributos" en la página 248.

Creación de interacciones

Acerca de esta tarea

El siguiente proceso describe cómo crear una interacción entre un sistema de fondo y un socio. Observe que es preciso crear una interacción para cada PIP que se desea enviar y una para cada PIP que se desea recibir.

Antes de comenzar, asegúrese de haber subido las definiciones de documento RNIF correspondientes y de que los paquetes para el PIP que desea utilizar han sido subidos.

Para crear una interacción para un PIP concreto, realice los siguientes pasos:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda el árbol **Origen** hasta el nivel de **Acción** y expanda el árbol **Destino** hasta el nivel de **Acción**.
4. En los árboles, seleccione las definiciones de documento que desea utilizar para el contexto de origen y para el contexto de destino. Por ejemplo, si el socio es el iniciador de un PIP E41, seleccione las siguientes definiciones de documento:

Tabla 17. PIP 3C6 iniciado por un socio

Origen	Destino
Paquete:RNIF(1.1)	Paquete Integración de programas de fondo (1.1)
Protocolo:RosettaNet(1.1)	Protocolo:RNSC(1.0)
Tipo de documento: E41 (4.0)	Tipo de documento: E41 (4.0)
Actividad: OrderCreate	Actividad:OrderCreate
Acción: Creación de pedido	Acción: Creación de pedido

Para un PIP de dos acciones como 3A4 iniciado por un socio, seleccione las siguientes definiciones de documento para la primera acción:

Tabla 18. PIP 3A4 iniciado por un socio

Origen	Destino
Paquete: RNIF (V02.00)	Paquete: Integración de programas de fondo (1.0)
Protocolo: RosettaNet (V02.00)	Protocolo: RNSC (1.0)
Tipo de documento: 3A4 (V02.02)	Tipo de documento: 3A4 (V02.02)
Actividad: Solicitud de pedido de compra	Actividad: Solicitud de pedido de compra
Acción: acción de solicitud de pedido de compra	Acción: acción de solicitud de pedido de compra

5. En el campo Acción, seleccione **Traducción bidireccional de RosettaNet y Contenido de servicio de RosettaNet con validación**.
6. Pulse **Guardar**.

Visualización de documentos de CIDX

Acerca de esta tarea

El Visor de RosettaNet muestra información acerca de los documentos de CIDX. Puede mostrar documentos sin formato y los sucesos y detalles de proceso de documentos asociados mediante criterios de búsqueda específicos. Esta información es útil si está intentando determinar si un documento se ha entregado satisfactoriamente o para determinar la causa de un problema.

Para mostrar el Visor de RosettaNet, lleve a cabo los siguientes pasos:

1. Pulse **Visores > Visor de RosettaNet**.

2. Seleccione los criterios de búsqueda adecuados.
3. Pulse **Buscar**.

documentos ebMS

El mecanismo ebMS proporciona una manera estándar de intercambiar mensajes empresariales entre socios comerciales de ebXML. El servicio de mensajería de ebXML proporciona una manera fiable de intercambiar mensajes empresariales sin tener que depender de tecnologías y soluciones propiedad de terceros. Este apartado muestra cómo configurar las definiciones de documento e interacciones para dichos documentos.

Creación de definiciones de documento

Acerca de esta tarea

La mensajería de ebMS requiere que se cargue un archivo XML CPA (Collaboration Profile Agreement) antes de poder definir los documentos.

Para subir un archivo XML CPA, complete los siguientes pasos:

1. Pulse **Administración del concentrador** > **Configuración del concentrador** > **ebMS**.
2. Pulse **Subir CPA**.
3. Pulse **Examinar** y seleccione el paquete CPA correspondiente.
4. Asegúrese de haber seleccionado **ebMS versión** 2.0.
5. Pulse **Subir**.

Durante el proceso de subida del CPA, se le solicitará que seleccione el socio interno de los socios presentes en el CPA. El socio interno se trata como el gestor en el flujo de ebMS y todos los destinos en el flujo de ebMS para el socio interno se utilizarán para el empaquetado de integración de fondo o N/D. Sin embargo, en la consola el socio aparecerá únicamente como un socio externo.

El ebMS aparece ahora como un paquete así como un protocolo bajo ebMS y Paquete: Integración de fondo en la página Gestionar definiciones de documento.

El flujo de ebMS también puede ser configurado en WebSphere Partner Gateway sin CPA. Para hacerlo, cree definiciones de documento ebMS, funciones B2B desde la consola de WebSphere Partner Gateway tal como se describe en el apartado “Visión general de los tipos de documento” en la página 107. En realidad, al subir el CPA, se realizarán todas las configuraciones automáticamente. En ausencia de CPA, siga los pasos descritos en este apartado.

Configuración de valores de atributo

Acerca de esta tarea

Para definiciones de documento ebMS, la mayoría de los valores de los atributos ya están configurados y no necesitan ser configurados. Sin embargo, sí es necesario definir los atributos siguientes:

paquete ebMS

- **Tiempo para el acuse de recibo en min.**- especifica la cantidad de tiempo que debe esperarse para un acuse de recibo antes de volver a enviar la solicitud

original. Este atributo se utiliza junto con Recuento de reintentos. El intervalo se especifica en minutos. El valor predeterminado es 30.

- **Recuento de reintentos**: especifica el número de veces que debe enviarse una solicitud si no se recibe un acuse de recibo. Este atributo funciona junto con Tiempo de acuse de recibo. El valor predeterminado es 3.
- **Se requiere no rechazo** - especifica si se debe o no almacenar el documento original en el almacén de no rechazo. El valor predeterminado es Sí.

  Nota: En WebSphere Partner Gateway 6.2, la información de no rechazo se obtiene a partir de los parámetros de conexión del socio. Los parámetros de conexión del socio se obtienen después de una comprobación de conexión de socio satisfactoria. De forma predeterminada, el no rechazo está establecido en "Yes", que significa que si la información no está disponible desde la conexión del socio por algún motivo, el documento se colocará en el almacén de no rechazo.
- **Almacén de mensajes necesario** - Establece si almacenar el documento en el almacén de mensajes. El valor predeterminado es Sí.

  Nota: La información del almacén de mensajes se obtiene de los parámetros de conexión del socio. Los parámetros de conexión del socio se obtienen después de una comprobación de conexión de socio satisfactoria. De forma predeterminada, el almacén de mensajes está establecido en "Sí", lo que significa que el documento se mantendrá en el almacén de mensajes.
- **Sin rechazo de recibo** - especifica si desea almacenar el recibo en el almacén de no rechazo. El valor predeterminado es Sí.
- **Intervalo de reintentos** - establece la cantidad de tiempo que el sistema espera entre reintentos. Este atributo se utiliza junto con Recuento de reintentos. El valor predeterminado es 5 minutos.

Para establecer los atributos, realice los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse los iconos **Expandir** para expandir individualmente un nodo al nivel de definición de documento correspondiente o seleccione **Todos** para expandir todos los nodos de definición de documento visualizados.
3. En la columna **Acciones**, pulse el icono **Editar valores de atributo** correspondiente al paquete que desea editar.
4. En el apartado **Atributos de contexto de definición de documento**, vaya a la columna **Actualizar** del atributo que desea definir o escriba el nuevo valor. Repita el mismo procedimiento para cada atributo que desee establecer.
5. Pulse **Guardar**.

Nota: puede también actualizar los atributos de ebMS en el nivel de la conexión pulsando **Atributos** para el origen o destino y, a continuación, entrando o modificando los valores en la columna **Actualizar**. Consulte el apartado “Especificación o cambio de atributos” en la página 248.

Creación de interacciones

Acerca de esta tarea

El siguiente proceso describe cómo crear una interacción entre un sistema de fondo y un socio.

Antes de empezar, asegúrese de haber cargado las definiciones de documento de ebMS correspondientes.

Para crear una interacción para un socio determinado, lleve a cabo los siguientes pasos:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda el árbol Origen hasta el nivel Acción y expanda el árbol Destino hasta el nivel Acción.
4. En los árboles, seleccione las definiciones de documento que desea utilizar para el contexto de origen y para el contexto de destino. Por ejemplo, si el socio es el iniciador de un ebMS, seleccione las siguientes definiciones de documento:

Tabla 19. ebMS iniciado por un socio

Origen	Destino
Paquete: ebMS	Paquete: Integración de programas de fondo (1.0)
Protocolo: ebMS	Protocolo: ebMS
Tipo de documento: ALMService	Tipo de documento: ALMService
Actividad: ALMService	Actividad: ALMService
Acción: Remittance ALMBusiness	Acción: ALMBusiness

Si el sistema de fondo es el iniciador del ebMS, seleccione las siguientes definiciones de documento:

Tabla 20. ebMS iniciado por un sistema de fondo

Origen	Destino
Paquete: Integración de programas de fondo (1.0)	Paquete: ebMS
Protocolo: ebMS	Protocolo: ebMS
Tipo de documento: ALMService	Tipo de documento: ALMService
Actividad: ALMService	Actividad: ALMService
Acción: ALMBusiness	Acción: Remittance ALMBusiness

5. Si lo desea, en el campo Acción seleccione **Dividir y analizar ebMS**.

   La selección de este manejador extraerá las cargas del mensaje ebMS procedentes del socio e introducirá las cargas de nuevo en el flujo como si procediesen del socio de forma independiente. Este manejador no debe ser seleccionado cuando el sistema de fondo es quien inicia el mensaje. Si no está seleccionando este manejador, seleccione Paso a través en el campo Acción
6. Pulse **Guardar**.

   Nota: en algunos flujos ebMS, por ejemplo, en especificaciones STAR, el elemento de servicio ebMS (el valor de Servicio ebMS es el mismo que el valor de WPG Channel Document Flow Definition no es un URI sino una cadena. En tales casos, como por la especificación ebMS 2.0, debe haber presente un atributo de tipo con el elemento de servicio en el mensaje SOAP de ebMS. Por ejemplo, en una especificación STAR, el atributo de tipo debe tener un valor de "STARBOD." Puede configurar tal atributo en el destino de los atributos de definición de flujo de documento. (Consulte la Tabla 22 en la página 146).

Correlación de CPA de ebMS con la configuración de WebSphere Partner Gateway

Acerca de esta tarea

Esta sección proporciona la correlación entre Collaboration Profile Agreement (CPA) y la configuración de la UI de WebSphere Partner Gateway. Las características están enumeradas junto con la configuración de la UI de WebSphere Partner Gateway correspondiente.

1.

Característica
Elemento/Atributo

1.1 CPAId 1

Importado/Configurado manualmente: importado

Configuración de la UI de WebSphere Partner Gateway:

CPAID se configura mediante los canales asociados entre los dos socios. Puede ver el valor accediendo a **Administración de concentrador > ebMS** en la consola de WebSphere Partner Gateway. Pulse Buscar y, a continuación, el icono Ver detalles en los resultados de búsqueda que se muestran.

2.

Característica
Elemento/Atributo

1.2. Estado 1

Importado/Configurado manualmente: importado pero no almacenado en WebSphere Partner Gateway. Tampoco se puede configurar manualmente.

Configuración de la UI de WebSphere Partner Gateway:

Este atributo no se puede configurar en WebSphere Partner Gateway. El valor se comprueba mientras se importa el CPA. Uno de los estados siguientes se muestra mientras se importa:

- Acordado: se puede importar el CPA.
- Firmado: se puede importar el CPA y la firma se verifica antes de la importación.
- Propuesto: no se puede importar el CPA.

3.

Característica
Elemento/Atributo

1.3 Iniciar 1

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Este atributo no se puede configurar en WebSphere Partner Gateway. Sólo se puede establecer desde la importación CPA. Puede ver el valor accediendo a **Administración de concentrador > ebMS** en la consola de WebSphere Partner Gateway. Pulse Buscar y, a continuación, el icono Ver detalles en los resultados de búsqueda que se muestran.

4.

Característica
Elemento/Atributo

1.4 Finalizar 1

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Este atributo no se puede configurar en WebSphere Partner Gateway. Sólo se puede establecer desde la importación CPA. Puede ver el valor accediendo a **Administración de concentrador > ebMS** en la consola de WebSphere Partner Gateway. Pulse Buscar y, a continuación, el icono Ver detalles en los resultados de búsqueda que se muestran.

5.

Característica
Elemento/Atributo

1.5 Restricciones de conversación 0, 1 (9.5) - invocationLimit 0,1 - concurrentConversations 0, 1

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Este atributo no se puede configurar en WebSphere Partner Gateway. Sólo se puede establecer desde la importación CPA. Puede ver el valor accediendo a **Administración de concentrador > ebMS** en la consola de WebSphere Partner Gateway. Pulse Buscar y, a continuación, el icono Ver detalles en los resultados de búsqueda que se muestran.

6.

Característica
Elemento/Atributo

1.6 PartyInfo 2
partyName 1

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Para ver los valores, vaya a **Administración de cuentas > Perfiles > Socio**. Pulse Buscar y, a continuación, el icono Ver detalles en los resultados de búsqueda que se muestran para el socio en CPA.

7.

Característica
Elemento/Atributo

1.6 PartyInfo 2
defaultMshChannelId 1

Importado/Configurado manualmente: importado pero no almacenado en WebSphere Partner Gateway. Tampoco se puede configurar manualmente.

Configuración de la UI de WebSphere Partner Gateway:

Los valores se utilizan mientras se importa el CPA para establecer los atributos de canal para los elementos de señal **Actividad- MSHService** como Ping, Solicitud de estado, MessageError y Acuse de recibo. Estos valores de canal están de nuevo alterados temporalmente si existe algún elemento "OverrideMshActionBinding" en CPA para cualquier elemento de acción específico.

8.

Característica
Elemento/Atributo

1.6 PartyInfo 2
defautMshPackageId 1

Importado/Configurado manualmente: importado pero no almacenado en WebSphere Partner Gateway. Tampoco se puede configurar manualmente.

Configuración de la UI de WebSphere Partner Gateway:

Los valores se utilizan mientras se importa el CPA para establecer los atributos de canal para los elementos de señal **Actividad- MSHService** como Ping, Solicitud de estado, MessageError y Acuse de recibo. Estos valores de canal están de nuevo alterados temporalmente si existe algún elemento "OverrideMshActionBinding" en CPA para cualquier elemento de acción específico.

9.

Característica
Elemento/Atributo

1.6 PartyInfo 2
PartyId 1, *

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Para ver los valores, vaya a **Administración de cuentas > Perfiles > Socio**. Pulse Buscar y, a continuación, el icono Ver detalles en los resultados de búsqueda que se muestran para el socio en CPA.

10.

Característica
Elemento/Atributo

1.6 PartyInfo 2
tipo

Importado/Configurado manualmente: no importado y no se puede configurar.

11.

Característica
Elemento/Atributo

1.6 PartyInfo 2

```
PartyRef 1,*= (8.4.2)
- xlink:type F
- xlink:href 1
- type Fixed
- schemaLocation Implied
```

Importado/Configurado manualmente: no importado y no se puede configurar.

12.

Característica
Elemento/Atributo

1.6 PartyInfo 2

```
1.6.3 CollaborationRole 1,*
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

WebSphere Partner Gateway da soporte a varios elementos de rol de colaboración.

13.

Característica
Elemento/Atributo

1.6 PartyInfo 2

```
.6.3.1 ProcessSpecification 1
- name 1
- version 1
- xlink:type 1
- xlink:href
1 - uuid ImpliedReference 0,*  (8.4.4.6)
- URI 0, 1
 Transforms 1
  Transform
1 - Algorithm Fixed
 DigestMethod 1
  DigestValue 1
```

Importado/Configurado manualmente: no importado.

Configuración de la UI de WebSphere Partner Gateway:

No se puede configurar.

14.

Característica
Elemento/Atributo

1.6 PartyInfo 2

```
1.6.3.2 Rol 1   (8.4.5)
- name 1
- xlink:type Fixed
- xlink:href 1
```

Importado/Configurado manualmente: el atributo **xlink:href** se importa, otros atributos no se importan.

Configuración de la UI de WebSphere Partner Gateway:

El valor se puede configurar en los atributos de canal **Administración de cuentas > Conexiones > Conexiones de socio**. Busque los canales y acceda al atributo de canal - **Rol**.

15.

Característica
Elemento/Atributo

1.6 PartyInfo 2

```
1.6.3.3  ApplicationCertificateRef 0,1  (8.4.6)
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

El valor no se puede configurar. El certificado especificado para el atributo **certId** se carga en el sistema de archivos pero no en WebSphere Partner Gateway.

16.

Característica
Elemento/Atributo

1.6 PartyInfo 2

```
1.6.3.4  ApplicationSecurityDetailsRef 0, 1 (8.4.7)
- securityId 1
```

Importado/Configurado manualmente: no importado.

Configuración de la UI de WebSphere Partner Gateway:

No se puede configurar.

17.

Característica
Elemento/Atributo

1.6.3.5 ServiceBinding 1

```
1.6.3.5.1 Servicio 1 (8.4.9)
- type  Implied
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

- **Servicio**: es el nombre de la definición del documento. Para ver el valor, vaya a **Administración de concentrador > Definiciones de documento**. El valor

Servicio se mostrará como Tipo de documento y Actividad en el paquete ebMS y en el paquete de integración de programas de fondo.

- **Tipo**: tipo se utiliza como el atributo de canal en **Administración de cuentas > Conexiones > Conexiones de socio**. Busque los canales y acceda al atributo del canal **Tipo de servicio**.

18.

Característica
Elemento/Atributo

1.6.3.5 ServiceBinding 1

```
1.6.3.5.1 Servicio 1 (8.4.9)
- type  Implied
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

- **Servicio**: es el nombre de la definición del documento. Para ver el valor, vaya a **Administración de concentrador > Definiciones de documento**. El valor Servicio se mostrará como Tipo de documento y Actividad en el paquete ebMS y en el paquete de integración de programas de fondo.
- **Tipo**: tipo se utiliza como el atributo de canal en **Administración de cuentas > Conexiones > Conexiones de socio**. Busque los canales y acceda al atributo del canal **Tipo de servicio**.

19.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
ThisPartyActionBinding 1
- action 1
- packageId 1
- xlink:href  Implied -
xlink:type Fixed
BusinessTransactionCharacteristics 1
- isNonRepudiationRequired
  All implied
isNonRepudiationReceiptRequired
- isConfidential
- isAuthenticated
- isAuthorizationRequired
- isTamperProof
- isIntelligibleCheckRequired
- timeToAcknowledgeReceipt
- timeToAcknowledgeAcceptance
- timeToPerform
- retryCountChannelId 1,*
ActionContext 0, 1
- binaryCollaboration 1
- businessTransactionActivity 1
- requestOrResponseAction 1
CollaborationActivity 0, 1
- name 1
OtherPartyActionBinding 0, 1
CanReceive 0, 1
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

- **CanSend** – Se crea un canal de **Integración de fondo > ebMS > Nombre de servicio > Acción del socioA** a **ebMS > Nombre de servicio > Acción del socioB** (teniendo el socioB el elemento **CanReceive** que se limita a través del elemento **OtherPartyActionBinding**).
- **Acción** – Importado y creado como un elemento de Acción bajo **Actividad** en definición de documento.
- **packageId** – Los atributos del ID del paquete de referencia se almacenan como atributos de canal.
- Xlink:href y xlink:type: No importados y no se pueden configurar.
- **isNonRepudiationRequired, isNonRepudiationReceiptRequired, isIntelligibleCheckRequired, timeToAcknowledgeReceipt, timeToPerform**: Estos atributos están configurados como atributos de canal.
- **isConfidential, isAuthenticated, isTamperProof, isAuthorizationRequired, timeToAcknowledgeAcceptance, retryCount** - No están importados y no se pueden configurar.
- **ChannelId** 1, * : Sólo se acepta un valor para WebSphere Partner Gateway. Los atributos de referencia se establecen como atributos de canal.
- **binaryCollaboration, businessTransactionActivity, requestOrResponseAction, CollaborationActivity** – No se importan y no se pueden configurar.
- **OtherPartyActionBinding** - Importado. La referencia se utiliza para crear el canal.
- **CanReceive** - Importado y se trata como síncrono si existe otro canal para la misma conexión.

20.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.3.5.3 CanReceive 0, *  (8.4.11)
ThisPartyActionBinding 1
OtherPartyActionBinding 0, 1
CanSend 0, 1
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

- **CanReceive** – Se crea un canal en **ebMS > Nombre de servicio > Acción del socioA** en **Integración de fondo > ebMS > Nombre de servicio > Acción del socioB** (teniendo el socioB el elemento **CanSend** que se limita a través del elemento **OtherPartyActionBinding**).
- **OtherPartyActionBinding** - Importado. La referencia se utiliza para crear el canal.
- **CanSend** - Importado y se trata como síncrono si existe otro canal para la misma conexión.

21.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.4 Certificate 1, * (8.4.18)
- certId  KeyInfo
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Los certificados se almacenan en el sistema de archivos y se deben cargar manualmente en WebSphere Partner Gateway en **Administración de cuentas > Perfiles > Certificados**.

22.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.5 SecurityDetails 0, *   (8.4.18)
- securityId 1 TrustedAnchor 0, *
AnchorCertificateRef 1, *
SecurityPolicy 0, 1
```

Importado/Configurado manualmente: no importado. Sólo los certificados de referencia se cargan en el sistema de archivos.

23.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.6 DeliveryChannel 1, * (8.4.22)
- channelId 1
- transportId 1
- docExchangeId1
MessagingCharacteristics 1
- syncReplyMode All implied
- ackRequested attribute
- ackSignatureRequested
- duplicateElimination
- actor
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

- **channelId**: Los atributos de referencia se establecen como atributos de canal.
- **transportId**: Los atributos de referencia se utilizan para crear la pasarela y se establece como la pasarela predeterminada para el canal.
- **docExchangeId**: Los atributos de referencia se establecen como atributos de canal.
- **syncReplyMode, ackRequested, ackSignatureRequested, duplicateElimination, actor**: estos atributos se importan y configuran como atributos de canal.

24.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.7 Transport 1, * (8.4.24)
- transportId 1
TransportSender 0, 1 (8.4.25)
TransportProtocol 1
- version 1
ImpliedAccessAuthentication 0, *
TransportClientSecurity 0, 1
TransportSecurityProtocol 1
- version 1
ImpliedClientCertificateRef  0, 1
- certId 1
ServerSecurityDetailsRef 0, 1
- securityId 1
EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

Importado/Configurado manualmente: no importado.

25.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.7 Transport 1, * (8.4.24)
TransportReceiver 0, 1 (8.4.33)
TransportProtocol 1
- version 1
ImpliedEndpoint 1, *
- uri 1
- type  ImpliedAccessAuthentication 0, *
TransportServerSecurity 0, 1
TransportSecurityProtocol 1
- version 1
ServerCertificateRef 1
- certId 1
ClientSecurityDetailsRef 0, 1
- SecurityId 1
EncryptionAlgorithm 0, *
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

- **Protocolo de transporte**: define el protocolo de pasarela.
- **Versión**: define la versión del protocolo de pasarela.
- **URL**: define el URL de la pasarela. Estos valores se pueden ver en **Administración de cuentas > Perfiles > PartnerSearch**. Para todos los socios y para el socio seleccionado, pulse la pestaña **Destinos**. Los valores de atributo restantes no se importan.

26.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.8 DocExchange (8.4.39)
- docExchangeId 1 1.6.8.2.1
ebXMLSenderBinding 0, 1 (8.4.40)
- version ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
PersistDuration 0, 1
SenderNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1 Implied
HashFunction 1
SignatureAlgorithm 1
- oid All implied
- w3c
- enumeratedType
SigningCertificateRef 1
- certId 1
SenderDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1  EncryptionAlgorithm 1
- minimumStrength All Implied
- oid
- w3c
- enumeratedType
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm: estos valores se importan y almacenan como atributos de canal, presentes en **Administración de cuentas > Conexiones > Conexiones de socio**. Busque los canales y vaya a **Atributos de canal**. Los valores restantes no están importados y no se pueden configurar.

27.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.8.2 ebXMLReceiverBinding 0, 1 (8.4.53)
- version 1
ReliableMessaging 0, 1
Retries 0, 1
RetryInterval 0, 1
MessageOrderSemantics 1
ReceiverNonRepudiation 0, 1
NonRepudiationProtocol 1
- version 1
HashFunction 1
SigningAlgorithm 1
- oid All Implied
- w3c
- enumeratedType
SigningSecurityDetailsRef 1
- securityId 1
ReceiverDigitalEnvelope 0, 1
DigitalEnvelopeProtocol 1
- version 1
EncryptionAlgorithm 1
- minimumStrength All Implied
```

```
- oid
- w3c
- enumeratedType
EncryptionCertificateRef 1
- certId 1
NamespaceSupported 0, *
- location 1
- version Implied
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm: estos valores se importan y almacenan como atributos de canal, presentes en **Administración de cuentas > Conexiones > Conexiones de socio**. Busque los canales y vaya a **Atributos de canal**. Los valores restantes no están importados y no se pueden configurar.

28.

Característica
Elemento/Atributo

```
1.6.3.5.2 CanSend 0, * (8.4.10)
        1.6.9  OverrideMshActionBinding 0, *  (8.4.58)
        - action 1
        - channelId
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Para la acción especificada, los atributos de canal se establecen mediante el ID de canal de referencia.

29.

Característica
Elemento/Atributo

```
1.6.3.5.2 CanSend 0, * (8.4.10)
        1.7 SimplePart (8.5)
        - id 1
        - mimetype 1
        - mimparameters  Implied
        - xlink:role
         ImpliedNamespaceSupported 0, *
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Mimetype : los valores se importan y almacenan como atributos de canal. Los valores restantes no están importados y no se pueden configurar.

30.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.8 Packaging (8.6)
- id 1
ProcessingCapabilities 1, *
- parse 1
- generate 1
CompositeList 0, *
Composite 0, *
- mimetype 1
- id 1
- mimeparameters ImpliedConstituent 1, *
- idref 1
- excludeFromSignature Implied
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Composite : mimetype, mimeparameters, Constituent-idref, Constituent-excludeFromSignature, signatureTransform, encryptionTransform, Algorithm: estos valores se importan y almacenan como atributos de canal en **Administración de cuentas > Conexiones > Conexiones de socio**. Busque los canales y vaya a **Atributos de canal**. Los valores restantes no están importados y no se pueden configurar.

31.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
Encapsulation 0, *
- mimetype 1
- id 1
- mimeparameters  ImpliedConstituent 1
- idref 1
- excludeFromSignature Implied
- minOccurs Implied
- maxOccurs Implied
SignatureTransform 0, 1
Transform 1, *
EncryptionTransform 0, 1
Transform 1, *
```

Importado/Configurado manualmente: importado.

Configuración de la UI de WebSphere Partner Gateway:

Encapsulation : mimetype, mimeparameters, Constituent-idref, Constituent-excludeFromSignature, signatureTransform, encryptionTransform, Algorithm: estos valores se importan y almacenan como atributos de canal en **Administración de cuentas > Conexiones > Conexiones de socio**. Busque los canales y vaya a **Atributos de canal**. Los valores restantes no están importados y no se pueden configurar.

32.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.9 Signature 0, 1 (8.7)
ds:Signature 1,3
SignedInfo 1
CanonicalizationMethod 0, 1
SignatureMethod 1
- AlgorithmReference 1, *
- URI FixedTransforms 1
Transform 1
- Algorithm Fixed
```

Importado/Configurado manualmente: no importado.

Configuración de la UI de WebSphere Partner Gateway:

No se puede configurar.

33.

Característica
Elemento/Atributo

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.10 Comments 0, * (8.8)
- xml:lang
```

Importado/Configurado manualmente: no importado.

Configuración de la UI de WebSphere Partner Gateway:

No se puede configurar.

Atributos de conexión

La tabla siguiente proporciona los atributos de objeto de direccionamiento, que se pueden ver en los canales de empresa del mensaje en el empaquetado ebMS.

Pulse **Administración de cuentas > Conexiones > Conexiones de socio** y seleccione Origen y Destino. Si el canal es para mensajes ebMS de entrada, pulse **Atributos** de origen, si el canal es para mensajes ebMS de salida, pulse **Atributos** de destino. Desplácese hacia abajo en la pantalla de resultados y pulse la carpeta **Acción**.

Tabla 21. Atributos de conexión

Atributos XML de CPA	Valor predeterminado	Valores posibles	Texto que se muestra en WebSphere Partner Gateway
isNonRepudiationRequired	False	True/false - correlacionado como Sí/No	No rechazo necesario
isNonRepudiationReceiptRequired	False	True/false - correlacionado como Sí/No	Sin rechazo de recibo
timeToAcknowledgeReceipt			Tiempo de acuse de recibo
Retries	3	Algún número	Recuento de reintentos
MessageOrderSemantics	No garantizado	"Guaranteed" "NotGuaranteed"	Semántica de orden de mensaje
PersistDuration	P1D		Duración continua

Tabla 21. Atributos de conexión (continuación)

Atributos XML de CPA	Valor predeterminado	Valores posibles	Texto que se muestra en WebSphere Partner Gateway
syncReplyMode	Ninguno	"mshSignalsOnly" "signalsOnly" "responseOnly" "signalsAndResponse" "none" (trasladado a fase 2)	Modalidad de respuesta sínc.
ackRequested	Por mensaje	"always" - implica que se debe solicitar siempre el acuse de recibo. "never" - implica que nunca se debe solicitar el acuse de recibo. “perMessage” - implica que se puede o no solicitar el acuse de recibo dependiendo del elemento ack presente en el documento ebXML.	Acuse de recibo solicitado
ackSignatureRequested	Por mensaje	"always" "never" "perMessage"	Firma de acuse de recibo solicitada
duplicateElimination	Por mensaje	"always" "never" "perMessage"	Eliminación de duplicados
Actor	"urn:oasis:names:tc:ebxml-msg:actor:nextMSH"	"urn:oasis:names:tc:ebxml-msg:actor:nextMSH""urn:oasis:names:tc:ebxml-msg:actor:toPartyMSH"	Actor
PartyRole	-	Rol en CPA	Rol
Intervalo de reintentos	270	-	Intervalo de reintentos
NonRepudiationProtocol	-	http://www.w3.org/2000/09/xmldsig#	Protocolo de firma
SignatureAlgorithm	-	1. http://www.w3.org.2000/09/xmldsig#dsa-sha1 2. http://www.w3.org/2000/09/xmldsig#rsa-sha1 **Nota:** En ebMS, no se da soporte a hmac-sha1.	Algoritmo de firma
isEncryptionRequired	No	True/false - correlacionado como Sí/No	EncryptionRequired
isCompressionRequired	No	True/false - correlacionado como Sí/No	Compresión necesaria
/Packaging/CompositeList /Encapsulation/Constituent: mimetype	-		Compresión Mimetype
/tp:SenderDigitalEnvelope /tp:DigitalEnvelopeProtocol	-	SMIME XMLEncryption	EncryptionProtocol

Tabla 21. Atributos de conexión (continuación)

Atributos XML de CPA	Valor predeterminado	Valores posibles	Texto que se muestra en WebSphere Partner Gateway
/tp:SenderDigitalEnvelope /EncryptionAlgorithm	-	3des-cbc, aes128-cbc, aes-256-cbc	Algoritmo de cifrado
/tp:ReceiverDigitalEnvelope /tp:DigitalEnvelopeProtocol	-	SMIME XMLEncryption	EncryptionProtocol
/tp:ReceiverDigitalEnvelope /EncryptionAlgorithm	-	3des-cbc, aes128-cbc, aes-256-cbc	Algoritmo de cifrado
/Packaging/CompositeList /Encapsulation tp:MimeType	-	text/xml application/pkcs7-mime	Tipo Mime de cifrado
/Packaging/CompositeList /Encapsulation- tp:mimeparameters	-		Parámetro Mime de cifrado
/Packaging/CompositeList /Encapsulation/Constituent: mimetype	-		Constituyente de cifrado
/Packaging/CompositeList / Composite/ tp:mimeparameters	-		Parámetro Mime de paquete
/Packaging/CompositeList / Composite /Constituent: mimetype	-		PackagingConstituent
/Packaging/CompositeList /Composite/Contituent /excludeFromSignature: mimetype	-		Excluir de firma
/Packaging/CompositeList / Composite/Contituent/ SignatureTransform	-	1. BASE64 2. ENVELOPED 3. XPATH 4. XPATH2 5. XSLT	Algoritmo de transformación de firma
/Packaging/CompositeList /Composite/Contituent/ EncryptionTransform	-	1. BASE64 2. ENVELOPED 3. XPATH 4. XPATH2 5. XSLT	Algoritmo de transformación de cifrado

Limitaciones

Las siguientes son las limitaciones de la correlación de CPA con WebSphere Partner Gateway:

1. Los certificados de CPA no se importan en WebSphere Partner Gateway. Están almacenados en el sistema de archivos y el administrador tiene que verificar manualmente estos certificados y subirlos a WebSphere Partner Gateway.
2. WebSphere Partner Gateway puede direccionar los flujos síncronos y asíncronos de CPA, pero no varios enlaces que tengan el mismo valor de acción.
3. Sólo hay soporte para ID de DUNS numéricos de 9 dígitos (no hay soporte para formato libre).

Correlación de las cabeceras SOAP de ebMS con las cabeceras de WebSphere Partner Gateway

La especificación 2.0 de ebMS define un conjunto de cabeceras que es obligatorio que estén presentes en el mensaje SOAP de ebMS. La siguiente tabla proporcionará la correlación entre algunas de dichas cabeceras obligatorias de ebMS y las cabeceras de WebSphere Partner Gateway de las cuales toman sus valores.

Tabla 22. Cabeceras SOAP de ebMS y sus cabeceras de WebSphere Partner Gateway correspondientes

Núm. serie	Nombre de cabecera en mensaje SOAP de ebMS	Nombre de cabecera correspondiente en WebSphere Partner Gateway
1	From PartyId	"x-aux-sender-id" establecido por el sistema de fondo
2	De rol	Atributo Rol en el lado de origen de los atributos de definición de documento
3	From PartyId Type	El usuario no puede configurarlo. Si PartyId es DUNS, el valor de "type" será "urn:duns". En caso contrario, será "string".
4	To PartyId	"x-aux-receiver-id" establecido por el sistema de fondo
5	A rol	Atributo Rol en el lado de destino de los atributos de Definición de documento.
6	To PartyId Type	El usuario no puede configurarlo. Si PartyId es DUNS el valor de "type" será "urn:duns", en caso contrario será "string"
7	CPAId	Si hay un CPA presente en la base de datos, WebSphere Partner Gateway utilizará el CPA-ID presente en el CPA. En caso contrario, el usuario puede configurar el atributo de ID de CPA presente en el lado de destino de los atributos de definición de documento. Si el usuario no ha configurado este atributo y no hay un CPA presente, WebSphere Partner Gateway generará un ID de CPA basado en los ID del socio.
8	ID de conversación	"x-aux-process-instance-id" establecido por el sistema de fondo. Si el sistema de fondo no lo especifica, WebSphere Partner Gateway generará su propio Conversation ID (ID de conversación).
9	Service	El valor de la definición de documento en la conexión del socio de destino. **Nota:** la definición de documento y la actividad serán la misma en un flujo ebMS.
10	Service Type	Atributo ServiceType en el lado de destino de los atributos de definición de documento
11	Acción	El valor de Acción en la conexión de socio de Destino
12	MessageId	"x-aux-msg-id" establecido por el sistema de fondo. Si el sistema de fondo no lo especifica, WebSphere Partner Gateway generará su propio Message ID (ID de mensaje).

Si está enviando una respuesta síncrona de ebMS a un documento de solicitud de ebMS, el sistema de fondo necesita establecer la cabecera "x-aux-request-msg-id" con el documento de respuesta. El valor de esta cabecera será el ID de mensaje del mensaje de solicitud. Además, el documento de respuesta debe estar en la misma conversación que el documento de solicitud. Esto quiere decir que el "x-aux-process-instance-id" de la respuesta debe ser el mismo que el ConversationId de la solicitud.

El ConversationId y MessageId del documento de solicitud se envían al programa de fondo como "x-aux-process-instance-id" y "x-aux-msg-id", respectivamente.

Visualización de documentos ebMS

Acerca de esta tarea

El Visor de ebMS muestra información acerca de documentos de ebMS. Puede mostrar documentos sin formato y los sucesos y detalles de proceso de documentos asociados mediante criterios de búsqueda específicos. Esta información es útil si está intentando determinar si un documento se ha entregado satisfactoriamente o para determinar la causa de un problema.

Para mostrar el Visor de ebMS, lleve a cabo los siguientes pasos:

1. Pulse **Visores > Visor de ebMS**.
2. Seleccione los criterios de búsqueda adecuados.
3. Pulse **Buscar**.

En el Visor de ebMS, los documentos se organizan en base al ID de conversación. Esto quiere decir que todos los documentos con el mismo ID de conversación serán agrupados y podrán ser vistos pulsando el icono Más detalles en la parte izquierda de cada fila del ID de conversación. Cuando pulse sobre el icono Más detalles, aparecerá una nueva página que muestra todos los mensajes en dicha conversación. En la parte superior de la página, existe un atributo llamado "Estado de conversación". El valor de este atributo es el siguiente mensaje esperado en dicha conversación.

Solicitud de estado de un mensaje ebMS

Acerca de esta tarea

Para solicitar el estado de un mensaje de ebMS, lleve a cabo los siguientes pasos:

1. Después de haber encontrado el documento ebMS que le interesa, pulse el icono **Ver detalles** junto al mismo.
2. Pulse Solicitar estado. Aparecerá entonces el estado de dicho documento.

Para renovar el estado, pulse **Ver estado**.

Cuando realice una configuración para documentos de solicitud de estado y de respuesta de estado de ebMS, tenga en cuenta la información siguiente:

- Sólo se tiene que crear la conexión de solicitud de estado. La conexión de respuesta de estado utilizará la conexión de solicitud de estado.
- En el caso de una conexión de solicitud de estado desde el socio interno hasta un socio externo, el destino del origen de la conexión no se utiliza.
- En el caso de una conexión de solicitud de estado desde un socio externo hasta un socio interno, el destino del origen de la conexión se utiliza para enviar el documento de respuesta de estado de vuelta al socio externo.
- Si un usuario no dispone de CPA, dicho usuario tendrá que habilitar las funciones B2B y crear un canal para el mensaje de solicitud de estado, tal como se indica a continuación:
  - En el caso del mensaje de solicitud de estado de ebMS de entrada, la posibilidad B2B de origen debería ser:

    Paquete: N/D (N/D)
    Protocolo: ebMS (2.0)
    Tipo de documento: MSHService (2.0)
    Actividad: MSHService (2.0)
    Acción: StatusRequest(N/A)

La posibilidad B2B de destino debería ser:

Paquete: ebMS (2.0)
Protocolo: ebMS (2.0)
Tipo de documento: MSHService (2.0)
Actividad: MSHService (2.0)
Acción: StatusRequest(N/A)

– En el caso del mensaje de solicitud de estado de ebMS de salida, la posibilidad B2B de origen debería ser:

Paquete: ebMS (2.0)
Protocolo: ebMS (2.0)
Tipo de documento: MSHService (2.0)
Actividad: MSHService (2.0)
Acción: StatusRequest(N/A)

La posibilidad B2B de destino debería ser:

Paquete: N/D (N/D)
Protocolo: ebMS (2.0)
Tipo de documento: MSHService (2.0)
Actividad: MSHService (2.0)
Acción: StatusRequest(N/A)

Entonces el usuario debe activar el canal y establecer los destino desde la página de conexión del socio.

Nota: Esta información contiene el valor true para el error de ebMS y Acknowledgement. La acción de estos canales cambiará a MessageError y Acknowledgment, respectivamente.

Ejecución de ping con socios ebMS

Acerca de esta tarea

Desde la página de conexión a Test Partner, puede hacer ping a los socios ebMS. Esto quiere decir que puede enviar un mensaje ping a un socio y, si el socio está preparado para recibir, el socio responderá con un mensaje pong. Una vez suba un CPA, se creará el canal ping-pong.

Para que Ping pueda trabajar, las conexiones deben definirse con el socio involucrado. Para obtener más información, consulte la sección de ejecución de ping para los socios ebMS en la *Guía de configuración del concentrador de WebSphere Partner Gateway*.

Para ejecutar ping a un socio ebMS, realice los pasos siguientes:

1. Pulse **Herramientas** > **Probar conexión de socio**.
2. Para **Mandato**, seleccione **PING ebMS**.
3. Seleccione **Socio de origen** y **Socio de destino**.
4. Opcionalmente, seleccione un **Destino** o escriba un **URL**.
5. Pulse **Probar** para enviar un mensaje ping.

Para determinar el estado del mensaje ping, pulse **Estado de ping**. El estado de la última solicitud de ping se muestra bajo Resultados.

Nota: La última solicitud de ping debería haberse iniciado desde la conexión de Test Partner o desde un reenvío del visualizador de documentos de un documento de ping.

servicios web

Un socio puede invocar un servicio web que albergue el socio interno. De forma similar, el socio interno puede invocar un servicio web albergado por un socio. El socio o socio interno invoca el servicio web a través del servidor de WebSphere Partner Gateway. WebSphere Partner Gateway actúa como proxy, transmitiendo la solicitud de servicio web al proveedor de servicios web y devolviendo la respuesta de manera síncrona del proveedor al solicitante.

Este apartado contiene la información siguiente para configurar un servicio web para su utilización por parte de un socio o de un socio interno:

- Identificación de los socios de un servicio web.
- Configuración de una definición de documento para un servicio web.
- Adición de definiciones de documento a las funciones B2B de los socios.
- Restricciones y limitaciones del soporte de servicio web.

Identificación de los socios de un servicio web

Cuando un El socio interno proporciona el servicio web para que lo utilicen los socios; WebSphere Partner Gateway requiere identificación tanto de los socios internos como de los externos. En WebSphere Partner Gateway existe la posibilidad de crear varios socios internos, uno de los cuales se establece como socio interno predeterminado. Para sobrescribir el socio interno predeterminado y seleccionar un socio interno, envíe parámetros adicionales al receptor de WebSphere Partner Gateway, como **FromPartnerBusinessId** o **ToPartnerBusinessId** en función del flujo entrante o saliente respectivamente. La condición de error es que si dos ID de socios externos se proporcionan a través de autenticación básica y URL, la autenticación básica tiene preferencia. Las varias series de consulta para el flujo externo son: `<URL-Receptor>?to=<ID de empresa>` and `<URL-Receptor?to=<ID de empresa>&from=<ID de empresa>`. Las varias series de consulta posibles para el flujo interno son:`<URL_receptor` y `URL_receptor?to=ID de empresa`. En caso de entrada, la **autenticación básica** es obligatoria.

Creación de definiciones de documento

Para configurar la definición de documento, debe subir los archivos WSDL (Web Service Definition Language) que definen el servicio web o bien especificar las definiciones de documento equivalentes manualmente a través de la consola.

Subida de archivos WSDL para un servicio web

Acerca de esta tarea

La definición de un servicio web deber estar contenida en un archivo WSDL primario, con la extensión `.wsdl`, que debe importar archivos WSDL adicionales a través del elemento `import`. Si existen archivos importados, estos pueden subirse con el archivo primario utilizando uno de los dos métodos siguientes:

- Si puede accederse a la vía de acceso del archivo o URL (HTTP) en el atributo `location` de cada elemento `import` desde el servidor de la Consola de comunidad (no la máquina del usuario), el archivo primario puede subirse directamente y los archivos importados se subirán automáticamente.

- Si todos los archivos importados y el archivo primario se comprimen en un archivo, cada uno de ellos con la vía de acceso zip correspondiente a la vía de acceso del atributo `location` de la importación (si existe), al subir el archivo comprimido se subirán todos los archivos WSDL primarios e importados que éste contenga.

Por ejemplo, suponga que el archivo WSDL primario `helloworldRPC.wsdl` contiene el siguiente elemento de importación:

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location=
"bindingRPC.wsdl"/>
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location=
"port/porttypeRPC.wsdl"/>
```

Además, suponga que el archivo WSDL importado, `bindingRPC.wsdl`, contiene el siguiente elemento de importación:

El archivo debe contener lo siguiente:

```
Nombre                  Vía de acceso

helloworldRPC.wsdl

bindingRPC.wsdl

porttypeRPC.wsdl              port\
```

Cuando se sube la definición de un archivo WSDL de un servicio web, el WSDL original se guarda como correlación de validación. (Los mensajes de servicio web no están realmente validados frente a WSDL por WebSphere Partner Gateway.) Esto se conoce como WSDL *privado*.

Además, un WSDL público se guarda con el URL privado sustituido por el URL de destino especificado en la página Subir/descargar paquetes. El WSDL público se facilitará a los usuarios del servicio web, que invocarán el servicio web en el URL del destino (el URL público). WebSphere Partner Gateway direccionará entonces la solicitud de servicio web a un destino que sea el URL privado del proveedor del servicio web original. WebSphere Partner Gateway actúa como proxy, enviando la solicitud de servicio web al URL de un proveedor privado, que se oculta del usuario del servicio web.

Tanto los WSDL públicos como privados (incluyendo cualquier archivo importado) pueden ser descargado de la Consola de comunidad después de haber subido el archivo WSDL.

Subir archivos WSDL con la consola de la comunidad: WebSphere Partner Gateway proporciona un método para importar archivos WSDL. Si un servicio web se define en un archivo WSDL individual, puede subir el archivo WSDL directamente. Si el servicio web se define utilizando múltiples archivos WSDL (tal como sucede cuando se han importado archivos WSDL en un archivo WSDL primario), estos se subirían en un archivo comprimido.

Importante: Se recomienda archivos WSDL del archivo comprimido deben estar dentro de un directorio especificado en el elemento de importación de WSDL. Por ejemplo, suponga que tiene el siguiente elemento de importación:

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
location="path1/bindingRPC.wsdl"/>
```

La estructura de directorios dentro del archivo comprimido sería: `path1/bindingRPC.wsdl`.

Considere este ejemplo:

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
 location="bindingRPC.wsdl"/>.
```

El archivo `bindingRPC.wsdl` estaría en el nivel de directorio raíz dentro del archivo comprimido.

Para subir un archivo WSDL o un archivo comprimido individual, siga el procedimiento siguiente.

1. Pulse **Administración del concentrador** > **Configuración del concentrador** > **Definición de documento**.
2. Pulse **Subir/descargar paquetes**.
3. En **Paquete WSDL**, pulse **Sí**.
4. En **URL público de servicio web**, realice uno de los siguientes pasos:
   - En el caso de un servicio web que proporcione el socio interno (que invocará un socio), escriba el URL público del servicio web. Por ejemplo:

     `https://<host_destino:puerto>/bcgreceiver/Receiver`

     El URL suele ser el mismo que el destino HTTP de producción definido en Destinos.
   - En el caso de un servicio web proporcionado por un socio (que invocará el socio interno), escriba el URL público del socio con una serie de consulta. Por ejemplo:

     `https://<target_host:port>/bcgreceiver/Receiver?to=<partner_business_ID>`
5. Pulse **Examinar** y seleccione el archivo WSDL o el archivo comprimido.
6. En **Confirmar en base de datos**, seleccione **No** si desea subir el archivo en modo prueba. Si selecciona **No**, el archivo no se instalará en el sistema. Utilice los mensajes generados por el sistema que aparecen en el recuadro de mensajes para solucionar cualquier error de subida. Seleccione **Sí** para subir el archivo a la base de datos del sistema.
7. En **Sobrescribir datos**, seleccione **Sí** para sustituir un archivo que actualmente se encuentra en la base de datos. Seleccione **No** para añadir el archivo a la base de datos.
8. Pulse **Subir**. El archivo WSDL se instala en el sistema.

Validación de paquetes utilizando archivos de esquema: Un conjunto de esquemas XML que describen los archivos XML que pueden subirse a través de la consola se proporciona en el soporte de instalación de WebSphere Partner Gateway. Los archivos que se suben se validan frente a estos esquemas. Los archivos de esquema son una referencia útil para averiguar la causa de un error cuando un archivo no puede cargarse debido a un XML no adecuado. Los archivos son: `wsdl.xsd`, `wsdlhttp.xsd` y `wsdlsoap.xsd`, que contienen el esquema que describe los archivos WSDL (Web Service Definition Language) válidos.

Los archivos se encuentran en: `B2BIntegrate\packagingSchemas`

Creación manual de la definición de documento

Para especificar definiciones manuales de documentos equivalentes, siga los procedimientos en este apartado. Debe también crear las entradas de Tipo de

documento, Actividad y Acción individualmente bajo **Protocolo: Servicio web**, prestando especial atención a los requisitos de la Acción y a su relación con los mensajes SOAP recibidos.

En términos de la jerarquía Paquete/Protocolo/Tipo de documento/Actividad/Acción de las definiciones de documento, un servicio web soportado está representado como se muestra a continuación:

- **Paquete: Ninguno**
- **Protocolo: Servicio web (1.0)**
- **Tipo de documento:** {*<espacio_nombres_servicio_Web>*:*<nombre_servicio_Web>*} (nombre y código), que debe ser único entre los tipos de documentos del protocolo de servicio web. Suele ser el espacio de nombres y el nombre de WSDL.
- **Actividad:** una actividad para cada operación de servicio web, con nombre y código:

  {*<nombre_espacio_operación>*}:*<nombre_operación>*
- **Acción**: una acción para el mensaje de entrada de cada operación, con nombre y código:

  {*<namespace_of_identifying_xml_element = namespace_of_first_child_of_soap:body>*}:
  <name_of _identifying_xml_element = name_of_first_child_of_soap:body>

Las definiciones clave son las acciones, pues WebSphere Partner Gateway utilizará un espacio de nombres y el nombre de una acción para reconocer un mensaje SOAP de solicitud de servicio web entrante y direccionarlo apropiadamente basándose en la conexión de socio definida. El espacio de nombres y nombre del primer elemento XML hijo del elemento `soap:body` del mensaje SOAP recibido debe coincidir con un espacio de nombres y nombre de acción conocidos en las definiciones de documento de WebSphere Partner Gateway.

Por ejemplo, suponga que un mensaje SOAP de solicitud de servicio web para un enlace SOAP documento-literal es:

```
<?xml version="1.0" encoding="UTF-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd=
"http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
 <soapenv:Body>
  <nameAndAddressElt xmlns="http://www.helloworld.com/xsd/helloDocLitSchema">
   <titleElt xmlns="">Mr</titleElt>
   <nameElt xmlns="">Joe Smith</nameElt>
   <addressElt xmlns="">
    <numberElt>123</numberElt>
    <streetElt>Elm St</streetElt>
    <cityElt>Peoria</cityElt>
   </addressElt>
  </nameAndAddressElt>
 </soapenv:Body>
</soapenv:Envelope>
```

WebSphere Partner Gateway buscaría una acción de servicio web definida con este código:

```
{http://www.helloworld.com/xsd/helloDocLitSchema}:nameAndAddressElt
```

Para un mensaje de solicitud SOAP de estilo de enlace RPC, por ejemplo:

```
<?xml version="1.0" encoding="UTF-8"?>

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd=
"http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
 <soapenv:Body>
  <ns1:helloWorldRPC soapenv:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/ xmlns:ns1="http://www.helloworld.com/helloRPC">
   <name xsi:type="xsd:string">Joe Smith</name>
  </ns1:helloWorldRPC>
 </soapenv:Body>
</soapenv:Envelope>
```

WebSphere Partner Gateway buscaría una acción de servicio web definida con este código:

```
{http://www.helloworld.com/helloRPC}:helloWorldRPC
```

Para un enlace RPC, el espacio de nombres y el nombre del primer elemento hijo de `soap:body` de un mensaje de solicitud SOAP debería ser el espacio de nombres y el nombre de la operación de servicio web aplicable.

Para un enlace documento-literal, el espacio de nombres y el nombre del primer elemento hijo de `soap:body` de un mensaje de solicitud SOAP debería ser el espacio de nombres y el nombre del atributo XML `element` en el elemento `part` de la definición de `message` para el servicio web.

Creación de interacciones

Acerca de esta tarea

Para crear una interacción para un servicio web, deberá utilizar la misma acción de tipo de documento de servicio web para el Origen y el Destino.

Para crear interacciones, siga este procedimiento.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Bajo **Origen**, expanda **Paquete: Ninguno > Protocolo: Servicio web > Tipo de documento: <** *tipo de documento*> **> Acción:** <*acción*>.
4. Repita el paso anterior en la columna **Destino**.
5. Seleccione **Paso a través** en la lista **Acción** al final de la página. (**Paso a través** es la única opción válida soportada en WebSphere Partner Gateway para un servicio web).

Restricciones y limitaciones del soporte de servicio web

WebSphere Partner Gateway soporta los estándares siguientes:

- WSDL 1.1
- SOAP 1.1
- WS-I Basic Profile v. 1.0 (que contiene restricciones importantes como mensajes SOAP para enlaces documento-literal)

Nota:

- WebSphere Partner Gateway tiene soporte parcial para Perfil básico 1.0.
- Se admiten los enlaces SOAP/HTTP.

- No se admite la constitución reiterada de enlaces.
- Se admiten los estilos de enlace RPC-codificado/RPC-literal y documento-literal (según las restricciones de WS-I Basic Profile).

Consulte los apartados “Validación de sobre SOAP” en la página 103 y “Desensobrar SOAP” en la página 104.

documentos de cXML

El Gestor de documentos de WebSphere Partner Gateway identifica un documento cXML por el nombre del elemento raíz del documento XML (es decir `cXML`) y la versión indicada por cXML DOCTYPE (DTD). Por ejemplo, el DOCTYPE siguiente es para cXML, versión 1.2.009:

```
<!DOCTYPE cXML SYSTEM "http://xml.cXML.org/schemas/cXML/1.2.009/cXML.dtd">
```

El Gestor de documentos se encarga de la validación DTD en los documentos de cXML; sin embargo, WebSphere Partner Gateway no proporciona DTD cXML. Puede descargarlos de www.cxml.org y seguidamente subirlos a WebSphere Partner Gateway a través del módulo de correlación de la validación en la Consola de comunidad. Después de subir el DTD, asócielo con el tipo de documento de cXML. Consulte el apartado “Asociación de correlaciones con definiciones de documentos” en la página 170 para obtener más información acerca de cómo asociar el DTD con el tipo de documento cXML.

El Gestor de documentos utiliza dos atributos del elemento raíz cXML para la gestión de documentos: ID de la carga e indicación de la hora. El ID de la carga cXML y la indicación de la hora se utilizan como número de identificación del documento e indicación de la hora del documento. Ambos aparecen en la Consola de comunidad para la gestión de documentos.

Los elementos de procedencia y destino (From y To) de la cabecera cXML contienen el elemento de credencial (Credential) que se utiliza para el direccionamiento y autenticación del documento. Se recomienda ejemplo siguiente muestra los elementos de procedencia y destino (From y To) del documento cXML.

Nota: aquí y en toda esta publicación, los números DUNS sólo se proporcionan como ejemplos.

```
<Header>
<From>

            <Credential domain="AcmeUserId">
                <Identity>admin@acme.com</Identity>
            </Credential>
            <Credential domain="DUNS">
                <Identity>130313038</Identity>
            </Credential>
</From
<To>
            <Credential domain="DUNS">
                <Identity>987654321</Identity>
            </Credential>
            <Credential domain="IBMUserId">
                <Identity>test@ibm.com</Identity>
            </Credential>
</To>
```

Si se utiliza más de un elemento de credencial, el Gestor de documentos utiliza el número DUNS como el identificador de empresa para direccionamiento y autenticación. Si no se indica ningún número DUNS, se utiliza la primera credencial.

WebSphere Partner Gateway no utiliza la información del elemento remitente.

Si la transacción es síncrona, la cabecera de procedencia y destino no se utiliza en un documento de respuesta cXML. El documento de respuesta se envía a través de la misma conexión que se establece mediante el documento de la solicitud.

Tipos de documentos cXML

Existen tres tipos de documento cXML: Request, Response o Message.

Request

Existen muchos tipos de peticiones cXML. El elemento `Request` dentro del documento cXML se corresponde con el tipo de documento en WebSphere Partner Gateway. Estos son algunos elementos de solicitud típicos:

- OrderRequest
- ProfileRequest
- PunchOutSetupRequest
- StatusUpdateRequest
- GetPendingRequest
- ConfirmationRequest
- ShipNoticeRequest

La siguiente tabla muestra la relación entre los elementos en un documento de solicitud cXML y las definiciones de documento dentro de WebSphere Partner Gateway:

Elemento cXML
definición de documento

cXML DOCTYPE
Protocolo

Versión DTD
Versión de protocolo

Request (tipo) Por ejemplo, OrderRequest
Tipo de documento

Response

El socio de destino envía una respuesta cXML para informar al socio de origen de los resultados de la solicitud cXML. Puesto que el resultado de algunas peticiones podrían no tener ningún dato, el elemento `Response` opcionalmente puede contener sólo un elemento `Status`. Un elemento `Response` también puede contener cualquier dato de nivel de aplicación. Durante PunchOut, por ejemplo, los datos de nivel de aplicación se incluyen en un elemento `PunchOutSetupResponse`. Estos son algunos elementos `Response` típicos:

- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

La siguiente tabla muestra la relación entre los elementos en un documento de respuesta cXML y las definiciones de documento dentro de WebSphere Partner Gateway:

Elemento cXML
definición de documento

cXML DOCTYPE
Protocolo

Versión DTD
Versión de protocolo

Response (tipo) Por ejemplo, ProfileResponse
tipo de documento

Mensaje

Un mensaje cXML contiene la información del tipo de documento WebSphere Partner Gateway en el elemento `Message` de cXML. Puede contener un elemento `Status` opcional idéntico al que se encuentra en un elemento `Responsenece`. Se utilizaría en mensajes de respuesta a mensajes de solicitud.

El contenido del mensaje se define según las necesidades empresariales del usuario. El elemento directamente por debajo del elemento `<Message>` corresponde el tipo de documento creado en WebSphere Partner Gateway. En el siguiente ejemplo, SubscriptionChangeMessage es el tipo de documento:

```
<Missatge>
<SubscriptionChangeMessage type="new">
           <Subscripción>
                <InternalID>1234</InternalID>
                <Name xml:lang="en-US">Q2 Prices</Name>
                <Changetime>1999-03-12T18:39:09-08:00</Changetime>
                <SupplierID domain="DUNS">942888711</SupplierID>
                <Format version="2.1">CIF</Format>
            </Subscription>
</SubscriptionChangeMessage>
</Message>
```

La siguiente tabla muestra la relación entre los elementos en un mensaje cXML y las definiciones de documento dentro de WebSphere Partner Gateway:

Elemento cXML
definición de documento

cXML DOCTYPE
Protocolo

Versión DTD
Versión de protocolo

Mensaje
Tipo de documento

La forma más sencilla de diferenciar un mensaje unidireccional de un documento de solicitud y respuesta es la presencia de un elemento `Message` en lugar de un elemento Request-Response.

Un mensaje puede tener los atributos siguientes:

- `deploymentMode`, que indica si el mensaje es un documento de prueba o un documento de producción. Los valores permitidos son producción (valor predeterminado) o prueba.
- `inReplyTo`, que especifica a qué mensaje responde este mensaje. El contenido del atributo `inReplyTo` es el ID de carga de un mensaje recibido anteriormente. Se utilizaría para formar una transacción bidireccional con diversos mensajes.

Cabeceras de tipo de contenido y documentos adjuntos

Todos los documentos de cXML deben incluir una cabecera Content-type. Para los documentos de cXML sin archivos adjuntos, se utilizan las siguientes cabeceras Content-type:

- Content-Type: text/xml
- Content-Type: application/xml

El protocolo cXML permite adjuntar archivos externos a través de MIME. Por ejemplo, los compradores con frecuencia necesitan clarificar los pedidos de compra con informes, dibujos o faxes adjuntos. Para los documentos de cXML que contienen archivos adjuntos debe utilizarse una de las cabeceras Content-type que aparecen en la siguiente lista:

- Content-Type: multipart/related; boundary=<*algo_único*>
- Content-Type: multipart/mixed; boundary=<*algo_único*>

El elemento `boundary` es cualquier texto único que se utiliza para separar la parte del cuerpo de la parte de carga del mensaje MIME. Consulte la publicación cXML User Guide en www.cxml.org para obtener más información.

Interacciones cXML válidas

WebSphere Partner Gateway da soporte a las siguientes interacciones de definición de documento cXML:

- Del socio externo al socio interno: Ninguno/De cXML a Ninguno/cXML con Paso a través y validación
- Del socio interno al socio externo:
  - Ninguno/cXML a Ninguno/cXML con Paso a través y validación.
  - Ninguno/XML a Ninguno/cXML con Paso a través, validación y transformación.

Creación de definiciones de documento

Acerca de esta tarea

Utilice el proceso siguiente para crear una nueva definición de documento para un documento cXML.

Nota: debe asegurarse de haber definido la versión correcta de cXML antes de crear una definición de documento cXML. La versión predeterminada es la 1.2.009.

1. Pulse **Administración del concentrador** > **Configuración del concentrador** > **Definición de documento**.
2. Pulse **>Crear definición de documentos**. Aparecerá la página Crear definiciones de documento.
3. Seleccione **Tipo de documento** para el tipo de documento.
4. Realice una de las siguientes tareas, en función del tipo de documento:

- Para peticiones, especifique el tipo de solicitud (por ejemplo, `OrderRequest`) en el campo **Nombre**.
- Para las respuestas, si la respuesta no tiene más distintivos subordinados que `<Status>`, especifique `Response`. En caso contrario, especifique el nombre de distintivo después de `<Status>`. En el ejemplo siguiente, debe especificar `Response` para el primer elemento Response y `ProfileResponse` para el segundo.

```
<cXML>
    <Response>
        <Status code="200" text="OK"/>
    </Response>
</cXML>
<cXML>
    <Response>
        <Status code="200" text="OK"/>
   </ProfileResponse>
    </Response>
</cXML>
```

5. Especifique **1.0** en **Versión**.

   El número de versión es sólo de referencia. La versión real del protocolo se obtiene a partir de la versión DTD del documento cXML.
6. Especifique una **Descripción** opcional.
7. Seleccione **Sí** en **Nivel de documento**.
8. Seleccione **Habilitado** para **Estado**.
9. Seleccione **Sí** para todos los atributos de **Visibilidad**.
10. Pulse la carpeta **Paquete: Ninguno** para desglosar las opciones de selección del paquete.
11. Seleccione **Protocolo: cXML (1.2.009): cXML**.
12. Pulse **Guardar**.

Creación de interacciones

Acerca de esta tarea

Después de crear la definición de documento, configure una interacción para el documento cXML.

Para crear interacciones, siga este procedimiento.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Si el documento cXML es el origen, bajo **Origen**, expanda **Paquete: Ninguno** y **Protocolo: cXML** y seleccione **Tipo de documento:**<*flujo_documento*>. Si el documento cXML es el destino, expanda **Paquete: Ninguno** y **Protocolo: cXML** y seleccione **Tipo de documento:** <*flujo_documento*> en la columna **Destino** .
4. Expanda la columna de origen o destino para la otra mitad de la interacción (el documento que será convertido a cXML o el documento que será transformado desde cXML) y expanda su paquete y protocolo y seleccione su tipo de documento.
5. Seleccione **Paso a través** en la lista **Acción** al final de la página. (**Paso a través** es la única opción válida soportada para documentos cXML).

Proceso de documentos de XML personalizado

Este apartado describe cómo puede configurar el concentrador para direccionar documentos XML que no sean gestionados por uno de los otros protocolos de direccionamiento incorporados.

XML personalizado es un término de WebSphere Partner Gateway utilizado para hacer referencia a documentos XML no gestionados por uno de los protocolos incorporados.

La manera en que los documentos XML personalizados son identificados es mediante un proceso de eliminación. Basándose en la ordenación de los pasos de análisis de protocolo de flujo de trabajo entrante fijo, el concentrador intenta emparejar los documentos XML con cada uno de los protocolos estándares antes de llamar al paso de análisis de protocolo que gestiona el XML personalizado. El manejador XML personalizado es llamado por cualquier documento XML que no coincida con los tipos de documentos XML estándares.

Para procesar un documento XML personalizado, el analizador de protocolos debe extraer información del documento. La recopilación de formatos XML, definiciones de protocolos de documentos y definiciones de tipo de documento proporciona la información necesaria al analizador de protocolo XML personalizado para que reconozca y procese un documento utilizando la configuración.

Desde un nivel superior, así es como funciona el protocolo XML personalizado:

1. Se analiza el documento XML para obtener cualquiera de los siguientes valores que existen: valor del nombre DTD del documento, espacio de nombres de distintivo de directorio raíz y el nombre de distintivo de directorio raíz.
2. Basándose en los identificadores obtenidos en el primer paso, un conjunto de familias de documentos puede contener formatos XML identificados como una posible coincidencia para el documento. Aprenderá a crear familias de documentos y formatos XML posteriormente en el apartado “Creación de formatos XML” en la página 160.
3. Cada posible coincidencia de formato XML de las familias se aplica al documento para ver si coincide con el documento. Las coincidencias se describen más adelante en este apartado.
4. Cuando se encuentra un formato XML coincidente, se utiliza para extraer datos del documento que el concentrador utiliza para procesar el documento. La familia de documentos de la cual el formato XML coincidente es miembro determina el protocolo de documento utilizado para el direccionamiento. El formato XML coincidente determina el tipo de documento utilizado para el direccionamiento.

Utilizando la página Gestionar protocolos XML, puede crear familias de documentos que estén asociadas con protocolos de documentos. A continuación puede rellenar las familias de formato con formatos XML que estén asociados con tipos de documentos.

Un formato XML se compone de dos tipos de información:

- Expresiones XPath utilizadas para extraer información de documentos XML.
- Datos literales utilizados como un valor constante.

Los formatos XML son utilizados por el Gestor de documentos para recuperar los valores que identifican de forma exclusiva un documento entrante y acceden a la información dentro del documento necesaria para su correcto direccionamiento y proceso.

La configuración de un direccionamiento XML personalizado es un proceso de varios pasos. Para llevarlos a cabo, debe completar lo siguiente:

1. Cree un protocolo que será utilizado para direccionar un conjunto de documentos relacionados y asócielo con un o varios paquetes.
2. Cree un tipo de documento para el formato y asócielo con el protocolo recién creado.
3. Cree una familia de documentos para que contenga un conjunto de formatos XML que coincidan con los documentos que se direccionarán con el protocolo.
4. Añada formatos XML a la familia que estén asociados con cada uno de los tipos de documentos del protocolo de familia.

A continuación, cree interacciones entre los nuevos tipos de documentos para que puedan establecerse conexiones.

Estos pasos se describen en los apartados siguientes. También puede encontrar un ejemplo de estos pasos en el apartado "Establecimiento del concentrador para documentos XML personalizados" en la página 335.

Creación de formatos XML

Los formatos XML se utilizan para identificar y extraer datos de documentos XML personalizados para que puedan ser procesados. Los formatos XML se encuentran dentro de las familias de documentos. Una familia de documentos es una recopilación de formatos XML relacionados que comparten un nombre DTD, un distintivo de elemento de directorio raíz o un espacio de nombres de elemento de directorio raíz comunes. Por lo tanto, hay tres tipos de familias de documentos: familias DTD, familias de distintivos de directorio raíz y familias de espacios de nombres.

Las familias de documentos tienen dos roles:

- Pueden determinar cómo se direcciona un documento. Durante el tiempo de ejecución, cuando un documento coincide con un formato XML, el protocolo de direccionamiento y la versión asociados con la familia de formato son utilizados para direccionar un documento.
- Pueden ayudar a organizar los formatos XML en el sistema. Cuando esté configurando el sistema, puede organizar los formatos XML por familias. Por ejemplo, puede agrupar los mensajes de compra en una familia llamada Mensajes de compra y, a continuación, buscar una familia de documentos para acceder a los formatos que se encuentren en una familia en particular.

Creación de una familia de documentos

Acerca de esta tarea

Para agrupar los formatos XML relacionados en una familia, debe primero crear una familia. Para crear una familia de documentos, lleve a cabo lo siguiente:

1. Pulse **Administración del concentrador** > **Configuración del concentrador** > **Formatos XML**.
2. Pulse **Crear familia de documentos**.
3. En la vista Nueva familia de documentos, especifique un **Nombre de familia**.

Nota: más de una familia puede tener el mismo identificador o nombre. El tipo de identificador combinado con el nombre forma una clave de familia única. Por ejemplo, supongamos que desea direccionar mensajes SOAP utilizando el manejador XML personalizado. Si tiene distintos tipos de mensajes SOAP, puede clasificarlos en familias con distintos nombres que tengan todas Sobre como el identificador de distintivo de directorio raíz.

4. Seleccione un **Protocolo** en la lista de protocolos disponibles en el sistema. Debe definir un protocolo personalizado antes de definir la familia que va a usarlo. No puede cambiar el protocolo de una familia después de crear la familia, por lo que es conveniente planificarlo de antemano.
5. Seleccione **Opción de archivo grande**: Ninguno, Utilizar procesador de archivos grandes o Utilizar procesador de archivos grandes con reconocimiento de espacio de nombres.

   Ninguno significa que los formatos XML de la familia pueden utilizar las expresiones XPath, versión 1.0, pero el tamaño de los archivos que se pueden procesar estarán limitados por varios factores, incluida la configuración de la memoria del gestor de documentos, la carga de trabajo del gestor de documentos y la estructura de los documentos procesados.

   Utilizar procesador de archivos grandes o **Utilizar procesador de archivos grandes con reconocimiento de espacio de nombres** quiere decir que el tamaño de archivo no es una limitación pero que está limitado a utilizar expresiones de vía de acceso de elemento sencillo en los formatos XML que sean miembros de la familia.

   Utilice una opción de archivos grandes si está escribiendo formatos XML que coinciden con documentos de gran tamaño que no pueden ser gestionados utilizando el procesador XPath completo. Si selecciona la opción con reconocimiento de espacio de nombres, las vías de acceso de los elementos incluirán prefijos de espacios de nombres cuando aparezcan en un documento.
6. Seleccione un **Tipo de familia** de documento en la lista: DTD, Distintivo de directorio raíz o Espacio de nombres.
7. Especifique un **Identificador de familia** para el tipo de familia que está creando:

Tabla 23. Identificadores de tipos de familia

Para este tipo de familia	Especifique este identificador
DTD	El nombre DTD
Distintivo raíz	El distintivo de directorio raíz que está en dicha familia **Nota:** omita el prefijo del espacio de nombres si hay uno.
Espacio de nombres	El espacio de nombres del distintivo de directorio raíz

   Este identificador se utiliza durante el tiempo de ejecución para seleccionar una familia de formatos XML, uno de los cuales puede coincidir con el documento y ser utilizado para extraer la información de proceso del mismo. Tenga en cuenta que si hay varias familias que utilizan el mismo identificador, los formatos en todas las familias serán comprobados con el mensaje hasta que se encuentre una coincidencia.
8. Pulse **Guardar** para guardar la nueva familia o pulse **Cancelar** para detener la creación de una familia de documentos o **Volver** para regresar a la vista inicial.

Búsqueda de una familia de documentos
Acerca de esta tarea

Para ver una familia de documentos primero es necesario encontrarla. Para encontrar una familia de documentos, siga estos pasos:

Procedimiento

1. Pulse **Administración del concentrador** > **Configuración del concentrador** > **Formatos XML**.
2. Seleccione el protocolo de la familia de documentos que desea ver.
3. Especifique un nombre de familia, si lo conoce. Puede utilizar un asterisco (*) para realizar una búsqueda por comodines
4. Seleccione el tipo de familia: Cualquier tipo, DTD, Espacio de nombres o Distintivo de directorio raíz.
5. Seleccione la opción de archivos grandes: Ninguno, Utilizar procesador de archivos grandes o Utilizar procesador de archivos grandes con reconocimiento de espacio de nombres.
6. Pulse **Buscar**. Todas las familias de documentos que encajen con el criterio de búsqueda aparecerán debajo del botón Buscar.
7. Pulse el icono **Ver detalles** junto a una familia de documentos para ver sus detalles.

Edición de una familia de documentos
Acerca de esta tarea

En la ventana de detalles Familia de documento, puede editar las propiedades de una familia. Para hacerlo, lleve a cabo los siguientes pasos:

Procedimiento

1. Pulse el botón del lápiz en la vista de detalles de familia para mostrar una vista de edición de Familia de documento. Tenga en cuenta que no es posible modificar el protocolo en esta vista. Esto es porque pueden haber mensajes direccionados utilizando formatos en la familia y dificultaría la tarea de depuración si el se cambia el protocolo asociado con la familia.
2. En la vista de edición de Familia de documento, puede ahora cambiar el nombre de familia, el tipo de familia y el identificador de familia.
3. Cuando haya realizado los cambios, pulse **Guardar** para guardarlos. Pulse **Cancelar** o el botón tachado del lápiz para regresar a la ventana de detalles de la familia sin guardar ningún cambio.

Adición de un nuevo formato XML a una familia
Acerca de esta tarea

Una vez ha creado una familia de documentos, puede añadir nuevos formatos XML a dicha familia. Para hacerlo, lleve a cabo los siguientes pasos:

Nota: en este apartado, el término expresión XPath se usa a menudo. Cuando un formato XML utiliza una opción de archivo grande, este término debe interpretarse como una expresión de vía de acceso de elemento, que es una vía de acceso simple desde el directorio raíz de un documento a un elemento que tiene un valor.

1. Desde la vista de detalles de la familia de documentos, pulse **Crear formato XML**. Aparecerá vista de definición de formato XML. Esta página se divide en

cuatro apartados bajo los encabezados **Definición de tipo de documento**, **Criterios de definición de tipo de documento**, **Atributos de documento** y **Atributos definidos por el usuario**.

2. Complete la el apartado **Definición de tipo de documento**.

   En el apartado Definición de tipo de documento existe una lista de selección con los tipos de documentos contenidos en el protocolo asociado con la familia de documentos. Seleccione un **Tipo de documento** en la lista. Cuando un documento coincide con el formato XML, el protocolo asociado con la familia de documentos y el tipo de documento asociado con el formato son utilizados para direccionar el documento.

3. Complete el apartado **Criterios de definición de tipo de documento**.

   Los apartados **Criterios de definición de tipo de documento** y **Atributos de documentos** incluyen campos en los que se especifican valores y vías de acceso de elementos si está utilizando una opción de archivo grande o especifica expresiones XPath, espacios de nombres de prefijos y tipos de retorno si no es así.

   Valor En este campo, especifique un valor para el identificador de formato. Se trata de un campo obligatorio.

   Vía de acceso de elemento
   En este campo, especifique una vía de acceso de elemento. Se trata de un campo obligatorio. Tenga en cuenta que una vía de acceso de elemento sólo se aplica a los formatos que utilicen una opción de archivo grande.

   Expresión XPath
   En este campo, especifique una expresión XPath válida para el documento que coincida con el formato o un valor de cadena literal que sea devuelto como una constante para cada documento. Se trata de un campo obligatorio. Tenga en cuenta que las expresiones XPath no utilizan una opción de archivo grande.

   Campo Espacio de nombres de prefijo
   En este campo, especifique la definición del último prefijo de espacio de nombres, si hay alguno, utilizado en la expresión XPath. Esto se entra con el formato prefijo=calificador de espacio de nombres. Por ejemplo, si el último prefijo de espacio de nombres en la expresión es SOAPENV y su calificador es http://schemas.xmlsoap.org/soap/envelope/, se especificaría SOAPENV=http://schemas.xmlsoap.org/soap/envelope/ para el prefijo de espacio de nombres. Tenga en cuenta que los formatos que utilizan una opción de archivo grande no tienen los campos de espacio de nombre de prefijo como parte de su definición.

   Tipo de retorno
   En este campo, seleccione el nombre de distintivo Constante, Texto o Elemento en la lista de selección. Utilice Constante cuando desee interpretar el campo Expresión XPath como un literal de cadena para todos los documentos. Utilice Texto cuando desee utilizar el motor de evaluación XPath para evaluar la expresión en el contexto del documento. Utilice el nombre de distinto Elemento cuando desee obtener el nombre de elemento para el primer elemento devuelto por la evaluación XPath de la expresión. Tenga en cuenta que los formatos que utilizan una opción de archivo grande no tienen un nombre de distintivo Elemento como tipo de retorno.

En el apartado Criterios de definición de tipo de documento, especifique valores y expresiones XPath. Los valores y resultados de la evaluación de la expresión son comparados cuando se procesan los documentos para determinar si un formato XML coincide con un documento. Cuando se encuentra una coincidencia entre un documento y un formato y cuando los identificadores de empresa de origen y de destino pueden encontrarse utilizando el formato, el documento se direcciona utilizando el protocolo y el tipo de documento nombrados en el apartado Definición de tipo de documento. Consulte la Tabla 24 para obtener detalles acerca de los campos en este apartado.

Tabla 24. Campos Criterios de definición de tipo de documento

Campo	Obligatorio/ Opcional	Acción
Identificador de formato	Obligatorio	Especifique la expresión XPath o vía de acceso de elemento que define la vía de acceso al contenido dentro de los documentos XML que identifica de forma exclusiva el documento. Por ejemplo, si el distintivo de directorio raíz tiene este aspecto <PurchasingMessage type="Purchase Order"> para pedidos de compra y tenía el siguiente aspecto <PurchasingMessage type="Order Confirmation"> para confirmaciones, la expresión XPath /PurchasingMessage/@type devolvería el texto 'Purchase Order' para algunos mensajes y 'Order Confirmation' para otros. Se escribirían dos formatos XML, uno para pedidos y otro para confirmaciones y el campo 'Value' de los pedidos indicaría 'Purchase Order' y el campo 'Value' de las confirmaciones diría 'Order Confirmation'. En el tiempo de ejecución, el formato adecuado puede ser encontrado por el sistema porque buscará un formato en el que el resultado de la evaluación de la expresión coincide con el valor. Cuando se encuentra la coincidencia, el Tipo de documento de direccionamiento asociado con el formato es utilizado por el sistema.
Versión de formato	Obligatorio	Especifique la expresión XPath o vía de acceso de elemento que define la versión del formato. La versión del formato se evalúa de una manera similar a la utilizada por el identificador de formato. Cuando la expresión de la versión coincide con el valor de versión en un formato, el formato podrá ser utilizado si el identificador también coincide. Tenga en cuenta que si sólo hay una versión de un documento, puede especificar '1' para la expresión con un tipo de retorno Constante y '1' para el valor. Esto quiere decir que la versión siempre coincidirá y sólo se utilizará el identificador para determinar un formato coincidente.

4. Complete el apartado **Atributos de documento**.

   En el apartado **Atributos de documento**, especifique valores y expresiones XPath como ya hizo en el apartado **Criterios de definición de tipo de documento**. Consulte la Tabla 25 en la página 165 para obtener más detalles acerca de los campos en este apartado.

Tabla 25. Campos de atributos de documento

Campo	Obligatorio/ Opcional	Acción
Identificador de empresa de origen	Obligatorio	Especifique la expresión XPath o vía de acceso de elemento que define la vía de acceso del ID de empresa de origen dentro del documento XML. Esta opción se utiliza para identificar al socio de origen para propósitos de direccionamiento. Tenga en cuenta que estos datos deben encontrarse para que pueda utilizarse el formato.
Identificar de empresa de destino	Obligatorio	Especifique la expresión XPath o vía de acceso de elemento que define la vía de acceso del ID de empresa de destino dentro del documento XML. Esta opción se utiliza para identificar el socio de destino para propósitos de direccionamiento. Tenga en cuenta que estos datos deben encontrarse para que pueda utilizarse el formato.
Identificador del documento	Opcional	Especifique la expresión XPath o vía de acceso de elemento que define la vía de acceso del número de ID de documento dentro del documento XML. Este valor aparecerá en el visor de documentos.
Fecha y hora del documento	Opcional	Especifique la expresión XPath o vía de acceso de elemento que define la vía de acceso de la fecha y hora de creación del documento dentro del documento XML. Este valor aparecerá en el visor de documentos.
Claves de comprobación duplicadas 1 - 5	Opcional	Especifique las expresiones XPath o vías de acceso de elementos que definen las vías de acceso utilizadas para identificar si un documento es exclusivo o si es un duplicado.
Distintivo síncrono	Opcional	Especifique una expresión XPath o vía de acceso de elemento que evalúa a *true* o *false*, indicando si este tipo de documento requiere una respuesta síncrona o no. Puede especificar una expresión XPath que utilice el contenido de documento para establecer el valor o bien especificar el literal de cadena true o false con un tipo de retorno de Constante. El atributo BCGDocumentConstants. BCG_GET_SYNC_RESPONSE será establecido en el BDO durante el proceso de análisis del canal si este campo está establecido en true.
Elemento raíz de validación	Opcional	Especifique una expresión XPath que defina el nodo de directorio raíz del contenido (carga) de un mensaje ensobrado dentro del documento XML. WebSphere Partner Gateway validará un documento que comience con este elemento. Necesita especificar una acción que realice la validación para que funcione. Este campo no ocurre en formatos que utilicen una opción de archivo grande.

Tabla 25. Campos de atributos de documento (continuación)

Campo	Obligatorio/ Opcional	Acción
ID de documento relacionado	Opcional	Especifique la expresión XPath o vía de acceso de elemento que proporcione el identificador de documento de un documento previamente direccionado con el que está asociado el documento actual. Por ejemplo, una Confirmación de pedido suele generalmente estar relacionada con un Pedido de compra. El valor de identificador de documento Pedido de compra puede obtenerse utilizando una expresión XPath (consulte las opciones anteriores). Si la Confirmación de pedido incluye el identificador de Pedido de compra, podrá ser obtenido entonces utilizando la expresión de ID de documento relacionado. Al hacerlo se enlazarán los documentos en el Visor de documentos.
Campos de búsqueda 1-10	Opcional	Especifique expresiones XPath o vías de acceso de elemento que definan la vía de acceso al contenido del documento que desea utilizar para búsquedas personalizadas dentro del documento XML. En el Visor de documentos, puede buscar documentos basados en los valores en estos campos.

5. Complete el apartado **Atributos definidos por el usuario**.

   En el apartado **Atributos definidos por el usuario** puede añadir atributos definidos por el usuario. Añada un atributo escribiendo su nombre en el campo de entrada y pulsando **Añadir**. Defina entonces este nuevo atributo como lo haría con el resto de atributos estándares especificando, según corresponda, la expresión XPath, vía de acceso del elemento, espacio de nombre de prefijo y seleccionando un tipo de retorno para este atributo

   Una vez haya añadido los atributos, se utilizarán de la misma manera que se utilizan los atributos estándares. Si desea eliminar un atributo definido por el usuario de un formato, pulse la X roja que aparece junto a su nombre. Los atributos definidos por el usuario están ideados para su utilización por manejadores escritos por usuarios que procesen el documento. Los nombres de atributos y sus valores se añaden al documento de empresa cuando se procesa el documento. El código del manejador puede acceder a estos obteniéndolos del documento de empresa utilizando los nombres que se hayan definido. Consulte la publicación *WebSphere Partner Gateway Programmer Guide* para obtener más información.

6. Después de especificar los valores en esta vista, desplácese a la parte inferior y pulse **Guardar** para guardar los cambios. Pulse **Cancelar** o el botón del lápiz tachado para cancelar los cambios y regresar a la vista de resumen de la familia.

Direccionamiento de mensajes XML con distintos prefijos de espacio de nombres

Acerca de esta tarea

Al direccionar mensajes XML, debe configurar una definición de formato XML que contiene el mismo espacio de nombres y prefijo definido en el mensaje XML. Si utiliza distintos prefijos de espacio de nombres, configure el direccionamiento de mensajes XML en la consola de WebSphere Partner Gateway. Los tres métodos para realizar la configuración son los siguientes:

- Creación de una familia de documentos y un formato XML para cada mensaje que utilice los distintos prefijos de espacio de nombres.
- Creación de una familia de documentos y un formato XML para el nombre local (distintivo raíz de esquema).
- Creación de una familia de documentos y un formato XML utilizando una combinación de nombre local y espacio de nombres.

Creación de una familia de documentos y un formato XML para cada mensaje que utilice los distintos prefijos de espacio de nombres:

1. Vaya a **Administración del concentrador** > **Configuración del concentrador** > **Formatos XML**.
2. Pulse **Crear familia de documentos**.
3. En la página **Nueva familia de documentos**, cree una nueva familia de documentos de tipo *Espacio de nombres*.
4. Pulse **Guardar**.
5. Pulse **Crear formato XML**. Este formato XML se creará bajo la familia de documentos recién creada.
6. En la página **Definición de formato XML**, defina el formato XML para el espacio de nombres y el prefijo que debe utilizar el mensaje.
7. Repita los pasos 2, 3, 4, 5 y 6 con cada formato XML que se defina para el prefijo de espacio de nombres. Sin embargo, cree una familia de documentos diferente para cada formato XML.

Cree una familia de documentos y un formato XML para el nombre local (distintivo raíz de esquema):

1. En la página **Nueva familia de documentos**, cree una **Familia de documentos** de tipo *Distintivo raíz*.
2. Cree el formato XML bajo la familia de documentos recién creada. Al definir la **Expresión XPath**, utilice el nombre local (distintivo raíz) para el identificador de formato (**Identificador de empresa de origen** y **Identificador de empresa de destino**).
3. Pulse **Guardar**.
4. Envíe el mensaje XML que contiene los distintos espacios de nombres del prefijo XML.

   Nota: El nombre local del esquema XML también puede utilizarse para definir otros campos del formato XML, por ejemplo, Campos de búsqueda. Campos de búsqueda también puede definirse con mandatos de correlación mediante el cliente DIS o a través de salidas de usuario personalizadas.

Creación de una familia de documentos y un formato XML utilizando una combinación de nombre local y espacio de nombres:

1. En la página **Nueva familia de documentos**, cree una familia de documentos de tipo *Espacio de nombres*.
2. Pulse **Guardar** para guardar la familia de documentos recién creada.
3. Cree el formato XML bajo la familia de documentos recién creada. Defina el formato XML utilizando una combinación de nombre local (distintivo raíz) y espacio de nombres.Por ejemplo, **Expresión XPath para identificador de empresa de origen:** *//*[namespace-uri()='http://edi.mycompany.com/2007/types/transnet' and local-name()="purchaseOrder"]/* [namespace-uri()='http://edi.mycompany.com/2007/types/transnet' and local-name()="senderID"]* **Expresión XPath para identificador de empresa de destino:** *//*[namespace-uri()='http://*

edi.mycompany.com/2007/types/transnet' and local-name()="purchaseOrder"]/ [namespace-uri()='http://edi.mycompany.com/2007/types/transnet' and local-name()="receiverID"]*

4. Envíe el mensaje XML que contiene los distintos espacios de nombres del prefijo XML.

   Nota: La combinación de nombre local y espacio de nombres del esquema XML también puede utilizarse para definir otros campos del formato XML, por ejemplo, Campos de búsqueda. Campos de búsqueda también puede definirse con mandatos de correlación mediante el cliente DIS o a través de salidas de usuario personalizadas.

Creación de una definición de protocolo

Acerca de esta tarea

En los pasos siguientes se describe cómo crear un formato de definición de protocolo XML personalizado:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Crear definición de documento**.
2. En **Tipo de definición de documento**, seleccione **Protocolo**.
3. En **Nombre**, especifique un identificador para la definición del documento. Por ejemplo, para un protocolo XML personalizado, puede especificar XML personalizado. Este campo es necesario.
4. En **Versión**, especifique un valor para la versión del protocolo. Se permiten valores numéricos o de cadena.
5. Si lo desea, puede especificar una descripción del protocolo.
6. Establezca **Nivel de documento** en **No**, ya que está definiendo un protocolo, en lugar de un tipo de documento (que definirá en el siguiente apartado).
7. Establezca **Estado** en **Habilitado**.
8. Establezca **Visibilidad** para este protocolo. Probablemente prefiera que esté visible para todos los socios.
9. Seleccione los paquetes en los que se envolverá este nuevo protocolo. Por ejemplo, si desea que este protocolo se asocie con los paquetes AS, Ninguno e Integración de programas de fondo, seleccione **Paquete: AS**, **Paquete: Ninguno**, **Paquete: Integración de programas de fondo**.
10. Pulse **Guardar**.

Creación de una definición de tipo de documento

Acerca de esta tarea

A continuación, vaya a la página Crear definición de documento de nuevo para crear un tipo de documento.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Crear definición de documento**.
2. En **Tipo de definición de documento**, seleccione **Tipo de documento**.
3. En **Nombre**, especifique un identificador para la definición del documento. Por ejemplo, puede especificar `Pedido de compra` como nombre del tipo de documento. Este campo es necesario.
4. En **Versión**, especifique un valor para la versión del tipo de documento. Se permiten valores numéricos o de cadena.
5. Especifique una descripción opcional del tipo de documento.

6. Establezca **Nivel de documento** en **Sí** (ya que está definiendo un objeto de direccionamiento que se corresponde con un documento real).
7. Establezca **Estado** en **Habilitado**.
8. Establezca **Visibilidad** para este flujo. Probablemente prefiera que esté visible para todos los socios.
9. Pulse el icono **Expandir** para expandir cada paquete seleccionado en el paso 9 en la página 168. Expanda la carpeta y seleccione el nombre del protocolo que ha creado en el apartado anterior (por ejemplo, Protocolo: XML personalizado).
10. Pulse **Guardar**.

Si ha usado los valores de ejemplo, la página Gestionar definiciones de documento contendrá ahora un tipo de documento de Pedido de compra y un protocolo XML personalizado bajo los paquetes de integración AS, Ninguno e Integración de fondo.

Finalización de la configuración

Después de definir la definición del protocolo, podrá elegirla como protocolo de direccionamiento para utilizarla para una familia de documentos XML. Después de añadir tipos de documento al protocolo, podrá asignarlos a las definiciones de formato XML que se encuentran en la familia de documentos. Los mensajes que coincidan con un formato en la familia serán direccionados utilizando el protocolo asociado con la familia y el tipo de documento asociado con el formato coincidente.

Antes de poder definir ningún canal que utilice las nuevas definiciones, necesitará habilitar interacciones entre los nuevos protocolos y tipos de documentos y otros protocolos y tipos de documentos. También necesita habilitar las funciones B2B de los socios para permitirles enviar y recibir documentos utilizando el nuevo protocolo y tipos de documentos.

Validación de archivos XML personalizados en relación a un archivo XSD

Después de haber realizado la configuración básica de XML personalizado (definición de tipo de documento, creación de la familia XML y el formato XML, funciones B2B y conexión) y de que el XML esté preparado para que la acción simple de "Paso a través" lo direccione, siga los siguientes pasos para permitir la validación de XML antes del paso a través:

1. En la página **Conexiones**, establezca *Paso a través de XML personalizado con validación* como la nueva acción.
2. Vaya a **Administración del concentrador** > **Configuración del concentrador** > **Definición de documento**.
3. Pulse el icono **Editar valores de atributo** (flecha azul) para el tipo de documento XML personalizado.
4. Seleccione **Subir correlación**.
5. Seleccione el correspondiente archivo XSD y pulse **Subir**.
6. Repita los pasos 2-3.
7. Pulse **Añadir atributos** para añadir Atributos de contexto de definición de documento.
8. Seleccione **Correlación de validación** y pulse **Guardar**.
9. En **Administración de cuentas**> **Conexiones** busque la conexión.

10. Pulse **Atributos** en el lado de **Origen** de la conexión.
11. Expanda el icono de nodo contraído (carpeta azul) de Tipo de documento.
12. En el desplegable **Correlación de validación**, seleccione la correlación de validación XSD y pulse **Guardar**.

Si necesita subir una nueva versión del archivo XSD, deberá eliminar primero la anterior. Esto se puede realizar en la página **Administrador del concentrador** > **Configuración del concentrador**> **Correlaciones** > **Correlaciones de validación**. Después de subir la nueva correlación, repita el paso 12, puesto que la supresión de una correlación restablece este atributo de conexión.

Utilización de correlaciones de validación

WebSphere Partner Gateway utiliza correlaciones de validación para validar la estructura de determinados documentos. Si desea asociar una correlación de validación con un documento, asegúrese primero de que la correlación está disponible en WebSphere Partner Gateway, tal como se describe en el apartado "Adición de correlaciones de validación". Para la gestión de correlaciones de validación, consulte el *capítulo Tareas de administración del concentrador de la Guía del administrador de WebSphere Partner Gateway*.

Adición de correlaciones de validación

Acerca de esta tarea

Una acción puede tener una correlación de validación asociada para garantizar que el socio de destino o sistema de fondo pueden analizar el documento. No olvide que una correlación de validación sólo valida la *estructura* del documento. No valida el contenido del mensaje.

Nota: una vez asocie una correlación de validación con una definición de documento no es posible desasociarlos.

Para añadir una correlación de validación al concentrador, siga este procedimiento.

1. Guarde el archivo de correlaciones de validación en el concentrador o en una ubicación donde WebSphere Partner Gateway pueda leer los archivos.
2. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones > Correlaciones de validación**.
3. Pulse **Crear**.
4. Escriba una descripción de la correlación de validación.
5. Desplácese hasta el archivo de esquema que desea utilizar para validar documentos y pulse **Abrir**.
6. Pulse **Guardar**.

Asociación de correlaciones con definiciones de documentos

Acerca de esta tarea

Para asocie una correlación de validación con una definición de documento, utilice el siguiente procedimiento.

1. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones > Correlaciones de validación**.
2. Pulse el icono **Ver detalles** junto a la correlación de validación para asociarla con la definición de documento.

3. Pulse el icono **Expandir** situado junto a un paquete para expandir de forma individual hasta el nivel adecuado (por ejemplo, **Acción** para un documento RosettaNet).
4. Seleccione la definición de documento que desea asociar con la correlación de validación.
5. Pulse **Guardar**.

Utilización de correlaciones de transformación

Pasos para utilizar los mapas de transformación, que se utilizan para convertir un documento de un formato a otro.

Acerca de esta tarea

WebSphere Partner Gateway utiliza correlaciones de transformación para convertir documentos de uno a otro formato, por ejemplo, para convertir documentos XML en EDI.

A continuación se proporcionan los pasos para utilizar las correlaciones de transformación:

1. Inicie sesión en la consola administrativa de WebSphere Partner Gateway.
2. Pulse **Asistentes**.
3. En el asistente de importación EIF, busque (**Examinar**) y especifique la ubicación del archivo .EIF.
4. Pulse **Importar**.
5. En la página Resumen de importación, pulse **Siguiente**.
6. En la pantalla Revisar correlaciones de transformación y Modificar interacciones que se deben crear, seleccione la correlación de transformación, agregue una interacción y seleccione la acción para la interacción creada.
7. Pulse **Finalizar**.

Importante: Si descarga un mapa de transformación de la consola de WebSphere Partner Gateway, se descarga un archivo con un tamaño de 0 KB; que es un problema conocido. Como método alternativo, utilice el cliente DIS para descargar o extraer mapas de transformación.

Visualización de documentos

Acerca de esta tarea

El Visor de documentos muestra información acerca de los documentos que componen un tipo de documento. Puede mostrar documentos sin formato y los sucesos y detalles de proceso de documentos asociados mediante criterios de búsqueda específicos. Esta información es útil si está intentando determinar si un documento se ha entregado satisfactoriamente o para determinar la causa de un problema.

Para mostrar el Visor de documentos, lleve a cabo los siguientes pasos:

1. Pulse **Visores > Visor de documentos**.
2. Seleccione los criterios de búsqueda adecuados.
3. Pulse **Buscar**.

Consulte la publicación *Guía del administrador de WebSphere Partner Gateway* para obtener más información sobre la utilización del Visor de documentos.

Configuración del registro cronológico de no rechazo

Puede configurar el registro cronológico de mensajes de no rechazo utilizando atributos del paquete, protocolo o flujo de documentos utilizado para direccionar documentos. El atributo se denomina Se necesita no rechazo, y su valor puede ser Sí o No. La definición de los atributos se facilita en el nivel de objetos de direccionamiento, y se puede sobrescribir cambiándola en el nivel de la posibilidad B2B o en el nivel de conexión.

Configuración del almacén de mensajes

Puede configurar el almacén de mensajes mediante atributos del paquete, protocolo o flujo de documentos utilizado para direccionar documentos. El atributo se denomina Se necesita almacén de mensajes, y su valor puede ser Sí o No. La definición de los atributos se facilita en el nivel de objetos de direccionamiento, y se puede sobrescribir cambiándola en el nivel de la posibilidad B2B o en el nivel de conexión.

Capítulo 10. Configuración de flujos de documentos EDI

Este capítulo describe cómo configurar las definiciones de documento e interacciones para intercambios EDI estándares. Asimismo, se incluyen descripciones de la recepción y transformación de documentos XML y de datos orientados a registros (ROD). Este capítulo incluye los siguientes temas.

También es posible realizar un intercambio EDI sin efectuar ningún desensobrado ni ninguna transformación. En el apartado "Documentos EDI con acción de paso a través" en la página 112 se muestran los pasos para crear interacciones para este tipo de intercambio.

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado la sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Visión general de EDI

EDI es un método de transmisión de información empresarial a través de una red entre asociados empresariales que acuerdan seguir los estándares nacionales o del sector aprobados en los procesos de conversión y de intercambio de información. WebSphere Partner Gateway proporciona el proceso de desensobrado, transformación y ensobrado para los siguientes estándares EDI:

- X12, Estándar EDI común aprobado por el organismo American National Standards Institute.
- UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Transport)
- UCS (Uniform Communication Standard)

En los siguientes apartados se proporciona una visión general de los intercambios EDI que cumplen los estándares X12, EDIFACT y UCS y de las transacciones y

grupos incluidos dentro de los intercambios. También se describe cómo se transforman los documentos XML y ROD y los intercambios EDI.

Estructura de intercambio EDI

Un intercambio EDI contiene una o más transacciones empresariales. En X12 y estándares relacionados, una transacción empresarial se denomina *conjunto de transacciones*. En EDIFACT y estándares relacionados, una transacción empresarial se denomina un *mensaje*. Este documento generalmente utiliza el término *transacción* o *transacción empresarial* para hacer referencia a un conjunto de transacciones X12 o UCS, o a un mensaje EDIFACT.

Los intercambios EDI están formados por *segmentos* que a su vez contienen *elementos de datos*. Los elementos de datos representan cosas como un nombre, una cantidad, una fecha o una hora. Un segmento es un grupo de elementos de datos relacionados. Los segmentos se identifican por un nombre de segmento o un identificador de segmento, que aparece al principio del segmento. (Los elementos de datos no se identifican por nombre sino que están delimitados por caracteres separadores especiales reservados para ello).

En algunos casos, es útil distinguir entre segmentos de detalles o datos de una transacción y otros segmentos que se utilizan para fines administrativos. Los segmentos administrativos se denominan *segmentos de control* en X12 y *segmentos de servicio* en EDIFACT. Los segmentos de *sobre* que definen los límites de un intercambio EDI son un ejemplo de estos segmentos de control o servicio.

Los intercambios EDI pueden contener tres niveles de segmentos. En cada nivel, hay un segmento de cabecera al principio y un segmento de cola al final.

Un intercambio siempre tiene un segmento de cabecera de intercambio y un segmento de cola de intercambio.

Un intercambio puede contener uno o más grupos. A su vez, un grupo contiene una o más transacciones asociadas. El nivel del grupo es opcional en EDIFACT, pero es necesario en X12 y estándares relacionados. Cuando hay grupos, existe un segmento de cabecera de grupo y un segmento de cola de grupo para cada grupo.

Un grupo (o un intercambio, donde no hay grupos) contiene una o más transacciones. Cada transacción tiene una cabecera del conjunto de transacciones y una cola del conjunto de transacciones.

Una transacción representa un documento de empresa, como un pedido de compra. El contenido del documento empresarial lo representan los segmentos de detalle entre el segmento de cabecera del conjunto de transacciones y el segmento de cola del conjunto de transacciones.

Cada estándar EDI proporciona su propio método para visualizar los datos incluidos en un intercambio. En la tabla siguiente se listan los segmentos para cada uno de los tres estándares EDI soportados.

Tabla 26. Segmentos para estándares EDI soportados

Segmento estándar	X12	UCS	EDIFACT
Inicio del intercambio	ISA	BG	UNB
Fin de intercambio	IEA	EG	UNZ

Tabla 26. Segmentos para estándares EDI soportados (continuación)

Segmento estándar	X12	UCS	EDIFACT
Inicio de grupo	GS	GS	UNG
Fin de grupo	GE	GE	UNE
Inicio de transacción	ST	ST	UNH
Fin de transacción	SE	SE	UNT

La Figura 22 muestra un ejemplo de un intercambio X12 y los segmentos que forman el intercambio.

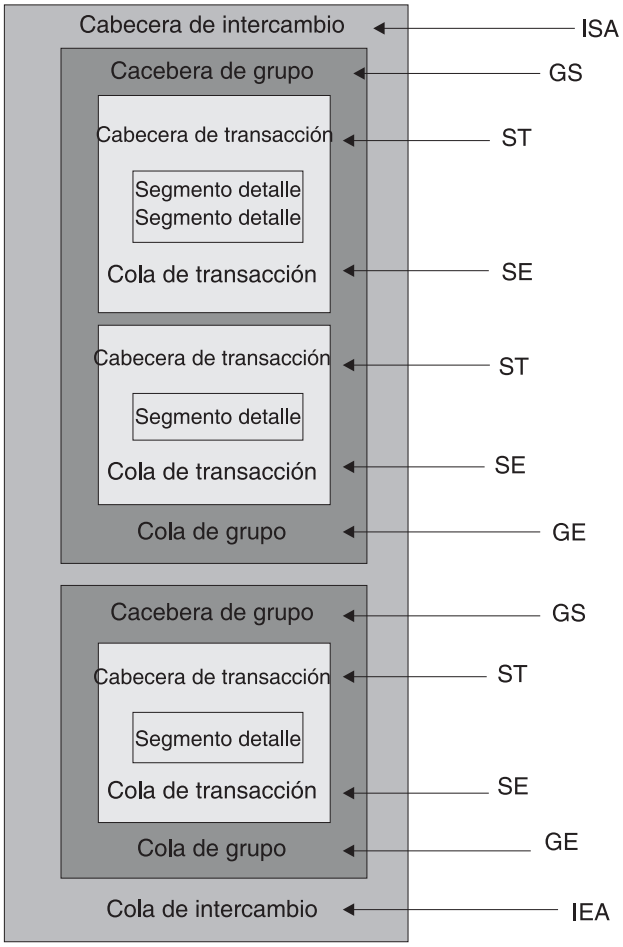


Figura 22. Un sobre de intercambio

Correlaciones

El especialista de correlaciones de Data Interchange Services Client crea correlaciones de transformación que describen cómo convertir un documento en un formato en un documento con un formato distinto. Por ejemplo, podría tener una correlación de transformación que transforme una transacción X12 en un mensaje EDIFACT. También puede transformar una transacción EDI en un documento XML o un documento de datos orientado a registros.

Los mapas se pueden crear mediante el estudio de diseño DIS o WTX. DIS se utiliza para crear correlaciones para la transformación WDI, mientras que el

estudio de diseño WTX se utiliza para la transformación WTX. Los mapas creados mediante DIS no se pueden migrar para la transformación WTX, pero deben sobrescribirse. Seguún la acción, el motor de transformación se seleccionará si ambos son operativos para usted.

Para crear cualquier correlación, es necesaria la definición de los documentos de origen y destino. WDI proporciona las definiciones de los documentos de origen para EDI, pero para ROD y XML deberá crearlas mediante el cliente DIS. Para que el código en tiempo de ejecución pueda utilizar este estándar, hay que compilarlo. En versiones anteriores, las correlaciones de transformación son necesarias para el estándar, pero esta versión permite compilar sin la correlación de transformación. Se importa el eif estándar para EDI, pero para ROD se crea mediant el cliente DIS. En el caso de XML, el DTD/XSD se importa a la base de datos de desarrollo. Para EDI, en la consola administrativa vaya a asistentes de EDI. Se mostrarán los formatos y estándares de datos disponible en el archivo EIF. Puede importarlo todo en una sola vez o seleccionar uno o más para importar. En una selección correcta la serie del control estándar se importará en la base de datos en tiempo de ejecución.

La correlación de transformación también puede crear varios documentos en un solo documento. Este tipo de correlación utiliza el *encadenamiento de correlaciones*, que genera varias salidas a partir de una sola transacción. En el encadenamiento de correlaciones, después de convertir satisfactoriamente un documento de origen en un documento de destino, se utilizará una correlación subsiguiente para convertir de nuevo el documento de origen y generar otro documento de destino. Esto puede repetirse tantas veces como sea necesario para generar tantos documentos como sea necesario.

Además de las correlaciones de transformación, puede utilizar correlaciones de acuse de recibo funcional y correlaciones de validación. Las correlaciones de acuse de recibo funcional proporcionan instrucciones para producir un acuse de recibo funcional, que notifica al remitente de un documento EDI que el documento ha llegado. Cuando se instala WebSphere Partner Gateway, se instalan varias correlaciones de acuse de recibo funcional estándar EDI. Consulte el apartado “Configuración de reconocimientos” en la página 218 para obtener una lista de estas correlaciones.

Cuando el concentrador de envío espera un reconocimiento funcional y no llega a tiempo de reconocerlo, el documento original se reenvía. El número de reintentos y su intervalo pueden configurarse. Esta característica no está activada de manera predeterminada. Deberá establecer manualmente el valor en las propiedades de EDI. Si el Tiempo para el reconocimiento se establece en Sí, los valores deben establecerse para reintantar el recuento y el intervalo. Los sucesos de reintento se registran con el propósito de monitorizarlos. Si los reintentos se agotan sin FA, el suceso apropiado se registrará para fines de supervisión.

El especialista de correlaciones de Data Interchange Services Client puede crear correlaciones de acuse de recibo funcional adicionales. WebSphere Partner Gateway genera un acuse de recibo funcional cuando se valida una transacción EDI y ésta tiene asociada una correlación de acuse de recibo funcional. El documento de origen debe ser un documento EDI.

WebSphere Partner Gateway proporciona un nivel de validación estándar sobre el documento EDI. Si se va a generar un acuse de recibo funcional, los resultados de la validación de un documento EDI se guardan. Las correlaciones de validación se crean para proporcionar validación adicional de un documento EDI. La generación

de un acuse de recibo funcional utiliza la correlación de acuse de recibo funcional y los resultados de la validación del documento EDI. La correlación de acuse de recibo funcional contiene mandatos de correlación que indican cómo utilizar los resultados de validación para crear un acuse de recibo funcional específico. Si se acepta un documento para que lo convierta el proceso de validación, se utilizará la correlación de transformación de datos adecuada para convertir el documento de origen.

Visión general de documentos XML y ROD

El especialista de correlaciones de Data Interchange Services Client puede crear definiciones de documento para documentos XML y documentos de datos orientados a registros y luego crear correlaciones de transformación que transforman un tipo de documento en otro.

documentos XML

Los documentos XML se definen por una DTD XML o un esquema XML. El especialista de correlaciones de Data Interchange Services Client crea una correlación de transformación basada en el DTD o esquema que describe cómo convertir el documento XML en otro formato. Un documento XML puede transformarse en otro documento XML, un documento de datos orientado a registros o una transacción EDI.

documentos ROD

El término datos orientados a registros (ROD) se refiere a documentos que cumplen las especificaciones de un formato con marca registrada. El especialista de correlaciones de Data Interchange Services Client define una definición de documentos ROD, que hace referencia a la forma en que una aplicación empresarial estructura datos en un documento. Después de definir una definición de documento, el especialista de correlaciones puede crear una correlación para transformar el documento ROD en otro documento ROD, un documento XML o una transacción EDI.

Divisores y varios documentos

Los documentos XML o ROD pueden especificar en el concentrador como documentos individuales o como un grupo de documentos dentro del mismo archivo. Es posible colocar varios documentos en el mismo archivo cuando, por ejemplo, un trabajo planificado en el socio o socio interno sube documentos de forma periódica para que sean enviados. Si varios documentos XML o ROD llegan en un archivo, el receptor llama al manejador de divisor asociado (XMLSplitterHander o RODSplitterHandler) para que divida el conjunto de documentos. (Los manejadores de divisor se configuran cuando se crea un destino. Consulte el apartado “ Preproceso” en la página 78 para más información). A continuación, los documentos se volverán a introducir en el Gestor de documentos para procesarlos individualmente.

Nota: los ID de emisor y receptor deben formar parte de la definición de documentos ROD asociada a la correlación de transformación. La información necesaria para determinar el tipo de documento y los valores de diccionario también deben estar en la definición de documento. Asegúrese de que el especialista de correlaciones de Data Interchange Services Client conoce estos requisitos al crear la correlación de transformación.

También pueden enviarse en un archivo varios intercambios EDI. Si varios intercambios EDI llegan en un archivo, el receptor llama a EDISplitterHandler para que divida el conjunto de intercambios. A continuación, los intercambios se volverán a introducir en el Gestor de documentos para procesarlos individualmente.

Nota: la división se realiza en el intercambio, no en las transacciones individuales internas de este. Las transacciones internas del intercambio se desensobran.

Visión general de la creación de tipos de documentos y configuración de atributos

Una definición de documento se compone, como mínimo, de un paquete, un protocolo y un tipo de documento. Las definiciones de documento especifican los tipos de documentos que serán procesados por WebSphere Partner Gateway.

El paquete hace referencia a la lógica necesaria para empaquetar un documento de acuerdo con una especificación, como AS2. Un flujo de protocolos es la lógica necesaria para procesar un documento que cumple las normas de un determinado protocolo, como EDI-X12. Un tipo de documento describe el aspecto del documento.

En los apartados siguientes se describen brevemente los pasos generales para configurar un flujo de documentos entre el socio interno y un socio externo. También se describen los puntos en los que pueden establecer atributos.

Paso 1: Asegúrese de que la definición del documento se encuentra disponible

Acerca de esta tarea

Antes de poder enviar o recibir un documento, es necesario definir una definición de documento para dicho documento. WebSphere Partner Gateway proporciona varias definiciones de documento predeterminados, incluyendo unas que representan acuses de recibo funcionales. Cuando importe correlaciones de transformación para transacciones EDI o documentos XML o ROD, las definiciones de documento asociadas aparecerán en la página Definiciones de documentos. Asimismo, si importa una correlación de acuse de recibo funcional que no esté ya definida, la definición del documento del acuse de recibo aparecerá en la página Definiciones de documento. Puede también crear sus propias definiciones de documento.

Como parte del establecimiento de la definición de documentos, puede modificar determinados atributos. Los atributos se utilizan para realizar varias funciones de direccionamiento y proceso de documentos, como la validación, la comprobación del cifrado y el recuento de reintentos. Los atributos que establezca en el nivel de definición proporcionan un valor global para el paquete, protocolo o tipo de documento asociado. Los atributos que se encuentran disponibles varían dependiendo de la definición del documento. Los atributos para definiciones de documento EDI tienen distintos atributos que las definiciones de documento de RosettaNet.

Por ejemplo, si especifica un valor para **Permitir una solicitud TA1** en el nivel de tipo de documentos ISA, el valor se aplicará a todos los documentos ISA. Si posteriormente establece el valor **Permitir un atributo de TA1** en el nivel de

funciones B2B para un socio o socio interno, dicho valor altera temporalmente el valor establecido en el nivel de definición del documento.

Para los atributos que pueden establecerse en varios niveles de la definición de flujo de documentos, los valores establecidos en el nivel de flujo de documentos tienen prioridad sobre los establecidos en el nivel de protocolo y los atributos establecidos en el nivel de protocolo tienen prioridad sobre los establecidos en el nivel de paquete. Por ejemplo, si especifica un perfil de sobre en el nivel de protocolo &X44TA1 pero especifica un perfil de sobre distinto en el nivel de tipo de documentos TA1, se utilizará el perfil de sobre que especifique en el nivel de tipo de documentos TA1.

Para crear interacciones, el tipo de documento debe aparecer en la lista en la página Gestionar definiciones de documento.

Paso 2: Crear interacciones

Acerca de esta tarea

a continuación, defina las interacciones, que son plantillas para crear conexiones de socios. Las interacciones indican cómo se recibe el documento y cómo éste se envía desde el concentrador.

Para algunos protocolos, sólo necesitará dos flujos, uno para describir el documento que se ha recibido en el concentrador (desde el socio o desde el socio interno) y otro que describa el documento que se ha enviado desde el concentrador (al socio externo o al socio interno). Sin embargo, si el concentrador envía o recibe un intercambio EDI que se desensobrará en transacciones individuales o en el que se requieren acuses de recibo, en realidad se crearán varias interacciones. Por ejemplo, si recibe un intercambio EDI en el concentrador, tendrá una interacción que describe cómo se envía el intercambio al concentrador y cómo se procesa en el mismo. También dispondrá de una interacción para cada transacción dentro del concentrador que describe cómo se procesa la transacción. Para los intercambios EDI que salen del concentrador, dispondrá de una interacción que describe cómo se envía el sobre de intercambio al destinatario.

Paso 3: Crear perfiles de socios, destinos y posibilidades B2B

Acerca de esta tarea

A continuación, cree perfiles de socios para el socio interno y para los socios externos. Defina los destinos (que determinan dónde se enviarán los documentos) y las funciones B2B, que especifican los documentos que el socio interno o un socio puede enviar y recibir. La página de funciones B2B lista todos los tipos de documentos que hayan sido definidos.

Puede establecer atributos en el nivel de funciones B2B. Todos los atributos establecidos en este nivel alterarán temporalmente los establecidos en el nivel de definición de documentos. Por ejemplo, si establece **Permitir una solicitud TA1** en **No** en el nivel de definición de documentos para documentos ISA pero a continuación lo establece en **Sí** en el nivel de funciones B2B, se utilizará el valor de **Sí**. Establecer un atributo en el nivel B2B permite personalizar el atributo a un socio concreto.

Si establece el perfil de sobre en el nivel de tipo de protocolo o documento (en la página Gestionar definiciones de documento) y, a continuación, lo establece en un valor distinto en la página de funciones B2B, se utilizará el último valor.

Para crear conexiones entre ellos deberá haber definido previamente los perfiles y funciones B2B del socio interno y de los socios externos.

Paso 4: Activar conexiones

Acerca de esta tarea

Finalmente, active las conexiones entre el socio interno y los socios externos. Las conexiones que estén disponibles se basan en las funciones B2B de los socios y en las interacciones que haya creado. Las interacciones dependen de las definiciones de documento que estén disponibles.

En algunos intercambios, sólo es necesaria una conexión. Por ejemplo, si un socio está enviando un documento binario a una aplicación de fondo del socio interno, sólo necesitará una conexión. Sin embargo, para el intercambio de intercambios EDI en el que el intercambio se desensobra y las transacciones individuales se transforman, se configuran varias conexiones.

Nota: en los intercambios EDI que se pasan tal como están, sólo se requiere una conexión.

Puede establecer atributos en el nivel de conexión. Todos los atributos establecidos en este nivel alterarán temporalmente los establecidos en el nivel de atributos B2B. Por ejemplo, si establece **Permitir una solicitud TA1** en **Sí** en el nivel de funciones B2B pero después se establece en **No** en el nivel de conexión, se utiliza el valor **No**. Si establece un valor para un atributo en el nivel de conexión, podrá personalizar más el atributo, dependiendo de los requisitos de direccionamiento de los socios y aplicaciones implicados.

Visión general de flujos posibles

Este apartado proporciona una visión general de los tipos de transformación que puede realizar WebSphere Partner Gateway. En el apartado “Definición de intercambios de documentos” en la página 204 se proporcionan más detalles de estas transformaciones y lo que es necesario hacer para configurarlas.

Flujo de EDI a EDI

WebSphere Partner Gateway puede aceptar un intercambio EDI desde un socio o desde el socio interno, transformarlo en un tipo diferente de intercambio EDI (por ejemplo, de EDI-X12 a EDIFACT), y enviar el documento al socio interno o socio. Los siguientes pasos se producen cuando un intercambio EDI se transforma en otro intercambio EDI:

1. El intercambio EDI recibido en el concentrador se desensobra.
2. Las transacciones individuales internas del intercambio EDI se transforman en el formato EDI del receptor.
3. Las transacciones EDI transformadas se ensobran y envían al destinatario.

La Figura 23 en la página 181 muestra un intercambio X12 en el que se desensobran tres transacciones. Las transacciones se transforman en un formato EDIFACT y, a continuación, se ensobran y envían al socio.

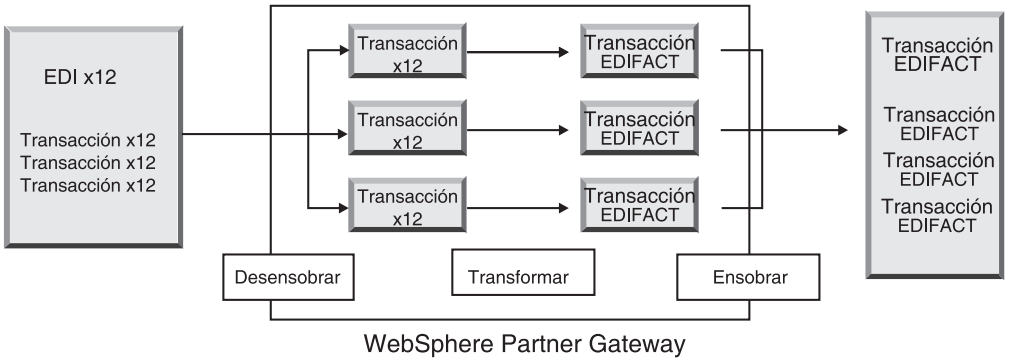


Figura 23. Flujo de intercambio EDI a intercambio EDI

Cada una de las transacciones tiene asociada una correlación de transformación que especifica cómo se transforma la transacción. La transacción puede transformarse en una sola transacción o en varias transacciones, si se ha utilizado un encadenamiento de correlaciones para crear la correlación. Si el proceso por lotes del ensobrador está activado, las transacciones que entran en el concentrador en un sobre saldrán del mismo en un sobre. Sin embargo, si hay puntos de ruptura del sobre (por ejemplo, distintos valores para atributos EDI o un perfil de sobre diferente) o si el proceso por lotes está desactivado, las transacciones saldrán en distintos sobres. Consulte el apartado "Ensobrador" en la página 192 para obtener una descripción general del ensobrador (que es el componente que reúne un conjunto de transacciones que deben enviarse a un socio, las pone en un sobre y las envía). Consulte el apartado "Modalidad de proceso por lotes" en la página 192 para obtener más información sobre el proceso por lotes.

La transacción también puede tener asociada una correlación de validación.

Flujo de EDI a XML o ROD

WebSphere Partner Gateway puede aceptar un intercambio EDI desde un socio o desde el socio interno, desensobrar el intercambio, y transformar las transacciones EDI obtenidas en documentos XML o ROD.

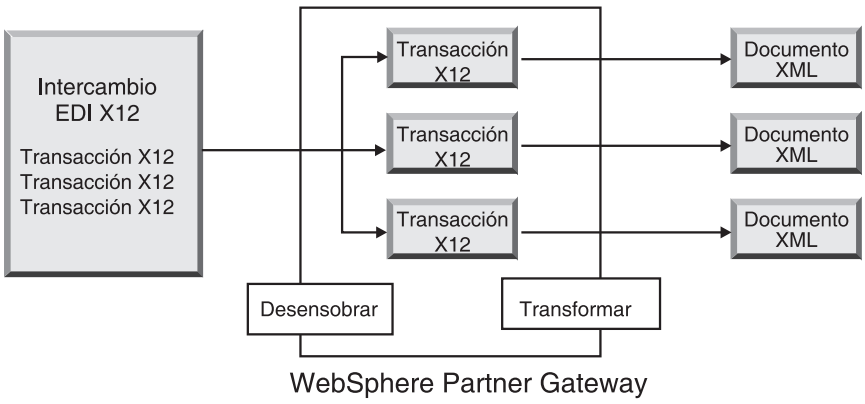


Figura 24. Flujo de intercambio EDI a documentos XML

La transacción puede transformarse en un solo documento o en varios documentos, si se ha utilizando un encadenamiento de transacciones para crear la correlación.

Flujo de XML o ROD a EDI

WebSphere Partner Gateway puede recibir documentos XML o ROD desde un socio o desde un socio interno, transformar los documentos en transacciones EDI, ensobrar las transacciones y, a continuación, enviárselas al socio interno o a un socio.

En la Figura 25 se muestran los documentos XML que se transforman en interacciones X12 y se ensobran.

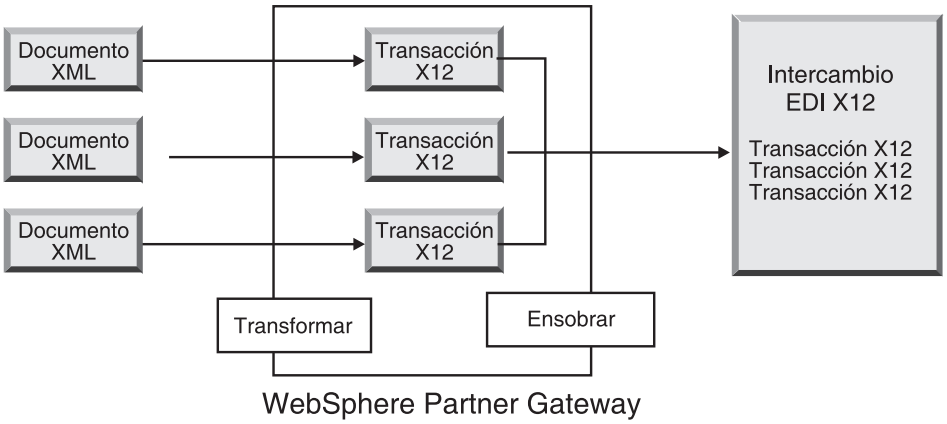


Figura 25. Flujo de documentos XML a intercambio EDI

Un documento puede transformarse en varias transacciones (si se ha utilizado el encadenamiento de correlaciones para crear la correlación) y las transacciones se pueden ensobrar en distintos intercambios. En la Figura 26 se muestra un documento XML que se transforma en tres transacciones X12. Dos de las transacciones se ensobran juntas. Una se pone en un sobre aparte.

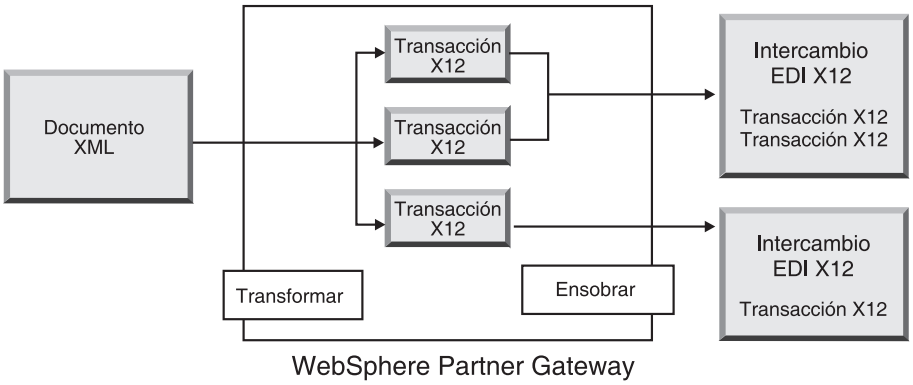


Figura 26. Flujo de documentos XML a varias transacciones EDI

Flujo de varios documentos XML o ROD a intercambio EDI

WebSphere Partner Gateway puede recibir un archivo, que consiste en uno o más documentos XML o ROD, desde un socio o desde el socio interno, transformar el documento o documentos en transacciones EDI, ensobrar las transacciones EDI en varios sobres, y enviárselos al socio interno o al socio.

Cada documento puede transformarse en una sola transacción o, si se ha utilizado un encadenamiento de correlaciones, en varias transacciones.

Notas:

1. Los documentos enviados en un archivo deben ser del mismo tipo, documentos XML o documentos ROD, pero no pueden ser de ambos.
2. Los documentos ROD deben ser del mismo tipo.

En la Figura 27 se muestra un conjunto de documentos XML que se está dividiendo, lo que resulta en documentos XML individuales. Los documentos XML se transforman en transacciones X12 y las transacciones se ensobran.

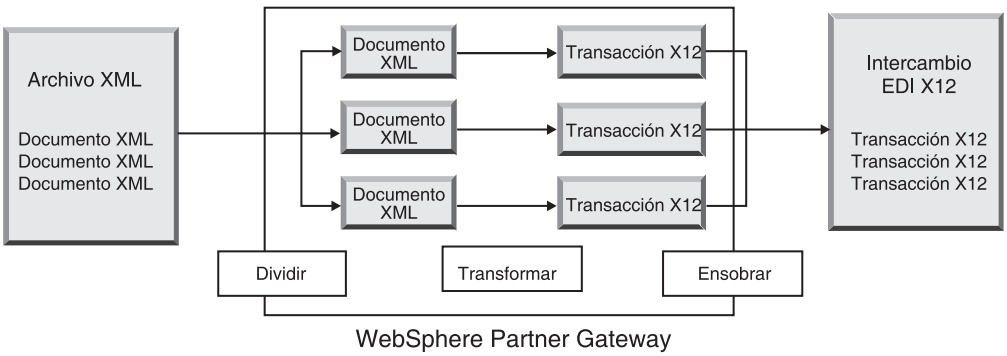


Figura 27. Flujo de varios documentos XML a intercambio EDI

En la Figura 27, los documentos se dividen (por el manejador de divisor XML) y las transacciones transformadas se ensobran juntas. El manejador de divisor XML debe tener activada la opción BCG_BATCHDOCS (el valor predeterminado) para que esto suceda. Si BCG_BATCHDOCS está activada y la modalidad de proceso por lotes del ensobrador está activada, estas transacciones pueden colocarse en el mismo sobre EDI. La modalidad de proceso por lotes del ensobrador se describe en el apartado “Modalidad de proceso por lotes” en la página 192.

Flujo de XML a ROD o ROD a XML

WebSphere Partner Gateway puede recibir un documento XML o ROD desde un socio o desde un socio interno, transformar el documento en otro tipo (de XML a ROD o de ROD a XML) y, a continuación, enviárselo al socio o al socio interno.

En la Figura 28 en la página 184 se muestra una serie de documentos XML que se transforman en documentos ROD.

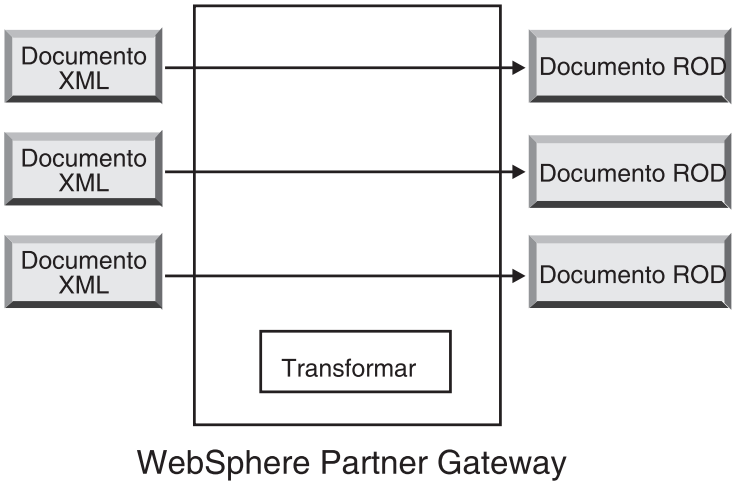


Figura 28. Flujo de documento XML a documento ROD

El documento puede transformarse en un solo documento o en varios documentos, si se ha utilizando un encadenamiento de transacciones para crear la correlación.

Flujo de XML a XML o de ROD a ROD

WebSphere Partner Gateway puede recibir un documento XML o ROD desde un socio o desde un socio interno, transformarlo en un documento del mismo tipo (de XML a XML, o de ROD a ROD) y, a continuación, enviárselo al socio o al socio interno.

En la Figura 29 se muestran documentos XML que se transforman en documentos XML de un formato distinto.

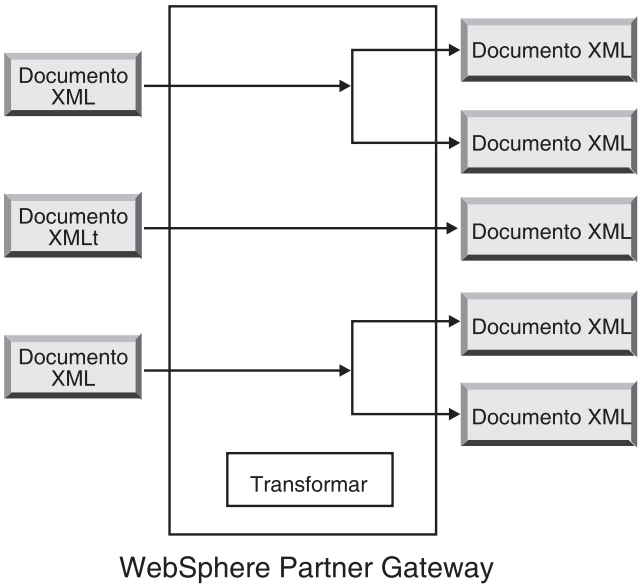


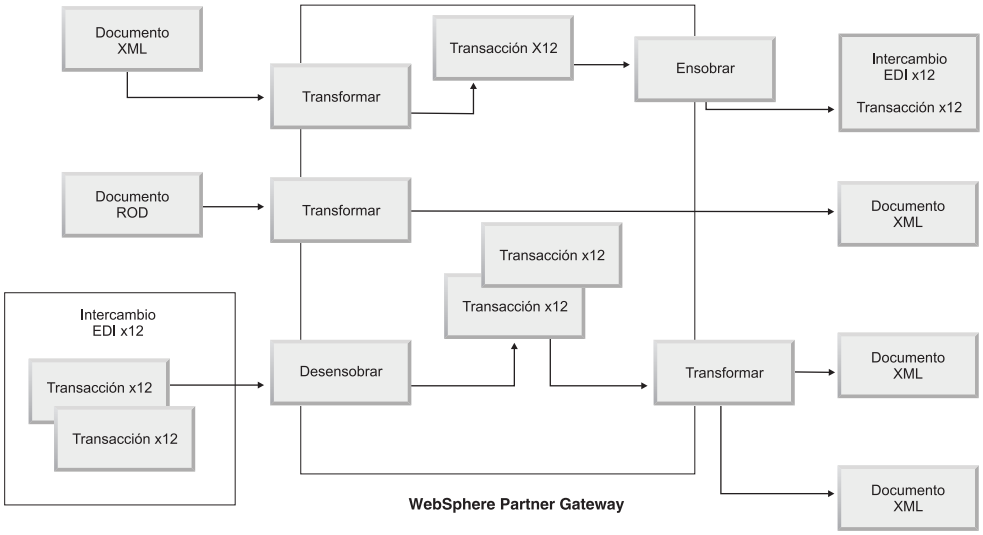
Figura 29. Flujo de documento XML a documento XML

El documento puede transformarse en un solo documento o en varios documentos, si se ha utilizando un encadenamiento de transacciones para crear la correlación.

De cualquier a cualquier flujo

WTX permite transformar cualquier formato en cualquier formato. El estudio de diseño se utiliza para crear correlaciones. Los diferentes flujos son De ROD a cualquier, De XML a cualquier y De EDI a cualquier. Siempre que sea necesario configure el divisor para partir los documentos. En caso de que ROD sea el documento fuente, también debe establecerse la información de direccionamiento. Los formatos XML proporcionan la información de direccionamiento necesaria si el XML es el documento fuente. Las diferentes acciones para los distintos flujos son:

- De ROD a cualquier: transformación WTX
- De XML a cualquier: transformación WTX
- De EDI a cualquier: desensobrador de EDI si desea desensobrar el intercambio. A continuación acciona el reensobrador de EDI y la transformación WTX se utiliza para reensobrar las transacciones y transformarlas en cualquier formato de EDI. Realice una validación de EDI si las transacciones lo requieren. Utilice la validación de intercambio EDI si desea validar el intercambio sin desensobrar.



Visión general de los motores de transformación

WebSphere Partner Gateway da soporte a dos motores de transformación diferentes: WDI y WTX nativos.

WDI nativos: las correlaciones de transformación se crean en el cliente DIS para los WDI nativos. Las diversas acciones que proporciona WebSphere Partner Gateway para la integración con WDI son: Desensobrado EDI, Traducción EDI, Reensobrado EDI, Ensobrado EDI, Traducción ROD y Traducción XML. No se necesita ninguna otra configuración para la integración ya que es WDI nativa.

WTX: las correlaciones de transformación se crean mediante el estudio de diseño de WTX. Las diversas acciones que proporciona WebSphere Partner Gateway para la integración con WTX son Transformación WTX, Validación de intercambio EDI, Desensobrado EDI, Validación EDI, Reensobrado EDI y Ensobrado EDI. RMI y nativo son dos enfoques de WTX. RMI se recomienda en caso que WTX no esté instalado en la misma máquina que WebSphere Partner Gateway. Los paso para invocar remotamente WTX son los siguientes:

1. En el directorio DTXHome, abra el archivo de propiedades rmiserver.propertiesy modifique las propiedades. Por ejemplo, puede establecer el número de puerto.
2. Desde el directorio DTXHome, ejecute startrmiserver.bat.
3. En las propiedades comunes de la consola, proporcione el nombre de host (donde se ejecuta el servidor RMI) y el número de puerto. Establezca la opción de servidor RMI a Sí.
4. Proporcione la ubicación física del mapa.

Para un enfoque nativo, establezca la vía de acceso del sistema como directorio padre de WTX. Además, establezca la propiedad No para rmiuseserver.

transacciones de sobre desde programas de fondo

Cuando utilice WTX en caso asíncrono, la aplicación de fondo consume las transacciones EDI generadas por WTX y las envía a WebSphere Partner Gateway para ensobrarlas con el paquete estándar de fondo. Las cabeceras de fondo predeterminadas se utilizan para proporcionar información de una transacción (x-aux-senderid, x-aux-receiverid, x-aux-protocol, x-aux-protocol-version, x-aux-process-type, x-aux-process-version, y x-aux-docSyntax). Los paquetes de fondo contendrán información acerca del diccionario/protocolo EDI (por ejemplo X12v4R1), Docsyntax (EDI_transaction) y acerca de la transacción del proceso (por ejemplo 850) contra las cabeceras especificadas anteriormente. Consulte la sección de acciones del sobre WTX.

Cómo se procesan los intercambios EDI

Normalmente un intercambio EDI recibido en el concentrador se desensobra y se procesan las transacciones individuales. A menudo, las transacciones EDI (como por ejemplo X12 850 o EDIFACT ORDERS, que representa un pedido de compra) se transforman en un formato que una aplicación de fondo pueda entender. Además, se suele enviar un acuse de recibo funcional al socio para indicar que se ha recibido el intercambio. El intercambio de intercambios EDI, por lo tanto, requiere diversas acciones (Desensobrar EDI, Conversión de EDI, Validación de EDI, Sobre EDI, Intercambio de validación de EDI, Reensobrar EDI, Transformación WTX, y Sobre WTX). Por ejemplo, si el intercambio contiene dos transacciones y no es necesario ningún acuse de recibo, WebSphere Partner Gateway lleva a cabo las siguientes acciones:

1. Desensobra el intercambio

   WebSphere Partner Gateway extrae información sobre el intercambio de los segmentos de cola y cabecera del sobre en los niveles de intercambio, grupo y transacción. Esta información puede incluir:

   - En el nivel de intercambio, los identificadores de empresa de los socios que envían y reciben, el indicador de utilización, que especifica si el intercambio tiene como destino un entorno de producción o uno de pruebas y la fecha y hora en que se preparó el intercambio
   - En el nivel de grupo, los identificadores de aplicación del remitente y receptor y la fecha y la hora en que se preparó el grupo
   - En el nivel de transacción, el tipo de transacción (como X12 850 o EDIFACT ORDERS)
   - Si la validación es necesaria para las transacciones individuales, el EDI se desensobra. Una vez finaliza la validación, las transacciones validadas se ensobran y se envían al motor de transformación (WDI o WTX para procesar) o al destino en función de la acción.

2. Transforma la primera transacción de acuerdo con la correlación asociada a la misma.
3. Transforma la segunda transacción de acuerdo con la correlación asociada a la misma.
4. Entrega los documentos transformados a la aplicación de fondo.

Asimismo, cuando el concentrador envía un documento o documentos que se han originado en la aplicación de fondo del socio interno, los documentos se transforman en transacciones EDI estándar. Las transacciones EDI resultantes son ensobradas antes de ser enviadas al socio. Al igual que en el caso de la recepción de un intercambio EDI, para crear, ensobrar y enviar un intercambio EDI se requieren varias acciones.

Las transacciones, grupos e intercambios individuales se identifican mediante números de control. WebSphere Partner Gateway establece estos números cuando tiene lugar un intercambio. Puede personalizar los números de control, no obstante, tal y como se describe en el apartado "Números de control" en la página 201.

En la ilustración siguiente se muestra una imagen global de cómo se envía un intercambio EDI, empaquetado como AS, de un socio con el objetivo final de entregar dos documentos XML transformados a dos destinos distintos en el sistema de programa de fondo del socio interno. En este ejemplo, las transacciones 850 se transforman en pedidos de compra que una aplicación de fondo pueda procesar. Las transacciones 890 se transforman en órdenes de envío de almacén que la aplicación de proceso de fondo puede procesar.

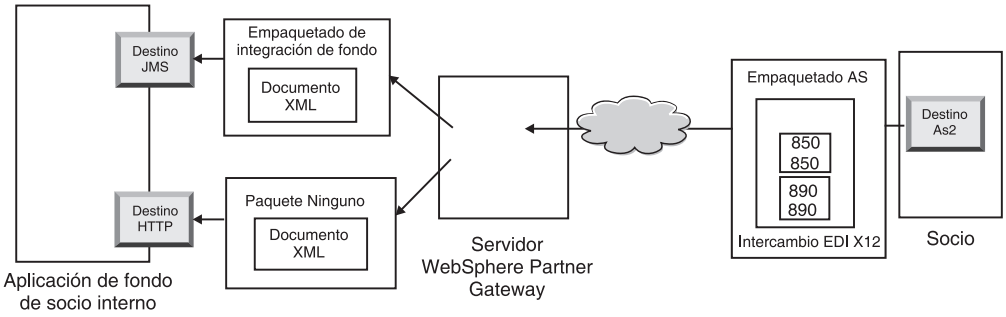


Figura 30. Flujo general de un socio al socio interno

En lugar de una conexión del socio al socio interno, este intercambio necesita tres conexiones:

- Una desde el socio al concentrador para desensobrar el intercambio. Puesto que este es un paso intermedio (el intercambio se desensobra pero no se entrega al socio), el lado de destino de la conexión del socio es N/D (no disponible).

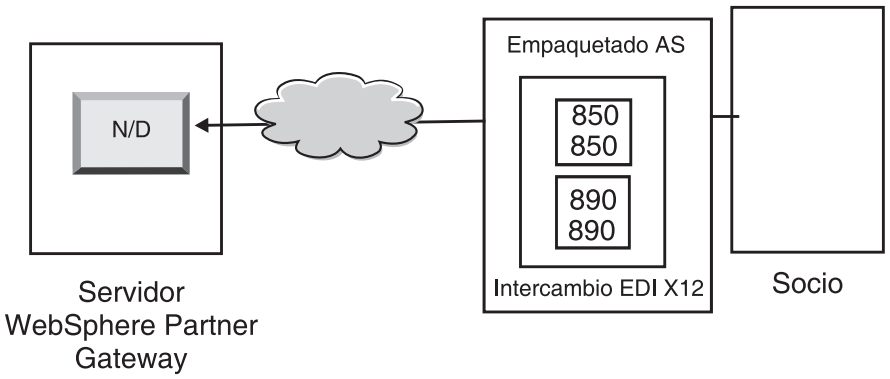


Figura 31. La conexión de desensobrado

- Una para la primera transacción que se va a transformar y entregar al destino JMS del socio interno y otra para la segunda transacción que se va a transformar y enviar al destino HTTP del socio interno.

  Para las transacciones, el paquete de origen no es aplicable porque las transacciones llegaron en el intercambio original que el sistema desensobró. Por lo tanto, el lado de origen de las transacciones debe tener **Empaquetado: N/D** especificado en la conexión del socio.

  Para la transacción que se transforme en XML y que fluya a la aplicación de fondo a través de JMS, el destino en la conexión de socio de esta transacción se debe especificar como el destino JMS del socio interno. Para la transacción que fue transformada en XML y que fluirá a la aplicación de fondo a través de HTTP, el destino de la conexión de socio de esta transacción debe ser especificado como el destino HTTP.

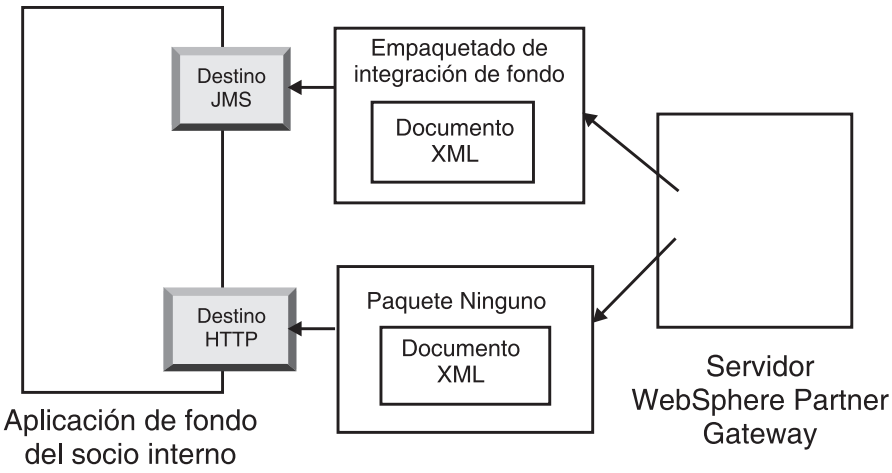


Figura 32. Conexiones para transacciones individuales

Puede utilizar el Visor de documentos para ver el intercambio y las transacciones individuales, que en lo que se refiere al Visor de documentos, son los *hijos* del intercambio. Con el Visor de documentos, puede visualizar los hijos asociados a un intercambio de origen o destino, así como los sucesos asociados con ellos. El visor de documentos se describe en el apartado "Visualización de sucesos y documentos" de la publicación *Guía del administrador de WebSphere Partner Gateway*.

Si el remitente solicita acuses de recibo, será necesario disponer de conexiones adicionales:

- Una para cada uno de los acuses de recibo enviados al socio. Los acuses de recibo funcionales son generados por el sistema y, por lo tanto, en el origen de la conexión de socio debería haberse especificado **Paquete: N/D**. Los acuses de recibo funcionales son ensobrados antes de ser entregados y, por lo tanto, en el destino la conexión de socio debe tener también **Paquete: N/D**. El ensobrador reúne estos acuses de recibo de acuerdo con una planificación establecida. Consulte el apartado "Ensobrador" en la página 192 para obtener más información acerca de la planificación.
- Una para ensobrar los acuses de recibo antes de devolverlos al socio. El sobre es generado por el sistema y, por lo tanto, en el origen de la conexión de socio debe haberse especificado **Paquete: N/D**. En el destino de la conexión de socio debe haberse especificado el destino como el destino del socio y, en este caso, haber especificado **Paquete: AS**. Puede utilizar un sobre predeterminado para el estándar EDI o puede personalizar sobres. Consulte el apartado " Perfiles de sobre" en la página 194 para obtener información sobre cómo personalizar sobres.

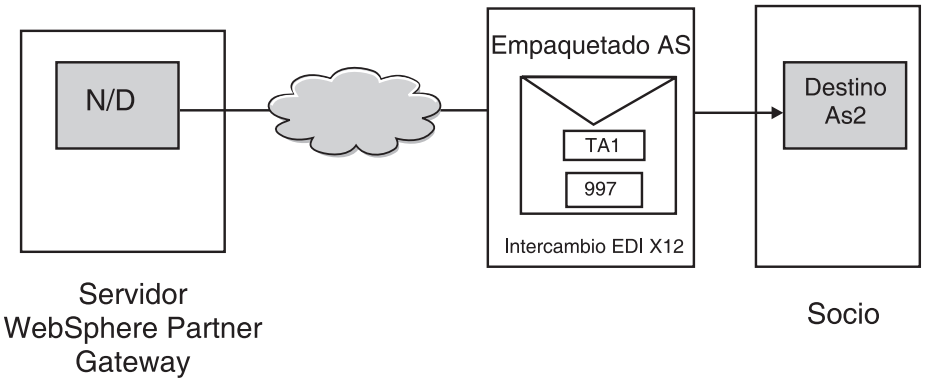


Figura 33. Ensobrado y envío de acuses de recibo al originador

Transformación síncrona

WTX ofrece posibilidades para transformar cualquier formato a otro formato mediante una única correlación. Se proporciona una opción para llamar directamente al API de WTX para la transformación. La transacción desensobrada y validada se envía a WTX para procesar después de ensobrar.

Nota: Consulte el apartado "Visión general de EDI" en la página 173para obtener información acerca de los formatos de EDI disponibles.

Una salida: el atributo de redireccionamiento determina si el documento de salida debería reintroducirse en el flujo de trabajo o enviarse directamente al flujo de trabajo saliente para que se procese.

Diversas salidas: basado en el distintivo de redireccionamiento, el hijo se pasará directamente al flujo de trabajo saliente o se redireccionará en el flujo de trabajo entrante fijado para que pase a través de un canal nuevo.

Transformación asíncrona

Cuando un socio interno envía un mensaje a un socio externo de manera asíncrona, el socio externo puede utilizar WESB/WMB o WTX para la transformación. No se necesita configuración ya que WTX se considera un destino JMS. WTX envía el documento después de procesar al fondo y no hay un flujo de

retorno a WebSphere Partner Gateway. El documento EDI se marcará como Enviado después de entregarse a la pasarela JMS.

Cómo se procesan los documentos XML o ROD

Un documento XML o ROD se recibe en el concentrador como un documento individual o como un grupo de documentos en el mismo archivo. Cuando se recibe un grupo de documentos en el mismo archivo en el concentrador, WebSphere Partner Gateway lleva a cabo las siguientes acciones:

1. Divide el conjunto de documentos en documentos individuales.
2. Transforma cada documento de acuerdo con la correlación asociada al mismo.
3. Si los documentos se transforman en transacciones EDI, ensobrará las transacciones y las entregará a la aplicación de fondo. Si los documentos se transforman en documentos XML o ROD, entregará los documentos transformados a la aplicación de fondo.

Si el documento XML o ROD se recibe como un solo documento, WebSphere Partner Gateway realiza las siguientes acciones:

1. Transforma el documento de acuerdo con la correlación asociada al mismo.
2. Si el documento se transforma en una transacción EDI, ensobrará la transacción y la entregará a la aplicación de fondo. Si el documento se transforma en otro documento XML o ROD, el documento se entregará a la aplicación de fondo.

Asimismo, cuando el concentrador envía un documento o documentos que se han originado en la aplicación de fondo del socio interno, los documentos se transforman en documentos XML o ROD, o en transacciones EDI. Con las transacciones EDI, las transacciones son ensobradas antes de ser enviadas al socio. Al igual que en el caso de la recepción de un intercambio EDI, se requieren varias acciones para transformar el documento o los documentos, ensobrar las transacciones resultantes y enviar el intercambio EDI.

Cómo ensobrar la integración WTX y la correlación polimórfica

En WebSphere Partner Gateway, se define el árbol de tipo de metadatos. Puede configurar y proporcionar información acerca del tipo de datos en cada tarjeta. Normalmente se espera que se configuren las propiedades siguientes. Los nombres de propiedades y valores distinguen entre mayúsculas y minúsculas. Los valores booleanos son los únicos que no distinguen entre mayúsculas y minúsculas.

Tabla 27. Propiedades del árbol de tipo de metadatos

Nombre de la propiedad	Valor de la propiedad	Descripción
BCG_DOCSYNTAX	EDI_INTERCHANGE EDI_TRANSACTION XML ROD	Debe establecerse EDI_INTERCHANGE si la salida es un intercambio EDI ensobrado. Debe establecerse EDI_TRANSACTION si la saalida es una transacción EDI y no está ensobrado. Debe establecerse XML y ROD para la salida XML y ROD respectivamente.
BCG_REENVELOPE	verdadero/falso	Si el valor es verdadero y BCG_DOCSYNTAX es EDI_INTERCHANGE, el sobre EDI se desensobrará. Después de desensobrar, cada transacción que se haya producido se considerará como documento individual para pasos posteriores.

Tabla 27. Propiedades del árbol de tipo de metadatos (continuación)

Nombre de la propiedad	Valor de la propiedad	Descripción
BCG_REROUTE	verdadero/falso	Si el valor es verdadero, el documento se redireccionará. Si es falso y la salida es única, el BDO existente se actualizará con el archivo nuevo y se enviará.
ProtocolName	Según convenga	El nombre del protocolo del documento de salida. Obligatorio en caso de que el redireccionamiento se establezca en verdadero. Esto se utilizará para recoger el canal del documento redireccionado.
ProtocolVersion	Según convenga	La versión del protocolo del documento de salida. Obligatorio en caso de que el redireccionamiento se establezca en verdadero. Esto se utilizará para recoger el canal del documento redireccionado.
ProcessCode	Según convenga	El código de proceso del documento de salida. Obligatorio en caso de que el redireccionamiento se establezca en verdadero. Esto se utilizará para recoger el canal del documento redireccionado.
ProcessVersion	Según convenga	La versión del proceso del documento de salida. Obligatorio en caso de que el redireccionamiento se establezca en verdadero. Esto se utilizará para recoger el canal del documento redireccionado.
SegmentCountElementName	SE01/UNT01	Si la salida es EDI_TRANSACTION, deberemos especificar este atributo. Dicho atributo deberá establecerse en función del tipo de sobre deseado.
SegmentCount	Según convenga	Si la salida es EDI_TRANSACTION, deberemos especificar este atributo. Este atributo dispondrá de la información acerca del número de segmentos de la transacción.

Si el destino es EDI después de la transformación, debe ensobrarse antes de enviarse a socios externos. El documento de salida transformado puede tener cualquier combinación de formatos. Esto depende de qué se codifique en el número de tarjeta de la tarjeta de metadatos. Esto contendrá las propiedades de otros detalles de la tarjeta. El creador de la correlación codificará la tarjeta. Los distintos atributos que se consideran son ReRoute, ReEnvelope y DocSyntax. ReRoute y ReEnvelope pueden tener valores de Verdadero o Falso, mientras que whereas DocSyntax puede tener cualquier valor que introduzca el usuario. Únicamente si el valor de DocSyntax es ediInchg, se tendrá en cuenta para el desensobrado. A continuación se explica el posible resultado de las distintas combinación de los valores Redireccionar y Reensobrar. Se asume que se establece docSyntax a EDI_INTERCHANGE:

- ReRoute = Verdadero, ReEnvelope = Falso: el documento se procesa de una manera similar a cualquier otro documento (XML o ROD).
- ReRoute = Falso, ReEnvelope = Falso: el documento se procesa de manera similar a cualquier otro documento (XML o ROD).
- ReRoute = Verdadero, ReEnvelope = Verdadero: el documento se desensobra primero. Para cada una de las transacciones hijo, se crea un hijo bdo. El diccionario y el documento se establecen como protocolo y proceso. Cada (transacción) ChildBDO se redirecciona con el paquete N/D. Debe haber un canal adecuado. El perfil del ensobrador se puede configurar en los atributos de destino de este canal. Debe crearse un canal separado para que el sobre fluya.

- ReRoute = Falso, ReEnvelope = Verdadero: se desensobra primero el documento. Si se produce una sola transacción como entrada, el documento empresarial se actualiza con el archivo de la transacción cuando de envía la ubicación. Si se producen diversas transacciones como salida, no se crean los BDO hijo para ningún registro y se envían. Se espera que el atributo de destino de este canal se configure adecuadamente para el perfil del ensobrador. Debe haber un canal para que el Ensobrador fluya.

Configuración del entorno EDI

Tal como se ha mencionado en el apartado anterior, puede especificar muchos atributos que pertenecen al intercambio de intercambios EDI. Por ejemplo, puede cambiar los perfiles de sobres proporcionados por el producto, puede definir sobres específicos para utilizarlos con determinadas conexiones, puede establecer números de control asignados a las distintas partes de un intercambio y puede establecer perfiles de conexiones para que pueda entregarse el mismo intercambio de distintas maneras. Estas tareas se describen en este apartado.

Ensobrador

El ensobrador es el componente que reúne un conjunto de transacciones que deben enviarse a un socio, las envuelve en un sobre y las envía. El ensobrador puede planificarse (o aceptar la planificación predeterminada) para indicar a WebSphere Partner Gateway cuándo desea que el ensobrador busque transacciones que estén esperando ser enviadas. También puede actualizar los valores predeterminados para el tiempo de bloqueo, el tiempo en cola y la modalidad de proceso por lotes.

Nota: la configuración del ensobrador es opcional. Si no cambia ninguno de los valores del ensobrador, se utilizarán los valores predeterminados proporcionados por el producto.

Bloqueo

Cada instancia del Gestor de documentos tiene su propio ensobrador. Si hay dos gestores de documentos instalados en el sistema, tendrá dos ensobradores. Es posible, por lo tanto, que dos (o más) instancias de un ensobrador intenten sondear si hay transacciones esperando ser ensobradas. Para asegurarse de que una transacción dada es sondeada únicamente por un ensobrador, se utilizan bloqueos. Los bloqueos garantizan que si hay implicados varios ensobradores, sólo uno sondea y procesa una transacción dada. Los ensobradores efectúan el sondeo simultáneamente, pero procesan en distintas transacciones.

Se establece un tiempo límite en el bloqueo. El valor predeterminado durante el que una instancia del ensobrador puede mantener un bloqueo es de 240 segundos.

Si el ensobrador tiene que esperar a que el bloqueo esté disponible, se coloca en una cola. El tiempo máximo en cola (el periodo de tiempo que el ensobrador debe esperar) es de 740 segundos.

En general, no es necesario cambiar ninguno de los valores predeterminados para el bloqueo.

Modalidad de proceso por lotes

Cuando llegan varios documentos en un archivo, éstos se dividen de acuerdo con el manejador de divisor que se haya configurado para dicho tipo de documento. (La configuración de manejadores de divisor, que forma parte de la definición de destinos, se describe en el apartado “ Modificación de puntos de configuración” en la página 77). Uno de los atributos del manejador de divisor es

BCG_BATCHDOCS. Cuando BCG_BATCHDOCS está establecido en activo (el valor predeterminado), el divisor añade varios ID de lote a los documentos después de dividirlos.

El ensobrador tiene un atributo para la modalidad de proceso por lotes, que está relacionado con el atributo BCG_BATCHDOCS. Si se asignaron ID de proceso por lotes a documentos individuales y acepta el valor predeterminado (activada) para la modalidad de proceso por lotes, el ensobrador se asegura de que todos los documentos que lleguen juntos en el mismo archivo se procesen antes de ensobrarlos y enviarlos, para asegurarse de que las transacciones se ensobran juntas. Por ejemplo, suponga que cinco documentos XML llegan en el mismo archivo. Los documentos XML deben transformarse en transacciones EDI y está previsto que se entreguen al mismo destinatario. Una vez que se han transformado sólo tres de los documentos, el ensobrador empieza su sondeo de transacciones planificado. Si se selecciona una modalidad de proceso por lotes, el ensobrador no procesa (ensobra) las tres transacciones que están listas. En lugar de ello, espera a que hayan terminado de procesarse las cinco transacciones antes de ensobrarlas y enviarlas. Las transacciones se ponen en el mismo sobre, a menos que el estándar EDI aplicable lo impida.

Modificación de los valores predeterminados

Acerca de esta tarea

Para modificar alguno de los valores predeterminados para el ensobrador, realice los pasos siguientes:

1. Pulse **Administración del concentrador > Configuración del concentrador > EDI > Ensobrador**.
2. Pulse el icono **Editar**.
3. Especifique valores nuevos para **Tiempo máximo de bloqueo (segundos)** y **Tiempo máximo en cola (segundos)** si desea asignar más o menos tiempo a estos atributos.

   Nota: en general, no es necesario cambiar ninguno de los valores predeterminados.
4. Si desea desactivar la modalidad de proceso por lotes, elimine la marca que hay junto a **Utilizar modalidad de proceso por lotes**.
5. Si desea cambiar la frecuencia con la que el ensobrador comprueba las transacciones que esperan ser enviadas, lleve a cabo uno de los siguientes conjuntos de tareas:
   - Para utilizar la planificación basada en intervalos (que es el valor predeterminado) pero cambia el periodo de tiempo, especifique un nuevo periodo junto a **Intervalo**. Por ejemplo, si cambia el valor a 30 segundos, el ensobrador comprobará la existencia de documentos cada 30 segundos, ensobrará dichos documentos y los enviará al destinatario.
   - Para utilizar la planificación basada en calendario, realice las siguientes tareas:
     a. Pulse **Planificación basada en calendario**.
     b. Elija el tipo de planificación (**Planificación diaria**, **Planificación semanal** o **Planificación personalizada**).
        – Si selecciona **Planificación diaria**, seleccione la hora del día (hora y minutos) en que el ensobrador debe comprobar si hay documentos.
        – Si elige **Planificación semanal**, seleccione uno o varios días de la semana además de la hora del día.

– Si elige **Planificación personalizada**, seleccione la hora del día y luego **Rango** o **Días selectivos** para la semana y el mes. Con **Rango**, indique la fecha de inicio y la fecha de finalización. (Por ejemplo, puede pulsar **Lunes** y **Viernes** si desea que el ensobrador compruebe si hay documentos a una determinada hora únicamente los días laborables). Con **Días selectivos** puede elegir los días concretos de la semana y del mes.

6. Pulse **Guardar**.

Perfiles de sobre

Un perfil de sobre determina los valores que se colocan en elementos específicos del sobre. Asigne el perfil de sobre a las transacciones EDI en el atributo **Perfil de sobre** de la definición de documento. WebSphere Partner Gateway proporciona un perfil de sobre predefinido para cada estándar soportado (X12, EDIFACT o UCS). Estos sobres predefinidos pueden utilizarse directamente, modificarse o copiarse en nuevos perfiles de sobre. Los pasos para modificar un perfil de sobre o para crear uno se describen en el apartado “Modificación de los valores predeterminados” en la página 195.

Los perfiles de sobres tienen un campo para cada elemento en el estándar de sobre. Los perfiles proporcionan datos literales o constantes para crear segmentos de cabecera o cola para conjuntos de transacciones, mensajes, grupos funcionales e intercambios. Sólo debe proporcionar los valores que es necesario rellenar y para los que no proporciona un valor algún otro font.

Los nombres de campo se han diseñado para facilitar la referencia cruzada. Por ejemplo, el campo UNB03 es el tercer elemento de datos en el segmento UNB.

Como se describe en el apartado “ Atributos de sobre”, los atributos establecidos en cualquier parte tienen prioridad sobre los valores establecidos en el perfil de sobre. Algunos de los atributos pueden ser alterados temporalmente en los atributos o correlaciones relacionados con definiciones.

Atributos de sobre

Durante el proceso de configuración, los atributos de sobre se pueden establecer en varios puntos diferentes y también pueden establecerse en la correlación de transformación asociada con el intercambio de documentos. Por ejemplo, el especialista de correlaciones de Data Interchange Services Client puede especificar la propiedad CtlNumFlag al definir una correlación. Esta propiedad también puede establecerse como parte del perfil de sobre (en el campo **Números de control por ID de transacción**). Todos los atributos establecidos en la correlación de transformación alteran temporalmente los valores relacionados establecidos en la Consola de comunidad. Por ejemplo, si CtlNumFlag se establece en la correlación de transformación en el valor **N** (no) y se especifica un valor **S** (sí) en el campo **Números de control por ID de transacción**, se utiliza el valor **N**.

Pueden establecerse otros perfiles de sobre en el nivel del protocolo (desde la página Gestionar definiciones de documento o desde la página de funciones B2B asociada con un socio), o pueden establecerse como parte de la conexión. El orden de prioridad se indica en la siguiente lista:

1. Las propiedades establecidas en la correlación de transformación tienen prioridad sobre los atributos asociados establecidos en la Consola de comunidad.
2. Los atributos establecidos en el nivel de conexión tienen prioridad sobre los establecidos en el nivel de funciones B2B.

3. Los atributos establecidos en el nivel de funciones B2B tienen prioridad sobre los establecidos en el nivel de definición de documento.
4. Los atributos establecidos en cualquier parte (en la correlación de transformación o en la definición de documento, funciones B2B o en el nivel de conexión) tienen prioridad sobre los valores establecidos en el perfil de sobre.

Si desea obtener una lista de propiedades de correlaciones de transformación y sus atributos de Consola de comunidad asociados, consulte el apartado "Propiedades de Data Interchange Services Client" en la página 447.

Modificación de los valores predeterminados

Acerca de esta tarea

En el apartado " Atributos de perfil de sobre" en la página 435 encontrará una tabla que muestra los valores predeterminados utilizados para cada atributo de sobre estándar EDI, si no especifica ningún valor en el perfil o si no crea un perfil. Asegúrese de que los perfiles de sobre que utiliza suministran todos los elementos obligatorios que no proporciona el sistema durante la ejecución.

Para configurar el perfil de sobre, siga estos pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Perfil de sobre**.
2. Lleve a cabo uno de los conjuntos de pasos siguientes:
   - Cree un sobre
     a. Pulse **Crear**.
     b. Escriba un nombre para el perfil de sobre. Es el nombre que aparecerá en la lista Perfiles de sobre.
     c. Si lo desea, escriba una **Descripción** del perfil.
     d. Pulse el **Estándar EDI** al que pertenece el sobre. Por ejemplo, si está intercambiando documentos que cumplen el estándar EDI-X12, seleccione **X12**.
   - Modifique un sobre
     a. Seleccione uno de los perfiles de sobre existentes pulsando el icono **Ver detalles** situado junto al nombre del perfil.
     b. Pulse el icono **Editar**.
3. El botón **General** está seleccionado de manera predeterminada. Puede especificar un valor en cada campo, a excepción de ENVTYPE, que se rellena con el estándar que se ha seleccionado en el paso 2d.

   Puede añadir valores para los siguientes campos:
   - **Longitud de número de control de intercambio**, para indicar cuántos caracteres deben utilizarse cuando se asigna un número de control a un intercambio dentro del sobre.
   - **Longitud de número de control de grupo**, para indicar cuántos caracteres deben utilizarse cuando se asigna un número de control a un grupo dentro del sobre.
   - **Longitud de número de control de transacción**, para indicar cuántos caracteres deben utilizarse cuando se asigna un número de control a una transacción dentro del sobre.
   - **Número máximo de transacciones**, para indicar el número máximo de transacciones que se permite en este sobre.
   - **Números de control por ID de transacción**, para indicar si desea utilizar el ID de transacción (como parte de la clave) cuando se buscan los números

establecidos en la base de datos. En caso afirmativo, para cada ID de transacción se utilizarán distintos conjuntos de números de control.

Los campos del perfil de sobre General son los mismos en los tres estándares, a excepción de EDIFACT que tiene un campo adicional: **Crear grupos para EDI**.

Si desea realizar algún cambio en la página General, pulse **Guardar**.

4. Para especificar valores para el intercambio, pulse **Intercambio**. En la página aparece un nuevo conjunto de campos. Los campos varían, en función del estándar EDI. Recuerde que alguno de los valores ya están rellenados o se rellenarán durante la ejecución.
   - Para el estándar EDI-X12, puede cambiar los siguientes campos:
     - **ISA01 Calificador de información de autorización**, que es un código para el tipo de información en ISA02.
     - **ISA02 Información de autorización**, que es la información utilizada para identificar o autorizar adicionalmente al remitente de los datos de intercambio.
     - **ISA03 Calificador de información de seguridad**, que es un código para el tipo de información en ISA04. Los valores válidos son:

       00 ISA04 no es significativo

       01 ISA04 contiene una contraseña
     - **ISA04: Información de seguridad**, que es la información de seguridad sobre los datos del intercambio o remitente. El código de ISA03 define el tipo de información.
     - **ISA11: ID de estándares de intercambio**, que es un código para la agencia que controla el intercambio. Los valores válidos son: **U** (Comunidad US EDI de ASC X12), **TDCC** y **UCS**.

       Nota: este atributo se utiliza para las versiones X12 a 4010. En X12 4020, se utiliza el elemento ISA11 para el separador de repetición.
     - **ISA12 ID de versión de intercambio**, que es el número de versión de la sintaxis utilizada en los segmentos de control de grupo funcional e intercambio.
     - **ISA14: Acuse de recibo solicitado**, que es el código del remitente para solicitar un acuse de recibo. Los valores válidos son:

       0 No solicitar ningún acuse de recibo

       1 Solicitar un acuse de recibo de que se han recibido y reconocido los segmentos ISA y IEA.
     - **ISA15: Indicador de prueba**, que es una indicación de qué intercambio es de prueba o de producción. Los valores válidos son:

       T Para datos de prueba

       P Para datos de producción
   - Para el estándar UCS, puede cambiar los siguientes campos:
     - **BG01: ID de comunicaciones**, que es la identificación de la empresa que transmite.
     - **BG02: Contraseña de comunicaciones**, que es una contraseña que asigna el receptor, para ser utilizada por los socios de la forma acordada.
   - Para el estándar EDIFACT, puede cambiar los siguientes campos:
     - **UNB0101: ID de sintaxis**, que es la Identificación de la agencia que controla la sintaxis que se utiliza. La agencia controladora es UNO. El nivel es A o B.

- **UNB0102: Versión de sintaxis**, que es el número de versión de la sintaxis identificada por el ID de sintaxis.
- **UNB0601: Referencia/contraseña de receptores**, que es una contraseña asignada por el receptor y que será utilizada de la forma acordada por los socios.
- **UNB0602: Calificador de referencia/contraseña de receptores**, que es un calificador para la contraseña del receptor y que será utilizado según acuerden los socios.
- **UNB07 Referencia de aplicación**, que es la identificación del área funcional del remitente con la que están relacionados los mensajes de intercambio.
- **UNB08: Prioridad**, que es el código del remitente para la prioridad de proceso, tal como se ha acordado con el socio. El código A es la prioridad más alta.
- **UNB09: Solicitud de acuse de recibo**, que es el código del remitente para solicitar un acuse de recibo.
- **UNB10: ID de acuerdo de comunicaciones**, que es el nombre o código del tipo de acuerdo utilizado para este intercambio, tal como se ha acordado con el socio.
- **UNB11: Indicador de prueba (indicador de prueba)**, que es una indicación de que el intercambio es de prueba. 1 indica un intercambio de prueba.

Si desea realizar algún cambio en la página Intercambio, pulse **Guardar**.

5. Para especificar valores para los grupos dentro del intercambio, pulse **Grupo**. Aparece un nuevo conjunto de campos. Los campos varían, en función del estándar EDI.

   Los campos de esta página generalmente definen el remitente y el receptor del grupo.

   - Para los estándares EDI-X12 y UCS, puede especificar valores en los siguientes campos:
     - **GS01: ID de grupo funcional**, que es una identificación del tipo de conjuntos de transacciones en el grupo.
     - **GS02: Remitente de aplicación**, que es el nombre o código para un departamento específico de la empresa del remitente.
     - **GS03: Receptor de aplicación**, que es el nombre o código para el departamento específico de la empresa del receptor que va a recibir el grupo.
     - **GS07: Agencia de grupo**, que es un código utilizado con GS08 para identificar la agencia que controla el estándar.
     - **GS08: Versión de grupo**, que es un código para la versión, el release y el sector del estándar.
   - Para el estándar EDIFACT, puede especificar valores en los siguientes campos:
     - **UNG01: ID de grupo funcional**, que es una identificación del tipo de mensajes en el grupo.
     - **UNG0201: ID de remitente de aplicación**, que es el nombre o código para un departamento específico de la empresa del remitente.
     - **UNG0202: Calificador de ID de remitente de aplicación**, que es el calificador para el código de ID de remitente. Consulte el directorio de elementos de datos para obtener una lista de calificadores de código.

- **UNG0301: ID de receptor de aplicación**, que es el nombre o código para el departamento específico de la empresa del receptor que va a recibir el grupo.
- **UNG0302: Calificador de ID de receptor de aplicación**, que es el calificador para el código de ID de receptor. Consulte el directorio de elementos de datos para obtener una lista de calificadores de código.
- **UNG06: Agencia controladora**, el código que identifica la agencia que tiene control del tipo de mensaje en el grupo funcional.
- **UNG0701: Versión de mensaje**, que es el número de versión del tipo de mensaje.
- **UNG0702: Release de mensaje**, que es el número de release dentro del número de versión para el tipo de mensaje.
- **UNG0703: Asociación asignada**, es el código que asigna la asociación responsable e identifica aún más el tipo de mensaje.
- **UNG08: Contraseña de aplicación**, que es la contraseña asignada por el departamento específico de la empresa del receptor.

Si desea realizar algún cambio en la página Grupo, pulse **Guardar**.

6. Para especificar valores para las transacciones dentro de un grupo, pulse **Transacción** o, en el caso de EDIFACT, **Mensaje**. Aparece un nuevo conjunto de campos. Los campos varían, en función del estándar EDI.
   - Para el estándar EDI-X12 o USC, puede especificar un valor para **ST03: Cadena de ID de convenio de implementación**.
   - Para el estándar EDIFACT, puede especificar un valor en los siguientes campos:
     - **UNH0201: Tipo de mensaje**, que es un código que asigna la agencia controladora para identificar el tipo de mensaje.
     - **UNH0202: Versión de mensaje**, que es el número de versión del tipo de mensaje.
     - **UNH0203: Release de mensaje**, que es el número de release dentro del número de versión para el tipo de mensaje.
     - **UNH0204: Agencia controladora**, que es un código para la agencia que tiene el control del tipo de mensaje.
     - **UNH0205: Código asignado de asociación**, es el código que asigna la asociación responsable e identifica aún más el tipo de mensaje.
     - **UNH03: Referencia de acceso común**, que es la clave que relaciona todas las transferencias de datos subsiguientes con un archivo común. Los socios pueden acordar utilizar una clave compuesta de componentes, pero no es posible utilizar separadores de subelementos.

   Si desea realizar algún cambio en la página Transacción, pulse **Guardar**.
7. Pulse **Guardar**.
8. Repita los pasos 2 en la página 195 a 7 para cualquier otro perfil de sobre que desee definir o cambiar.

Después de definir un perfil de sobre, éste se lista en la lista Perfiles de sobre. En la lista, seleccione el perfil y pulse el icono **Donde se utiliza** para determinar las conexiones que utilizan el perfil.

Perfiles de conexión

Los perfiles de conexión se utilizan con las transacciones desensobradas y con los intercambios EDI creados por el ensobrador. En las transacciones, el perfil de

conexión determina cómo se procesa la transacción una vez desensobrada. En los intercambios, el perfil de conexión determina cómo se entrega el intercambio.

Utilice la ventana del Perfil de conexión para crear un perfil nuevo o editar la información de perfil existente. El nombre de cada perfil definido actualmente y su descripción, si existe alguna, se muestran en la Lista de perfiles de conexión. Consulte la *Guía de configuración del concentrador de WebSphere Partner Gateway* para obtener más información acerca de los perfiles de conexión.

Transacciones

Cuando un intercambio EDI se recibe en Interchange WebSphere Partner Gateway, la primera acción generalmente es desensobrar el intercambio en transacciones individuales. Cuando se crean las transacciones, la acción Desensobrar establece el **Indicador de uso del intercambio** y la información de grupo (**Identificador de remitente de aplicación de grupo**, **Identificador de receptor de aplicación de grupo** y **Contraseña de aplicación de grupo**) en los metadatos de transacción. A continuación, WebSphere Partner Gateway vuelve a procesar cada transacción en su propio flujo de trabajo.

Suponga que tiene dos transacciones del mismo tipo (por ejemplo, 850) que es necesario manejar de forma distinta, en función del grupo en el que están o de los valores de sus indicadores de uso del intercambio. Si el **Indicador de uso** es Producción (**P**), por ejemplo, podría utilizar una correlación (A) y si el **Indicador de uso** es Prueba (**T**), podría utilizar una segunda correlación (B). Para esta transacción 850 se requieren dos conexiones parecidas; la única diferencia es que una conexión utiliza la correlación A y la otra utiliza la correlación B.

Debido a que las transacciones son iguales (tienen el mismo socio de origen y de destino, paquete, protocolo y tipo de documento), el Gestor de documentos necesita una manera de determinar qué conexión utilizar. Esto lo hace asociando el atributo de perfil de conexión establecido con los metadatos de transacción. En este ejemplo, si crea dos perfiles de conexión, uno (CPProduction) con el **Tipo de utilización de EDI** establecido en **P** y el otro (CPTest) con el **Tipo de utilización de EDI** establecido en **T**, el Gestor de documentos asocia la transacción que tiene el Indicador de uso P con el perfil CPProduction. Entonces sabrá que debe utilizar la correlación A para convertir la transacción.

En el ejemplo de este apartado se ha empleado el atributo **Indicador de uso del intercambio**, aunque también puede utilizar el **Identificador de remitente de aplicación de grupo**, **Identificador de aplicación de receptor de grupo** y **Atributos de contraseña de aplicación de grupo** como factor distintivo de una transacción.

Intercambios

Para los intercambios, utilice el atributo **Calificador 1 de perfil de conexión**.

Por ejemplo, suponga que está en medio del proceso de migrar su empresa que utiliza VAN (paquete Ninguno) o Internet (paquete AS2). Desea que las transacciones 840 (Solicitud de cuota) utilicen VAN y las transacciones 850 (Pedido de compra) utilicen Internet. Establezca dos conexiones de socio, ambas con el mismo intercambio de origen pero con distintos destinos (uno con paquete Ninguno y el otro con paquete AS2). Los perfiles de conexión ayudan a distinguir las dos conexiones.

La configuración del perfil de conexión para intercambios incluye varios pasos. A continuación se indican los pasos que deben realizarse para crear dos perfiles de conexión para el ejemplo:

1. Cree dos conexiones para las transacciones. Establezca el atributo **Calificador 1 de perfil de conexión** en el lado de destino para ambas conexiones. El valor debe ser significativo (por ejemplo, ConNinguno y ConAS2).
2. Defina dos perfiles de conexiones (por ejemplo, CPNinguno y CPAS2), cada uno con el valor de **Calificador1** establecido de modo que coincida con los atributos **Calificador 1 de perfil de conexión** establecidos en el paso 1 (ConNinguno y ConAS2).
3. Cree dos conexiones para el intercambio. Cada conexión tiene el mismo empaquetado de origen (N/D) y un empaquetado de destino distinto (Ninguno y AS2). La conexión de socio con el perfil de conexión CPNinguno tendrá el destino establecido en el destino de FTP Scripting que puede conectarse a la VAN. La conexión de socio con el perfil de conexión CPAS2 tendrá el empaquetamiento de destino configurado como AS.
4. Asocie a cada una el perfil de conexión adecuado.

El ensobrador utiliza el atributo **Calificador 1 del perfil de conexión** en el lado "A" de la conexión de socio como un punto de interrupción del sobre. Por eso, las transacciones que tienen valores diferentes para el atributo **Calificador 1 de perfil de conexión** se ensobrarán en distintos sobres. Cuando se establecen distintos valores para las transacciones, el ensobrador nunca ensobrará las transacciones 840 y 850 en el mismo intercambio.

Cuando el Gestor de documentos busca la conexión, se encuentran las dos conexiones posibles, aunque se utilizará la que coincida con el perfil de conexión.

Configuración de perfiles de conexión

Acerca de esta tarea

La configuración de perfiles de conexión es opcional. Si no es necesario tener más de una conexión para cada tipo de documento que intercambiará con un socio, pase por alto este apartado.

Para configurar un perfil de conexión:

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Perfiles de conexión**.
2. Pulse **Crear perfil de conexión**.
3. En la página Detalles de perfil de conexión, escriba un nombre necesario para este perfil de conexión.
4. Si lo desea, escriba una descripción del perfil.

   El nombre y la descripción (si escriba una descripción) aparecerán en la página Lista de perfiles de conexión.
5. Si lo desea, especifique un valor para **Calificador 1** para indicar el valor que determina qué conexión utilizar para un intercambio EDI. Consulte el apartado " Intercambios" en la página 199 para ver un ejemplo de la utilización de **Calificador 1**.
6. Si lo desea, especifique un valor para **Tipo de utilización de EDI** para indicar si es un intercambio de pruebas, producción o de información. Consulte el apartado " Transacciones" en la página 199 para ver un ejemplo de la utilización de **Tipo de utilización de EDI**.
7. Si lo desea, escriba un valor para **ID de remitente de aplicación** para indicar la aplicación o sección de la empresa asociada al remitente del grupo.
8. Si lo desea, escriba un valor para **ID de receptor de aplicación** para indicar la aplicación o sección de la empresa asociada al receptor del grupo.

9. Si lo desea, escriba un valor para **Contraseña** si se requiere una entre el remitente de aplicación y el receptor de aplicación.
10. Pulse **Guardar**.

Para aquellas transacciones que desee poner en determinados sobres de intercambio, puede especificar el atributo **Calificador 1 del perfil de conexión** que se corresponde con el perfil de conexión con el mismo valor que el atributo **Calificador 1**. El atributo **Calificador 1 del perfil de conexión** puede establecerse en el nivel de protocolo de una definición de documento (por ejemplo, puede editar los atributos del protocolo X12V5R1 en la página Gestionar definiciones de documento para indicar qué perfil de conexión desea utilizar pulsando el valor de atributo **Calificador 1 del perfil de conexión**). A continuación, al activar la conexión del intercambio, asocie el perfil de conexión pulsando el botón **Perfil de conexión** y seleccionando el perfil de la lista.

Números de control

El ensobrador utiliza números de control para proporcionar una numeración única para los intercambios, grupos y transacciones dentro de un sobre. Los números de control se establecen para el socio interno y para los socios externos. Cuando se produce el intercambio de documentos, también se generan los números de control para el *par* de socios.

Para cada socio que tenga posibilidades B2B de EDI, hay un conjunto de valores de inicialización de origen para números de control. Estos valores se utilizan la primera vez que un intercambio EDI se crea y envía entre un par de socios. Los valores de inicialización se aplican al socio al que se envía el intercambio. Cuando un documento se ha enviado de un socio a otro, los últimos números utilizados se pueden ver en la página Números de control actuales. Pueden haber varias entradas para un par de socios si **Números de control por ID de transacción** está establecido en **S**. Cuando una entrada existe, se utiliza para generar nuevos números de control.

Como parte de la inicialización de número de control, puede utilizar máscaras para modificar la creación por parte del ensobrador del número de control normal. Las máscaras se utilizan para basar el número de control en el intercambio o en el número de control de grupo. A continuación se ofrecen las descripciones de las máscaras. Sustituya la *n* en la máscara de edición por el número de bytes que desea utilizar para crear el valor de número de control. En la Tabla 28 encontrará las descripciones de los códigos disponibles.

Tabla 28. Máscaras de número de control

Código	Número de control	Descripción
G	Transacción	El número de control de transacción es el mismo que el número de control de grupo. Sólo se permite una transacción por grupo.
G*n*	Transacción	Se toman *n* bytes del número de control de grupo. El resto del número de control de transacción se rellena con ceros hasta alcanzar el tamaño máximo. Sólo se permite una transacción por grupo.
C	Grupo, Transacción	El resto de bytes del campo del número de control de transacción o de grupo se utilizan para conservar un número de control para ese socio.

Tabla 28. Máscaras de número de control (continuación)

Código	Número de control	Descripción
V	Grupo, Transacción	Se utiliza un valor incremental para que el primer grupo o transacción tenga un valor de 1, el segundo un valor de 2, y así sucesivamente.
V*n*	Transacción	Se utiliza un valor incremental de *n* bytes de longitud para que la primera transacción tenga un valor de 1, la segunda un valor de 2, y así sucesivamente.
G*n*C	Transacción	Se utilizan *n* bytes del número de control de grupo, y el resto de bytes del campo de número de control de transacción se utilizan para conservar un número de control. El número de posiciones que faltan determina el valor máximo del número de control. Por ejemplo, G5C deja cuatro posiciones; por lo tanto, el valor máximo es 9999. El número de control varía cíclicamente del valor máximo a 1.
G*n*V	Transacción	Se toman *n* bytes del número de control de grupo. En el resto de bytes, en el campo de número de control de transacción se utiliza un valor incremental para que la primera transacción tenga un valor de 1, la segunda un valor de 2, y así sucesivamente.
G*n*V*m*	Transacción	Se toman *n* bytes del número de control de grupo. En el resto de bytes, hasta *m* bytes en el campo de número de control de transacción, se utiliza un valor incremental para que la primera transacción tenga el valor de 1, la segunda el valor de 2, y así sucesivamente.
I	Grupo, Transacción	El número de control de transacción o de número debería ser el mismo que el número de control de intercambio. Sólo se permite un grupo para el intercambio y sólo se permite una transacción para el grupo o intercambio.
I*n*	Grupo, Transacción	Se toman *n* bytes del número de control de intercambio. El resto del campo correspondiente número de control de transacción o de grupo se rellena con ceros hasta alcanzar el tamaño máximo. Sólo se permite un grupo para cada intercambio y sólo se permite una transacción para cada grupo.
I*n*C	Grupo, Transacción	Se toman *n* bytes del número de control de intercambio. El resto de bytes del campo de número de control de transacción o de grupo se utilizan para conservar un número de control. El número de posiciones que faltan determina el valor máximo del número de control. Por ejemplo, en I5C faltan cuatro posiciones; por lo tanto, el valor máximo es 9999. El número de control varía cíclicamente del valor máximo a 1.
I*n*V	Grupo, Transacción	Se toman *n* bytes del número de control de intercambio. En el resto de bytes, en el campo de número de control de transacción o de grupo, se utiliza un valor incremental para que el primer grupo o transacción tenga el valor de 1, el segundo el valor de 2, y así sucesivamente.

Tabla 28. Máscaras de número de control (continuación)

Código	Número de control	Descripción
I*n*V*m*	Transacción	Se toman *n* bytes del número de control de intercambio. En el resto de bytes, hasta *m* bytes en el campo de número de control de transacción, se utiliza un valor incremental para que la primera transacción tenga el valor de 1, la segunda el valor de 2, y así sucesivamente.
I*n*G*m*	Transacción	Se utilizan *n* bytes del número de control de intercambio, y un máximo de *m* bytes del número de control de grupo. Si *n* más *m* es superior a 9, sólo se utilizarán 9 - *n* bytes del número de control de grupo. Por ejemplo, si se utiliza I4G6, se toman 4 del intercambio.
I*n*G*m*C	Transacción	Se utilizan *n* bytes del número de control de intercambio, y *m* bytes del número de control de grupo. El resto de bytes del campo de número de control de transacción se utilizan para mantener un número de control. El número de posiciones que faltan determina el valor máximo del número de control. Por ejemplo, I2G4C deja tres posiciones; por lo tanto, el valor máximo es 999. El número de control varía cíclicamente del valor máximo a 1.
I*n*G*m*V	Transacción	Se utilizan *n* bytes del número de control de intercambio, y *m* bytes del número de control de grupo. En el resto de bytes, en el campo de número de control de transacción se utiliza un valor incremental para que la primera transacción tenga un valor de 1, la segunda un valor de 2, y así sucesivamente.
I*n*G*m*V*o*	Transacción	Se utilizan *n* bytes del número de control de intercambio, y *m* bytes del número de control de grupo. Para los bytes restantes, hasta *0* bytes del campo de número de control de transacción, se utiliza un valor incremental de modo que la primera transacción tenga un valor 1, la segunda un valor 2, etc.

Inicialización de número de control

Acerca de esta tarea

Para configurar los números de control que utilizará el ensobrador, lleve a cabo los siguientes pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Inicialización de número de control**.
2. Escriba un nombre de socio y pulse **Buscar** o pulse **Buscar** sin especificar un nombre para mostrar todos los socios. Si deja seleccionado **Con posibilidad EDI**, limitará la búsqueda a aquellos socios que tengan funciones B2B de documentos EDI. Si elimina la comprobación, buscará todos los socios.
3. Pulse el icono **Ver detalles** junto al socio.
4. Las asignaciones de número de control actual del socio (si las hay) se listan en la página Detalles de configuración de número de control. Pulse el icono **Editar** para añadir o cambiar los valores.

5. Escriba (o cambie) el valor situado junto a **Intercambio** para indicar el número que desea utilizar para inicializar la generación de números de control para los intercambios.
6. Escriba (o cambie) el valor situado junto a **Grupo** para indicar el número que desea utilizar para inicializar la generación de números de control para los grupos. También puede pulsar **Máscara** y escribir una máscara que se utilizará en lugar de un valor fijo.
7. Escriba (o cambie) el valor situado junto a **Transacción** para indicar el número que desea utilizar para inicializar la generación de números de control para las transacciones. También puede pulsar **Máscara** y escribir una máscara que se utilizará en lugar de un valor fijo.
8. Pulse **Guardar**.

Números de control actuales

Para un par de socios determinado que ya tenga datos en la tabla de control, puede cambiar la generación de números de control. Puede:

- Restablecer la generación de números de control para el par en un estado inicial.
- Editar el intercambio, el grupo o el número de transacción (o cualquier combinación de estos números) y guardarlo con un nuevo valor.

Nota: el restablecimiento de la generación de números de control o edición de un grupo o máscara debe realizarse con precaución para que no se produzcan problemas de números fuera de secuencia o de números de control duplicados. Puede que desee realizar cualquiera de estas acciones durante la fase de prueba o si un socio solicita de manera específica distintos números de control.

Para determinar qué socios tienen números de control asignados (y para determinar cuáles son esos números), utilice la característica Números de control actuales.

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Números de control actuales**.
2. Lleve a cabo uno de los conjuntos de pasos siguientes:
   - Si desea ver el estado actual de todos los socios, deje **Cualquier socio** seleccionado en las listas de socios y pulse **Ver estado actual**.
   - Si desea ver el estado de los socios actuales, lleve a cabo los siguientes pasos:
     a. Especifique el nombre de los socios de origen y destino y pulse **Buscar**. Si desea limitar los resultados de búsqueda a sólo aquellos socios que estén intercambiando documentos EDI, deje **Buscar con posibilidad de EDI** seleccionado.
     b. En las listas de resultados, seleccione uno o más socios en cada lista y pulse **Ver estado actual**.

Definición de intercambios de documentos

Puede definir intercambios de documentos manualmente o utilizando asistentes. Si desea definir las conexiones utilizando los asistentes consulte el apartado "Definición de intercambios de documentos utilizando asistentes" en la página 205. Si desea hacerlo manualmente o modificar manualmente las conexiones, consulte el apartado "Definición manual de intercambios de documentos" en la página 207.

Definición de intercambios de documentos utilizando asistentes

WebSphere Partner Gateway incluye dos asistentes para ayudar en la definición de intercambios de documentos. Estos son el Asistente de importación EIF y Asistente de conexión EDI.

El Asistente de importación EIF guía al usuario a través de los pasos necesarios para importar correlaciones contenidas dentro de archivos EIF, muestra los detalles de las correlaciones subidas, asocia dichas correlaciones con los objetos de direccionamiento correctos y crea interacciones lógicas. Al completar el asistente, las nuevas correlaciones se suben y cualquier interacción necesaria se creará en el sistema. Debe utilizar el Asistente de conexión EDI para crear conexiones utilizando sus correlaciones que acaba de subir.

Nota: para evitar confusiones, sólo un usuario puede utilizar el Asistente de importación EIF al mismo tiempo.

El Asistente de conexión EDI puede ser utilizado después del asistente EIF y guía al usuario a través de los pasos necesarios para configurar una interacción EDI (enviando o recibiendo un documento EDI). Al terminar el asistente, los socios seleccionados estarán completamente configurados para la interacción EDI. Esto incluye la habilitación de funciones B2B, creación de interacciones válidas, creación de conexiones de socio y asignación de los atributos EDI necesarios. El Asistente de conexión genera las conexiones de socio basándose en la entrada del usuario. A continuación puede encontrar una lista de las posibles conexiones generadas:

- Desensobrador para mensaje base
- Transformación
- Ensobrador para mensaje base
- Generación de TA1
- Generación de FA
- Ensobrador para TA1 y/o FA
- Desensobrador para TA1 y/o FA

Ambos asistentes se encuentran en la pestaña Asistentes en la consola.

Importación de correlaciones utilizando el Asistente de importación EIF

Acerca de esta tarea

Para importar correlaciones utilizando el Asistente de importación EIF, complete los siguientes pasos:

1. Inicie la consola de WebSphere Partner Gateway.
2. Pulse **Asistentes**.
3. Pulse **Asistente de importación EIF**.
4. Especifique el nombre del archivo que desea importar o pulse **Examinar** para encontrarlo.

   Nota: cuando importe un archivo EIF que contenga varias correlaciones, asegúrese de que los nombres de correlaciones incluidos en el archivo sean exclusivos. Si se suban varias correlaciones del mismo archivo EIF con el mismo nombre de correlación, la última correlación coincidente sobrescribirá las correlaciones coincidentes anteriores en la base de datos.

5. Pulse **Importar**.
6. Aparecerá una lista de las correlaciones que han sido importadas satisfactoriamente. Pulse **Finalizar** para aceptar los valores predeterminados o pulse **Siguiente** para verlos o modificarlos.
7. Si ha pulsado **Siguiente**, se le solicitará que revise las correlaciones de transformación y que modifique cualquier interacción. Seleccione una correlación de transformación. Si existe una interacción, aparecerá como de sólo lectura. Para añadir una interacción, pulse **Añadir una interacción**.
8. En la ventana Añadir una interacción, seleccione una interacción y pulse **Añadir esta interacción** para añadir una interacción a lista.
9. Cuando termine de revisar las correlaciones de transformación, pulse **Siguiente** para revisar las correlaciones de validación.
10. Revise las correlaciones de validación importadas. Si son correctas, pulse **Finalizar**. Si desea ver las correlaciones de FA, pulse **Siguiente**.
11. Revise las correlaciones FA importadas y pulse **Finalizar** y aparecerá una ventana final mostrando las correlaciones que han sido importadas de manera satisfactoria así como las interacciones que han sido creadas. .

Configuración de conexiones utilizando el Asistente de conexión EDI

Acerca de esta tarea

Antes de configurar las conexiones utilizando el Asistente de conexión EDI, es necesario haber creado lo siguiente:

- El socio interno
- Al menos un socio externo
- Un ID de empresa EDI para cada socio. En este asistente un ID de empresa EDI se define como un Freeform Business Identifier con el formato *qq-xxxxxxxxx*, donde *qq* es el calificador de intercambio EDI de dos dígitos y *xxxxxxxxx* es el identificador de intercambio EDI de 9 dígitos.
- Destinos y destinos predeterminados
- Perfiles de sobre

Es posible que necesite realizar varios pasos de configuración adicionales antes de que los flujos EDI puedan ejecutarse de forma satisfactoria. Los siguientes son ejemplos:

- Configurar formatos XML (si está enviando o recibiendo XML)
- Configurar receptores con divisores ROD (si está recibiendo ROD)
- Configurar atributos de conexión adicionales para AS o AS2 (si está utilizando paquetes AS)

Para crear conexiones utilizando el Asistente de importación EDI, lleve a cabo los siguientes pasos:

1. Inicie la consola de WebSphere Partner Gateway.
2. Pulse **Asistentes**.
3. Pulse **Asistente de importación EDI**.
4. Pulse el tipo de tarea que desea configurar (**Enviar un documento EDI a un socio EDI** o **Enviar un documento EDI a un socio EDI**) y, a continuación, pulse **Siguiente**.

5. Dependiendo de si ha seleccionado **Recibir un documento EDI de un socio EDI** o **Enviar un documento EDI a un socio EDI**, especifique el socio de origen o de destino y pulse **Buscar**.
6. Seleccione el socio de origen o de destino en la lista desplegable y pulse **Siguiente**.
7. Seleccione las propiedades generales del socio de origen o de destino. Si la sintaxis es EDI, deberá también especificar las propiedades EDI. Cuando haya seleccionado todas las propiedades que desee, pulse **Siguiente**.

   Nota:

   a. Las propiedades TA1 y FA sólo son visibles si el origen es un socio externo. El tiempo necesario de FA sólo es visible si el destino es un socio externo.
   b. El Asistente de conexión EDI contiene una lista de los valores comunes que deben utilizarse como valores de delimitador EDI. Si desea utilizar un valor que no esté en la lista proporcionada, deberá editar el atributo de conexión a mano después de completar el asistente. Puede editar los atributos de conexión pulsando **Administración de cuentas > Conexiones**.
   c. Está obligado a especificar un destino para cada modalidad de funcionamiento. Esto quiere decir que no es posible seleccionar la opción en blanco ("No hay ningún destino seleccionado"). Forzar esta configuración adicional no afecta negativamente a la mayoría de situaciones de envío y recepción de documentos. Si necesita eliminar la especificación de Destino de la conexión, puede hacerlo después de completar el asistente pulsando **Administración de cuentas > Conexiones**.
8. Seleccione la **Correlación de validación**, **Acción** y **Correlación de transformación** para el socio de origen o de destino. Las descripciones de correlación aparecen después de seleccionar una correlación. El paquete está en blanco para impedir una confusión en casos como cuando EDI utilice el paquete AS. Cuando haya seleccionado estos, pulse **Siguiente**.
9. Revise las conexiones sugeridas, pulse **Atributos**, **Acciones** o **Destinos** para revisar los valores.

   Nota: las conexiones que ya existen y no están siendo creadas aparecerán en gris. Estas conexiones también tienen un icono Existe junto a ellas y no tienen un recuadro de selección Crear. Si las conexiones ya existen, no serán sobrescritas por este asistente. En este caso, un aviso aparecerá explicando esta situación.
   Si las conexiones necesitan ser modificadas, pulse **Atrás**. Cuando esté satisfecho con las conexiones listadas, pulse **Finalizar**. Si necesitan ser modificadas, pulse **Atrás**. y aparecerá una ventana final mostrando las conexiones que se han creado satisfactoriamente.

Definición manual de intercambios de documentos

El Asistente de importación EIF y el Asistente de conexión EDI pueden ayudar a definir intercambios de documentos (para obtener más información acerca de estos asistentes consulte el apartado "Definición de intercambios de documentos utilizando asistentes" en la página 205). Sin embargo, también puede definir los documentos manualmente. Este apartado proporciona una visión general de alto nivel de las tareas que es necesario realizar para establecer el intercambio de documentos para intercambios EDI entrando el concentrador, documentos o transacciones transformadas en el concentrador y para los intercambios EDI enviados desde el concentrador. Los pasos que se muestran en los siguientes apartados son generales y sólo se aplican a la importación de correlaciones y a la configuración de interacciones. Los pasos generales para habilitar las funciones B2B

para socios (para todos los tipos de intercambios de documentos) se describen en el apartado "Establecimiento de posibilidades B2B" en la página 28. Los pasos generales para gestionar conexiones (para todos los tipos de intercambios de documentos) se describen en el apartado Capítulo 12, "Gestión de conexiones", en la página 247. Si desea ver un ejemplo completo de un intercambio de documentos EDI, desde la importación de correlaciones hasta la gestión de conexiones, consulte el Capítulo 20, "Ejemplos EDI", en la página 341. El apéndice incluye los siguientes ejemplos específicos:

- " Ejemplo de EDI a ROD" en la página 341
- " Ejemplo de EDI a XML" en la página 355
- " Ejemplo de ROD a EDI" en la página 368
- " Ejemplo de XML a EDI" en la página 360

Importación manual de correlaciones

Acerca de esta tarea

Las correlaciones de transformación para documentos EDI, XML o de datos orientados a registros (ROD) pueden crearse con el programa Data Interchange Services Client. Data Interchange Services Client es un programa utilizado para crear y mantener definiciones de documento de esquema XML, definiciones de documento DTD XML, estándares EDI, definiciones de documento ROD y correlaciones.

Las correlaciones WTX se crean mediante el estudio de diseño WTX y se importan a WebSphere Partner Gateway.

Data Interchange Services Client es un programa que se instala por separado y que se incluye en el soporte de WebSphere Partner Gateway pero que normalmente reside en otro sistema. El especialista de correlaciones de Data Interchange Services crea una correlación que especifica cómo se mueven los elementos de un documento a los elementos de un documento distinto. Además de disponer de instrucciones que explican cómo convertir un documento de un formato en otro, Data Interchange Services también debe conocer el diseño, o el formato, del destino de origen y del destino. En Data Interchange Services el diseño de un documento es una *definición de documento*.

Cuando la correlación de transformación se importa en WebSphere Partner Gateway, las definiciones de documento creadas en Data Interchange Services aparecen como definiciones de documento (paquete, protocolo y tipo de documento) en la página Correlación de transformación y Gestionar definiciones de documento.

Por ejemplo, si se convierte un documento XML en una transacción X12, se importa la correlación que define las definiciones de documento de transacción XML y X12 y la transformación que debe tener lugar.

Existen dos métodos para recibir los archivos de correlaciones de Data Interchange Services. Si Data Interchange Services Client tiene una conexión directa con la base de datos de WebSphere Partner Gateway, el especialista de correlaciones de Data Interchange Services puede exportar el archivo directamente a la base de datos. Un caso de ejemplo más probable es que se reciban los archivos mediante el correo electrónico o una transferencia FTP. Si los archivos se transfieren al usuario a través de FTP, tenga en cuenta que debe hacerse en formato binario.

Si se produce un error durante la exportación de una correlación desde Data Interchange Services Client, es posible que siga viendo el nombre de correlación en la Consola de comunidad. La correlación no puede utilizarse para convertir documentos. Es necesario notificar al especialista de correlaciones de Data Interchange Services Client que ha habido un problema en la exportación y solicitarle que vuelva a exportar la correlación para poder utilizarla para convertir documentos.

Para importar una correlación, lleve a cabo los siguientes pasos:

1. Abra una ventana de mandatos.
2. Escriba el siguiente mandato o script:
   - En un sistema UNIX:

     `<ProductDir>/bin/bcgDISImport.sh <control_string_map>`
   - En un sistema Windows:

     `<ProductDir>\bin\bcgDISImport.bat <control_string_map>`

     donde *<ID_usuario_base_datos>* y *<contraseña>* son los valores utilizados al instalar la base de datos como parte de la instalación de WebSphere Partner Gateway. La *<correlación_serie_control>* es la vía de acceso completa del archivo de serie de control de correlación exportado desde Data Interchange Services Client.
3. Para las correlaciones de transformación, verifique que se ha importado la definición de documento.
   a. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de transformación**.
   b. En la página Correlaciones de transformación, pulse el icono **Ver detalles** situado junto a la correlación de Data Interchange Services. Podrá observar que aparecen las definiciones de documento del origen y del destino, indicando el formato en que se recibirá el documento en el concentrador y el formato en el que será entregado desde el concentrador.
   c. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   d. Expanda los paquetes y protocolos asociados con las definiciones de documento que puede observar en la página Correlaciones de transformación para verificar que los tipos de documentos aparecen en la página Gestionar definiciones de documento.

Para añadir la validación de estándares EDI adicionales a cualquier proceso de conversión que incluya estándares EDI, puede utilizar correlaciones de validación junto con correlaciones de transformación. Las correlaciones de validación proporcionan un control completo sobre la validación de un documento EDI.

Tenga en cuenta que las correlaciones de transformación y validación exportadas de Data Interchange Services Client o importadas con el programa de utilidad bcgDISImport no pueden descargarse de la Consola de comunidad de WebSphere Partner Gateway. El especialista de correlaciones de Data Interchange Services Client administra estas correlaciones conectándose a la base de datos de WebSphere Partner Gateway a través de Data Interchange Services Client.

Importación de correlaciones WTX

Acerca de esta tarea

Las correlaciones WTX que se creen mediante el estudio de diseño WTX deben importarse a WebSphere Partner Gateway, de manera que se pueda asociar a una

conexión de participante específica. Debe crear un DFD manualmente. Los DFD que se crean se exportan desde el estudio de diseño WTX en forma de correlación para el sistema operativo nativo. Para importar esto en WebSphere Partner gateway, vaya a **Administración del concentrador > Correlaciones > Correlaciones de transformación** y pulse **Crear**. La correlación importada se almacenará en el sistema de archivos común bajo una carpeta específica dedicada a las correlaciones WTX (comunes/correlaciones).

Importación de EIF estándar de WDI

Acerca de esta tarea

Para poder realizar la validación de las transacciones en WebSphere Partner Gateway, el formulario compilado del estándar EDI debe estar disponible en WebSphere Partner Gateway. Para crear esta serie de control del estándar compilado, realice lo siguiente:

1. Descargue el estándar EDI desde el sitio web de soporte WDI.
2. Cree una correlación de transformación de datos para la transformación y seleccione la transacción EDI que desee validar en WebSphere Partner Gateway. Por ejemplo, si desea validar la transacción 810 de X12V4R1, cree una correlación de transformación de datos de X12V4R1-810 a X12V4R1-810.
3. Correlacione únicamente un segmento obligatorio y compile la correlación de transformación.
4. Exporte la serie de control de la correlación de transformación de datos en la base de datos del gestor de documentos. Esto también exportará el estándar compilador en la base de datos del gestor de documentos, que se puede usar para la validación.

Nota: De manera alternativa, se proporcionan algunos EIF de muestra que incluyen únicamente la serie de control estándar compilada.

Configuración de un flujo de EDI a EDI

Acerca de esta tarea

En este apartado se describen las interacciones necesarias para recibir un intercambio EDI, desensobrar el intercambio, transformar una transacción con un formato EDI en otro formato, ensobrar la transacción y entregarla.

1. Verifique que exista una definición de documento para el intercambio EDI que se reciba en el concentrador. Recuerde que después de desensobrar el intercambio, el sobre original dejará de procesarse. Es decir, no tiene punto de entrega. Por ello, utilizará **N/D** para Paquete en la interacción de destino.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   b. Compruebe si ya existe una definición de documento. Por ejemplo, si un socio envía un intercambio EDI en un paquete AS, el protocolo EDI-X12 y tipo de documento ISA, la definición ya estará disponible. De forma similar, una definición de documento N/D/EDI-X12/ISA ya existe.
   c. Escriba un valor (o seleccione el valor en la lista) para cualquier atributo que desea asociar al perfil. Por ejemplo, si desea especificar que el sobre debe descartarse si se encuentran errores con cualquiera de las transacciones, pulse el icono **Editar valores de atributo** junto a **Definiciones de documento**. En la fila **Descartar sobre si hay errores**, seleccione **Sí** en la lista.
   d. Si no existe una definición de documento, cree una seleccionado el Protocolo de paquete y Tipo de documento.

Nota: No se puede utilizar el atributo Descartar sobre si hay errores cuando la acción en la conexión es Validación de intercambio EDI.

2. Cree una interacción para el intercambio.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Seleccione las definiciones de origen y destino. Excepto por el empaquetado (que será **N/D** para el destino), las definiciones de documento serán las mismas.
   d. Seleccione **Desensobrar EDI** en la lista Acción.
3. Importe la correlación de transformación que proporciona definiciones de documento de las transacciones EDI y que describe cómo se transforma la transacción de un formato EDI a otro. Consulte el apartado " Importación manual de correlaciones" en la página 208.

   Si el intercambio contiene más de una transacción, repita este paso para cada transacción.
4. Si desea editar atributos de las definiciones de documento asociadas a la correlación, efectúe los pasos siguientes:
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   b. Pulse el icono **Editar valores de atributo** situado junto al protocolo. Para protocolos EDI, verá una larga lista de atributos que puede establecer.
   c. Escriba un valor (o seleccione el valor en la lista) para cualquier atributo que desea asociar al protocolo.
   d. Pulse el icono **Editar valores de atributo** junto a la definición de documento. Generalmente verá una lista de atributos más pequeña que la lista de atributos asociados al protocolo.
   e. Especifique un valor (o seleccione el valor de la lista) para cualquier atributo que desee asociar con el tipo de documento. Por ejemplo, puede cambiar la **Correlación de validación** asociada con el tipo de documento.

      Asegúrese de seleccionar un perfil de sobre para la transacción.
5. Cree una interacción para la correlación que acaba de importar.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Bajo **Origen**, seleccione el tipo de documento asociado con la transacción. Expanda el paquete y protocolo y seleccione el tipo de documento. Este será generalmente **N/D** (ya que la transacción no se ha originado en un socio), el protocolo definido en la correlación (por ejemplo, **X12V4R1**) y el documento EDI real definido en la correlación (por ejemplo, **850**).
   d. Bajo **Destino**, seleccione la definición de documento para el documento transformado. Expanda el paquete y protocolo y seleccione el tipo de documento. Debido a que la transacción será ensobrada (y no será, por tanto, entregada directamente a un socio), el paquete será de nuevo **N/D**.
   e. En la lista de correlaciones de transformación, seleccione la correlación que define cómo transformar este documento.
   f. En la lista Acción, seleccione **Validación de EDI y conversión de EDI** para WDI nativos. En el caso de WTX, seleccione **Validación EDI y transformación WTX**.

6. Verifique que existe una definición de documento para el intercambio EDI que se envía desde el concentrador y establezca cualquier atributo que desee asociar con el intercambio.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   b. Compruebe si ya existe una definición de documento. El paquete de origen será N/D y el protocolo y tipo de documento coincidirán con el protocolo y tipo de documento utilizado para entregar el intercambio. Por ejemplo, si el intercambio se entregará como AS/EDI-X12/ISA, el origen será N/D/EDI-X12/ISA.
   c. Edite todos los atributos relacionados con el intercambio que se está entregando.
   d. Si no existe una definición de documento, cree una seleccionado el Protocolo de paquete y Tipo de documento.
7. Cree una interacción para el intercambio EDI que se envía desde el concentrador después de transformar la transacción.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Seleccione los documentos de origen y destino. Excepto por el paquete (que será **N/D** para el documento de origen), las definiciones de documento serán las mismas.
   d. Seleccione **Paso a través** en la lista **Acción**.

Para añadir un acuse de recibo al flujo, consulte el apartado "Configuración de reconocimientos" en la página 218.

Después de configurar las interacciones, cree funciones B2B para los socios.

- Para el socio de origen, habilite tres definiciones de documento (bajo **Establecer origen**), una para el tipo de documento de origen, una para la transacción EDI y una para el sobre.
- Para el socio de destino, habilite tres definiciones de documento (bajo **Establecer destino**), una para el tipo de documento desensobrado, una para la transacción EDI transformada y una para el sobre EDI.

Los pasos detallados para crear funciones B2B se describen en el "Establecimiento de posibilidades B2B" en la página 28.

Después de configurar las funciones B2B de los socios, cree las conexiones. Son necesarias tres conexiones:

- Una para el sobre del socio de origen al concentrador.
- Una para la transacción EDI de origen a la transacción EDI de destino.
- Una para el sobre del concentrador al socio de destino.

Los pasos detallados para crear conexiones se describen en el Capítulo 12, "Gestión de conexiones", en la página 247.

Configuración de un flujo de EDI a XML o ROD

Acerca de esta tarea

En este apartado se describen las interacciones necesarias para recibir un intercambio EDI, desensobrar el intercambio, transformar una transacción con un formato EDI en un documento XML o ROD y entregarlo.

Nota: si desea ver un ejemplo completo del flujo de EDI a XML, consulte el apartado " Ejemplo de EDI a XML" en la página 355. Si desea ver un ejemplo completo del flujo de EDI a ROD, consulte el apartado " Ejemplo de EDI a ROD" en la página 341.

1. Verifique que exista una definición de documento para el intercambio EDI que se reciba en el concentrador. Recuerde que después de desensobrar el intercambio, el sobre dejará de procesarse. Es decir, no tiene punto de entrega. Por ello, utilizará **N/D** para Paquete en la interacción de destino.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   b. Compruebe si ya existe una definición de documento. Por ejemplo, si un socio envía un intercambio EDI en un paquete AS, el protocolo EDI-X12 y tipo de documento ISA, la definición ya estará disponible. De forma similar, una definición de documento N/D/EDI-X12/ISA ya existe.
   c. Si no existe una definición de documento, cree una.
2. Cree una interacción para el intercambio EDI que se recibe en el concentrador.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Seleccione los documentos de origen y destino. Excepto por el empaquetado (que será **N/D** para el destino), las definiciones de documento serán las mismas.
   d. Seleccione **Desensobrar EDI** en la lista Acción.
3. Importe la correlación de transformación que proporciona definiciones de documento de la transacción EDI y el documento XML o ROD que describe cómo se transforma la transacción en el documento XML o ROD. Consulte el apartado " Importación manual de correlaciones" en la página 208.

   Si el intercambio contiene más de una transacción, repita este paso para cada transacción.
4. Cree una interacción para la correlación que acaba de importar.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Bajo **Origen**, seleccione el tipo de documento asociado con la transacción. Expanda el paquete y protocolo y seleccione el tipo de documento. Este será generalmente **N/D** (ya que la transacción no se ha originado en un socio), el protocolo definido en la correlación (por ejemplo, **X12V4R1**) y el documento EDI real definido en la correlación (por ejemplo, **850**).
   d. Bajo **Destino**, seleccione la definición de documento para el documento (XML o ROD) transformado. Expanda el paquete y protocolo y seleccione el tipo de documento.
   e. En la lista de correlaciones de transformación, seleccione la correlación que define cómo transformar este documento.
   f. En la lista Acción, seleccione **Validación de EDI y conversión de EDI** si es WDI nativo. En el caso de WTX, seleccione **Validación EDI y transformación WTX**.

Para añadir un acuse de recibo al flujo, consulte el apartado "Configuración de reconocimientos" en la página 218.

Después de configurar las interacciones, cree funciones B2B para los socios.

- Para el socio de origen, habilite las definiciones de documento (bajo **Establecer origen**), una para el sobre y otra para la transición EDI.
- Para el socio de destino, habilite dos definiciones de documento (bajo **Establecer destino**), una para el sobre EDI y otra para el documento XML o ROD.

Los pasos detallados para crear funciones B2B se describen en el "Establecimiento de posibilidades B2B" en la página 28.

Después de configurar las funciones B2B de los socios, cree las conexiones. Son necesarias dos conexiones:

- Una para el sobre del socio de origen al concentrador.
- Una para la transacción EDI de origen al documento XML o ROD.

Los pasos detallados para crear conexiones se describen en el Capítulo 12, "Gestión de conexiones", en la página 247.

Configuración de un flujo de XML o ROD a EDI

Acerca de esta tarea

En este apartado se describen las interacciones necesarias para recibir un documento XML o ROD, transformarlo en una transacción EDI, ensobrar la transacción y entregarla.

Nota: si desea ver un ejemplo completo del flujo de XML a EDI, consulte el apartado " Ejemplo de XML a EDI" en la página 360. Si desea ver un ejemplo completo del flujo de ROD a EDI, consulte el apartado " Ejemplo de ROD a EDI" en la página 368.

1. Importe la correlación de transformación que proporciona definiciones de documento del documento XML o ROD y la transacción EDI y que describe cómo se transforma el documento en la transacción EDI. Consulte el apartado " Importación manual de correlaciones" en la página 208.
2. Cree una interacción para la correlación que acaba de importar.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Bajo **Origen**, seleccione la definición de documento asociada con el documento XML o ROD. Expanda el paquete y protocolo y seleccione el tipo de documento.
   d. Bajo **Destino**, seleccione el tipo de documento asociado con la transacción EDI. Expanda el paquete y protocolo y seleccione el tipo de documento. Puesto que la transacción no se entregará directamente (se pondrá en un sobre antes de entregarse), **N/D** se listará para Paquete.
   e. En la lista de correlaciones de transformación, seleccione la correlación que define cómo transformar este documento.
   f. En la lista Acción, seleccione **Conversión de XML y Validación de EDI** o **Conversión de ROD y Validación de EDI** para WDI nativos. En el caso de WTX, seleccione **Transformación WTX**.
3. Verifique que existe una definición de documento para el intercambio EDI que se envía desde el concentrador y establezca cualquier atributo que desee asociar con el intercambio.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.

b. Compruebe si ya existe una definición de documento. **N/D** debe utilizarse para Paquete para el documento de origen (el intercambio que se envía desde el concentrador).
c. Edite todos los atributos relacionados con el intercambio que se está entregando.
d. Si no existe una definición de documento, cree una seleccionado el Protocolo de paquete y Tipo de documento.

4. Cree una interacción para el intercambio EDI que se envía desde el concentrador después de transformar el documento.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Seleccione los documentos de origen y destino. Los documentos de origen y de destino tienen paquetes distintos (el documento de origen tiene un paquete de N/D), pero el protocolo (por ejemplo, EDI-X12) y el tipo de documento (por ejemplo, ISA) deben ser el mismo.
   d. Seleccione **Paso a través** en la lista Acción.

Después de configurar las interacciones, cree funciones B2B para los socios.

- Para el socio de origen, el número de definiciones de documento necesarias (bajo **Establecer origen**) varía, dependiendo del tipo de documento.
  - Por ejemplo, para un documento XML en el que el tipo de documento sea ICGPO y la transacción EDI convertida sea MX12V3R1, habilite tres definiciones de documento (bajo **Establecer origen**), una para el documento XML (ICGPO), una para la transacción EDI (MX12V3R1) y una para el sobre que se está enviando al concentrador.
  - Para otros documentos XML y documentos ROD, habilite dos definiciones de documento (bajo **Establecer origen**), una para el documento XML o ROD y otra para el sobre que se envía desde el concentrador.
- Para el socio de destino, habilite dos definiciones de documento (bajo **Establecer destino**), una para la transacción EDI y otra para el sobre EDI que se recibe. Para la transacción EDI, pulse el icono **Editar valores de atributo** situado junto al protocolo y especifique un perfil de sobre. También puede especificar otros atributos.

Los pasos detallados para crear funciones B2B se describen en el "Establecimiento de posibilidades B2B" en la página 28.

Después de configurar las funciones B2B de los socios, cree las conexiones. Son necesarias dos conexiones:

- Una para el documento XML o ROD de origen a la transacción EDI.
- Una para el sobre del concentrador al socio.

Los pasos detallados para crear conexiones se describen en el Capítulo 12, "Gestión de conexiones", en la página 247.

Configuración de varios documentos XML o ROD en un archivo para el flujo EDI

Acerca de esta tarea

En este apartado se describen las interacciones necesarias para recibir varios documentos XML o ROD en un archivo, transformar los documentos en transacciones EDI, ensobrar las transacciones y entregar el intercambio EDI.

1. Importe la correlación de transformación que proporciona definiciones de documento de los documentos XML o ROD y las transacciones EDI y que describe la transformación. Consulte el apartado " Importación manual de correlaciones" en la página 208.
2. Cree una interacción para los documentos de origen y destino.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Para WDI nativos, seleccione los documentos de origen y destino y seleccione **Conversión de XML y Validación de EDI** o **Conversión de ROD y Validación de EDI** en la lista Acción. Para WTX, seleccione **Transformación WTX** y **Validación de EDI**.
3. Repita el paso 2 para el documento de origen y cada documento de destino generado por la correlación de transformación.
4. Verifique que existe una definición de documento para el intercambio EDI que se envía desde el concentrador y establezca cualquier atributo que desee asociar con el intercambio.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   b. Compruebe si ya existe una definición de documento. El origen será N/D, con el protocolo y tipo de documento que coincidan con el protocolo y tipo de documento utilizado para entregar el intercambio. Por ejemplo, si el intercambio se entregará como AS/EDI-X12/ISA, el origen será N/D/EDI-X12/ISA.
   c. Edite todos los atributos relacionados con el intercambio que se está entregando.
   d. Si no existe una definición de documento, cree una seleccionado el Protocolo de paquete y Tipo de documento.
5. Cree una interacción para el intercambio EDI que se envía desde el concentrador después de transformar la transacción.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Seleccione los documentos de origen y destino. Los documentos de origen y de destino tienen paquetes distintos (el documento de origen tiene un paquete de N/D), pero el protocolo (por ejemplo, EDI-X12) y el tipo de documento (por ejemplo, ISA) deben ser el mismo.
   d. Seleccione **Paso a través** en la lista Acción.

Después de configurar las interacciones, cree funciones B2B para los socios.

- Para el socio de origen, el número de definiciones de documento necesarias (bajo **Establecer origen**) varía, dependiendo del tipo de documento.
  - Por ejemplo, para un documento XML en el que el tipo de documento sea ICGPO y la transacción EDI convertida sea MX12V3R1, habilite tres definiciones de documento (bajo **Establecer origen**), una para el documento XML (ICGPO), una para la transacción EDI (MX12V3R1) y una para el sobre que se está enviando al concentrador.
  - Para otros documentos XML y documentos ROD, habilite dos definiciones de documento (bajo **Establecer origen**), una para el documento XML o ROD y otra para el sobre que se envía desde el concentrador.

Los pasos detallados para crear funciones B2B se describen en el "Establecimiento de posibilidades B2B" en la página 28.

Después de configurar las funciones B2B de los socios, cree las conexiones. Son necesarias varias conexiones:

- Una para cada documento XML o ROD que se transforma en una transacción EDI.
- Una para el sobre del concentrador al socio.

Los pasos detallados para crear conexiones se describen en el Capítulo 12, "Gestión de conexiones", en la página 247.

Configuración de un flujo de documentos de XML a ROD o ROD a XML

Acerca de esta tarea

En este apartado se describen las interacciones necesarias para recibir un documento XML o ROD, transformarlo en otro tipo de documento (de XML a ROD o de ROD a XML) y entregarlo.

1. Importe la correlación de transformación que proporciona definiciones de documento de los documentos XML y ROD y que describe cómo se transforman los documentos. Consulte el apartado " Importación manual de correlaciones" en la página 208.
2. Pulse **Administración del concentrador > Configuración del concentrador > Correlaciones> Correlaciones de transformación** y pulse el icono **Ver detalles** situado junto a la correlación que acaba de importar.
3. Cree una interacción para la correlación que acaba de importar.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
4. Seleccione los documentos de origen y destino, y seleccione **Transformación WTX** para WTX o **Conversión ROD y validación EDI** de la lista de acciones.

Después de configurar las interacciones, cree funciones B2B para los socios.

- Para el socio de origen, habilite las definiciones de documento (bajo **Establecer origen**) para el documento XML o ROD.
- Para el socio de destino, habilite definiciones de documento (bajo **Establecer destino**) para el documento XML o ROD.

Los pasos detallados para crear funciones B2B se describen en el "Establecimiento de posibilidades B2B" en la página 28.

Después de configurar las funciones B2B de los socios, cree las conexiones. Es necesaria una conexión para el flujo de XML a ROD o para el flujo de ROD a XML. Los pasos detallados para crear conexiones se describen en el Capítulo 12, "Gestión de conexiones", en la página 247.

Configuración de un flujo de XML a XML o ROD a ROD

Acerca de esta tarea

En este apartado se describen las interacciones necesarias para recibir un documento XML o ROD, transformarlo en un documento del mismo tipo (de XML a XML o de ROD a ROD) y entregarlo.

1. Importe la correlación de transformación que proporciona definiciones de documento de los documentos XML o ROD y que describe cómo se transforman los documentos. Consulte el apartado " Importación manual de correlaciones" en la página 208.
2. Pulse **Administración del concentrador > Configuración del concentrador > Correlaciones> Correlaciones de transformación** y pulse el icono **Ver detalles** situado junto a la correlación que acaba de importar.
3. Cree una interacción para la correlación que acaba de importar.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Seleccione los documentos de origen y destino.
   d. Para WDI nativos, seleccione **Conversión de XML y Validación de EDI** o **Conversión de ROD y Validación de EDI** en la lista Acción. Para WTX, seleccione **Transformación WTX** y **Validación de intercambio EDI**.

Después de configurar las interacciones, cree funciones B2B para los socios.

- Para el socio de origen, habilite una definición de documento (bajo **Establecer origen**) para el documento XML o ROD.
- Para el socio de destino, habilite una definición de documento (bajo **Establecer destino**) para el documento XML o ROD.

Los pasos detallados para crear funciones B2B se describen en el "Establecimiento de posibilidades B2B" en la página 28.

Después de configurar las funciones B2B de los socios, cree las conexiones. Es necesaria una conexión para el flujo de XML a XML o para el flujo de ROD a ROD. Los pasos detallados para crear conexiones se describen en el Capítulo 12, "Gestión de conexiones", en la página 247.

Configuración de reconocimientos

En este apartado se describe cómo configurar interacciones para enviar acuses de recibo de la recepción de intercambios o transacciones al originador del documento.

Acuses de recibo funcionales

Las correlaciones de acuses de recibo funcionales se utilizan para proporcionar la generación de acuses de recibo funcionales cuando se responde a documentos EDI recibidos desde un socio. WebSphere Partner Gateway proporciona un conjunto de correlaciones de acuse de recibo funcional que generan los acuses de recibo funcionales EDI que se utilizan más habitualmente. El especialista de correlaciones también puede crear correlaciones de FA y de validación, en cuyo caso estas correlaciones deberán subirse a WebSphere Partner Gateway.

Nota: sólo debe crearse una correlación de acuse de recibo funcional cuando se requiere un acuse de recibo funcional personalizado.

Además de las correlaciones de acuse de recibo funcional que se suministran con WebSphere Partner Gateway, también se proporciona el protocolo &FUNC_ACK_METADATA_DICTIONARY y la definición &FUNC_ACK_META asociada. Aparecen listados bajo **Paquete: Ninguno** en la página Definiciones de documento. &FUNC_ACK_META es la definición de documento de origen para todas las correlaciones de acuse de recibo funcional. Esta correlación proporciona la estructura del acuse de recibo funcional. Un acuse de recibo funcional fluye hasta

los socios y la correlación de acuses de recibo le dice al sistema cómo debe generarse el acuse de recibo. El nombre de la definición de origen no puede cambiarse. El especialista de correlaciones de Data Interchange Services Client no puede crear una correlación de acuse de recibo funcional sin esta definición de documento en la base de datos.

La definición de documento de destino en una correlación de acuse de recibo funcional describe el diseño del acuse de recibo funcional. Debe ser una definición de documento EDI con el nombre 997, 999 o CONTRL.

Las siguientes correlaciones de acuse de recibo funcionales se instalan con WebSphere Partner Gateway y aparecen en la página Gestionar definiciones de documento bajo **Paquete: N/D**:

Tabla 29. Correlaciones de acuse de recibo funcional proporcionadas por el producto

Protocolo	Tipo de documento	Descripción
&DTCTL21	CONTRL	Acuse de recibo funcional CONTRL – UN/EDIFACT versión 2 release 1 (D94B)
&DTCTL	CONTRL	Acuse de recibo funcional CONTRL – UN/EDIFACT antes de D94B
&DT99933	999	Acuse de recibo funcional 999 – UCS versión 3 release 3
&DT99737	997	Acuse de recibo funcional 997 – X12 versión 3 release 7
&DT99735	997	Acuse de recibo funcional 997 – X12 versión 3 release 5
&DT99724	997	Acuse de recibo funcional 997 – X12 versión 2 release 4

Además, el protocolo &X44TA1 (con un tipo de documento TA1 asociado) aparece listado bajo **Paquete: N/D**. Esta correlación se utiliza para generar un TA1. TA1 es un acuse de recibo funcional que se genera para intercambios X12 entrantes.

El protocolo &WDIEVAL (con una X12ENV asociada) también se proporciona bajo **Paquete: N/D**.

Al igual que las transacciones EDI, los acuses de recibo funcionales siempre se colocan en un intercambio EDI antes de entregarse.

Acuses de recibo TA1

TA1 es un segmento EDI que proporciona un acuse de recibo de intercambio X12. Reconoce la recepción y la corrección sintáctica de un par formado por la cabecera y la cola de intercambio X12 (ISA e IEA). El remitente puede solicitar un TA1 del receptor estableciendo el elemento 14 de la cabecera de control de intercambio ISA en **1**. El número de control de intercambio de un TA1 se asocia con un intercambio X12 transmitido anteriormente con el mismo número de control para completar el proceso de acuse de recibo.

Al igual que las transacciones EDI y los acuses de recibo funcionales, los TA1 siempre se colocan en un intercambio EDI antes de entregarse.

Adición de un acuse de recibo al tipo de documento

Acerca de esta tarea

Para añadir un acuse de recibo a un flujo, efectúe los siguientes pasos:

Procedimiento

1. Si WebSphere Partner Gateway no facilita la correlación de reconocimiento funcional, impórtela de Data Interchange Services Client. Consulte el apartado " Importación manual de correlaciones" en la página 208.
2. Asocie la correlación de FA con una definición de documento:
   a. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de acuse de recibo funcional de EDI**.
   b. Pulse el icono **Ver detalles** situado junto a la correlación.
   c. Pulse el icono **Expandir** situado junto a un paquete para expandir de forma individual hasta el nivel adecuado (por ejemplo, expanda las carpetas **Paquete** y **Protocolo** y seleccione la transacción).
   d. Pulse **Guardar**.
3. Cree una interacción para la correlación que acaba de importar.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Bajo **Origen**, seleccione el tipo de documento asociado con el acuse de recibo funcional. Expanda el paquete y protocolo y seleccione el tipo de documento.
   d. Bajo **Destino**, seleccione los mismos valores.
   e. En la lista Acción, seleccione **Paso a través**.
4. Verifique que existe una definición de documento para el intercambio EDI que se envía desde el concentrador y establezca cualquier atributo que desee asociar con el intercambio.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
   b. Compruebe si ya existe una definición de documento. El origen será N/D, con el protocolo y tipo de documento que coincidan con el protocolo y tipo de documento utilizado para entregar el intercambio. Por ejemplo, si el intercambio se entregará como AS/EDI-X12/ISA, el origen será N/D/EDI-X12/ISA.
   c. Edite todos los atributos relacionados con el intercambio que se está entregando.
   d. Si no existe una definición de documento, cree una seleccionado el Protocolo de paquete y Tipo de documento.
5. Cree una interacción para el intercambio EDI que se envía desde el concentrador después de transformar el documento.
   a. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
   b. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
   c. Seleccione los documentos de origen y destino.
   d. Seleccione **Paso a través** en la lista **Acción**.

Resultados

Después de configurar las interacciones, cree funciones B2B para los socios. Tenga en cuenta que el socio de destino en una transmisión de acuse de recibo funcional es el socio de origen del documento EDI original.

- Para el socio de origen, habilite las definiciones de documento (bajo **Establecer origen**) para el acuse de recibo funcional. Habilite también una definición de documento para el sobre que se está enviando al concentrador.
- Para el socio de destino, habilite una definición de documento (bajo **Establecer destino**) para el acuse de recibo funcional. Habilite también una definición de documento para el sobre EDI que se recibe.

  Para el acuse de recibo funcional, pulse el icono **Editar valores de atributo** situado junto al protocolo y especifique un perfil de sobre.

Los pasos detallados para crear funciones B2B se describen en el "Establecimiento de posibilidades B2B" en la página 28.

Después de configurar las funciones B2B de los socios, cree las conexiones. Son necesarias dos conexiones:

- Una para el acuse de recibo funcional.
- Una para el sobre del concentrador al socio.

Los pasos detallados para crear conexiones se describen en el Capítulo 12, "Gestión de conexiones", en la página 247.

Conceptos relacionados

Capítulo 12, "Gestión de conexiones", en la página 247

Tareas relacionadas

" Importación manual de correlaciones" en la página 208
"Establecimiento de posibilidades B2B" en la página 28

Visualización de transacciones e intercambios EDI

Acerca de esta tarea

Tal como se ha mencionado anteriormente en este capítulo, utilice el Visor de documentos para mostrar información sobre las transacciones y los intercambios EDI que constituyen un flujo de documentos. Puede mostrar documentos sin formato y los sucesos y detalles de proceso de documentos asociados mediante criterios de búsqueda específicos. Esta información es útil si está intentando determinar si un intercambio EDI se ha entregado satisfactoriamente o para determinar la causa de un problema.

Para mostrar el Visor de documentos, lleve a cabo los siguientes pasos:

1. Pulse **Visores > Visor de documentos**.
2. Seleccione los criterios de búsqueda adecuados.
3. Pulse **Buscar**.

Consulte la publicación *Guía del administrador de WebSphere Partner Gateway* para obtener más información sobre la utilización del Visor de documentos.

Limitaciones de OpenPGP al recibir y enviar documentos EDI a través de distintos protocolos de transporte

Al recibir documentos EDI, los ID de empresa se determinan a partir del contenido y tienen que coincidir con los ID de empresa como se determina en el empaquetado o la estructura de carpetas. Las siguientes son las limitaciones de la recepción de datos EDI a través de distintos protocolos de transporte:

1. Al recibir un documento a través de HTTP, la autenticación básica determina el socio remitente. Si se utiliza el parámetro 'A', determina el ID de empresa del socio receptor. La cabecera de transporte 'X-receiver' también puede utilizarse para identificar el socio destinatario. Tiene que contener el ID de empresa del socio destinatario. Si no se especifica el socio destinatario, el socio interno predeterminado se considera el destinatario. La autenticación básica contiene el ID de usuario y contraseña. Se recomienda utilizar HTTP(S) con autenticación de servidor y autenticación básica.
2. Al recibir un documento a través de FTP(S), el socio remitente se determina mediante la estructura de carpetas específica de WebSphere Partner Gateway, configurada para receptores FTP(S).
3. En el caso de documentos binarios, cuando el documento se recibe a través de SFTP, el socio remitente se determina según los valores de configuración proporcionados en el manejador de preproceso genérico adjunto del receptor SFTP.

Capítulo 11. Creación de destinos

Después de crear los socios, se definen los destinos de los socios. Los destinos definen puntos de entrada en el sistema del socio.

Este capítulo incluye los siguientes temas:

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado la sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Visión general de los destinos

WebSphere Partner Gateway utiliza destinos para direccionar los documentos a sus destinos. El destinatario puede ser un socio externo o interno.
El protocolo de transporte de salida determina la información que se utiliza

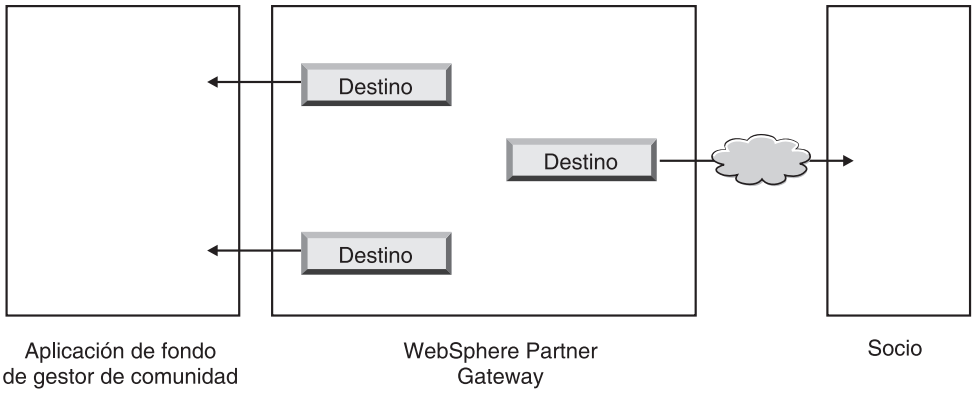


Figura 34. Destinos a socio interno y socios externos

durante la configuración del destino.

Los siguientes transportes están soportados (de manera predeterminada) para los destinos de socios:

- HTTP/1.1
- HTTPS/1.0
- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP

  Nota: Puede definir un destino SMTP para socios externos únicamente (no para el socio interno).
- SFTP
- Directorio de archivos
- FTP Scripting

También puede especificar un transporte definido por el usuario, que va a subir durante la creación del destino.

Como administrador del concentrador, puede configurar los destinos de los socios o los socios pueden realizar esta tarea por sí mismos. En este capítulo, se muestra cómo realizar la tarea para los socios. Para la gestión de destinos, consulte el *capítulo Tareas de administración del concentrador de la Guía del administrador de WebSphere Partner Gateway*.

Configuración de los valores de transporte global

Acerca de esta tarea

Establezca atributos de transporte global que se aplican a todos los destinos de FTP Scripting. Si no está definiendo ningún destino de FTP Scripting, este apartado no es pertinente.

El transporte FTP Scripting utiliza un mecanismo de bloqueo que impide que más de una instancia de FTP Scrtipting acceda al mismo destino al mismo tiempo. Se proporcionan valores predeterminados, como el intervalo de tiempo que una instancia de pasarela esperará para obtener el bloqueo y la cantidad de veces que intenta recuperarla si el bloqueo está en uso. Puede utilizar estos valores predeterminados o cambiarlos.

1. Pulse **Administración de cuentas > Perfiles**.
2. Pulse **Destinos**.
3. Seleccione **Atributos de transporte global** en Detalles del destino.

   Si ha actualizado **Tiempo máximo de bloqueo (segundos)** o **Tiempo máximo de bloqueo (segundos)** cuando ha especificado los valores de transporte global durante la creación de los destinos, estos valores actualizados se reflejan aquí.
4. Si los valores predeterminados son adecuados para la configuración, pulse **Cancelar**. En caso contrario, continúe con los restantes pasos en este apartado.
5. Pulse el icono **Editar** situado junto a **Transporte FTP Scripting**.
6. Para cambiar uno o varios de los valores, escriba el nuevo valor o los nuevos valores. Puede cambiar:

- **Recuento de reintentos de bloqueo**, que indica cuántas veces intentará el destino obtener un bloqueo si el bloqueo está actualmente en uso. El valor predeterminado es 3.
- **Intervalo de reintento de bloqueo (segundos)**, que indica el periodo de tiempo que transcurrirá entre intentos para obtener el bloqueo. El valor predeterminado es 260 segundos.
- **Tiempo máximo de bloqueo (segundos)**, que indica cuánto tiempo puede el destino mantener el bloqueo. El valor predeterminado es 240 segundos (a menos que se haya cambiado al crear destinos).
- **Cola máxima de bloqueo (segundos)**, que indica cuánto tiempo puede esperar el destino en una cola para obtener el bloqueo. El valor predeterminado es 740 segundos (a menos que se haya cambiado al crear destinos).

7. Pulse **Guardar**

Configuración de un proxy de avance

Acerca de esta tarea

En el transporte HTTP, puede configurar el soporte de proxy de avance de modo que los documentos se envíen a través de un servidor proxy configurado. Con WebSphere Partner Gateway, puede configurar los siguientes tipos de soporte:

- Soporte de proxy a través de HTTP
- Soporte de proxy a través de HTTP con autenticación
- Soporte de proxy a través de SOCKS

Nota: WebSphere Partner Gateway se conecta a un servidor proxy sólo en el puerto HTTP.

Después de configurar un proxy de avance, puede hacer que sea global para el transporte haciendo que sea el destino predeterminado (por ejemplo, que todos los destinos HTTP utilice el proxy de avance).

Para configurar un proxy de avance, siga estos pasos:

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Destinos**.
3. Pulse **Soporte de proxy de avance**.
4. En la página Lista de proxy de avance, pulse **Crear**.
5. Escriba un nombre para el proxy.
6. Si lo desea, escriba una descripción del proxy.
7. Seleccione el tipo de transporte en la lista.

   Nota: los transportes disponibles son HTTP y HTTPS.
8. Escriba la siguiente información. Especifique el host de proxy y el puerto de proxy *o* el host de proxy de socks y el puerto de proxy de socks.
   - En **Host de proxy**, escriba el servidor proxy que desea utilizar (por ejemplo: http://proxy.abc.com).
   - En **Puerto de proxy**, escriba el número de puerto.
   - Si el servidor proxy requiere un nombre de usuario y una contraseña, indíquelos en los campos **Nombre de usuario** y **Contraseña**.

- En **Host de proxy de socks**, escriba el servidor proxy SOCKS que va a utilizar.
- En **Puerto de proxy de socks**, escriba el número de puerto.

9. Seleccione este recuadro de selección si desea que este proxy sea el proxy predeterminado (que puede ser utilizado por cualquier otro socio que tenga especificado el soporte para proxy).
10. Pulse **Guardar**.

Nota: La técnica de transmisión a través de túnel HTTP se utiliza en el proxy de avance, pero no existe ningún soporte para Secure Forward Proxy. La transmisión a través de túnel HTTP se crea con el servidor proxy. Debe comprobar la conectividad antes de pasar cualquier tipo de datos (HTTP o HTTPS) al socio final. Los datos están cifrados en SSL. El puerto utilizado para Forward Proxy debe ser HTTP puerto 80. Básicamente es un paso a través de reconocimiento SSL entre WebSphere Partner Gateway y el socio.

Configuración de un destino HTTP

Acerca de esta tarea

Configure un destino HTTP para que se puedan enviar documentos del concentrador a la dirección IP del socio. Cuando configura un destino HTTP, también se especifica que los documentos se envíen a través de un servidor proxy configurado.

Para iniciar un proceso de creación de un destino HTTP, utilice el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Detalles del destino

Acerca de esta tarea

Desde la página **Lista de destino**, lleve a cabo los siguientes pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio. Es el nombre que aparecerá en la lista de destinos.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. Si lo desea, seleccione el servidor proxy que se debe utilizar. La **Lista de proxy de avance** incluye los servidores proxy que ha creado, incluido el servidor proxy predeterminado. El valor predeterminado de este campo es **Utilizar proxy de avance predeterminado**. Si desea que el socio seleccionado utilice un servidor proxy distinto, seleccione el servidor de dicha lista. Si no desea que el servidor utilice esta característica con el socio seleccionado, seleccione **Utilizar proxy no de avance**.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Se trata de un campo obligatorio.

   El formato es: http://*<nombre_servidor>*:*<puerto_opcional>*/*<vía_de_acceso>*

   Un ejemplo de este formato sería:

   ```
   http://anotherserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   Nota: Si está especificando una dirección IPv6, proporcione el formato numérico, no el nombre de máquina o el nombre de sistema principal.

   Ejemplos de direcciones IPv6 son:

   ```
   http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
   http://[1080:0:0:0:8:800:200C:417A]/index.html
   http://[3ffe:2a00:100:7031::1]
   http://[1080::8:800:200C:417A]/foo
   http://[::192.9.5.5]/ipng
   http://[::FFFF:129.144.52.38]:80/index.html
   http://[2010:836B:4179::836B:4179]
   ```

   Cuando está configurando un destino para que sea utilizado por un servicio web, especifique el URL privado proporcionado por el proveedor de servicios web. Ahí es donde WebSphere Partner Gateway invocará el servicio web cuando actúe como proxy para el proveedor de servicios web.
3. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor HTTP.
4. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
5. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.
6. En el campo **Número de hebras**, especifique el número de documentos que pueden procesarse simultáneamente. El valor predeterminado es 3.
7. En el campo **Validar IP de cliente**, seleccione **Sí**, si desea que la dirección IP del remitente se valide antes de procesar el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
8. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si está a punto de producirse una anomalía de entrega porque que haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

   Cuando se selecciona **Cola automática**, todos los documentos permanecerán en la cola hasta que el destino se ponga en línea manualmente.

9. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
10. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 243. De lo contrario, pulse **Guardar**.

Configuración de un destino HTTPS

Acerca de esta tarea

Configure un destino HTTPS para que se puedan enviar documentos del concentrador a la dirección IP del socio. Cuando configura un destino HTTPS, también se especifica que los documentos se envíen a través de un servidor proxy configurado.

Para crear destinos HTTPS, utilice el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Detalles del destino

Acerca de esta tarea

Desde la página Detalles del destino, lleve a cabo los siguientes pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.
5. Seleccione **HTTPS/1.0** o **HTTPS/1.1** de la lista **Transporte** .

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. Si lo desea, seleccione el servidor proxy que se debe utilizar. La **Lista de proxy de avance** incluye los servidores proxy que ha creado, incluido el servidor proxy predeterminado. El valor predeterminado de este campo es **Utilizar proxy de avance predeterminado**. Si desea que el socio seleccionado utilice un servidor proxy distinto, seleccione el servidor de dicha lista. Si no desea que el servidor utilice esta característica con el socio seleccionado, seleccione **Utilizar proxy no de avance**.
2. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Se trata de un campo obligatorio.

El formato es: https://<*nombre_servidor*>:<*puerto_opcional*>/<*vía_de_acceso*>

Por ejemplo:

```
https://anotherserver.ibm.com:57443/bcgreceiver/Receiver
```

Nota: Si está especificando una dirección IPv6, proporcione el formato numérico, no el nombre de máquina o el nombre de sistema principal.

Ejemplos de direcciones IPv6 son:

```
https://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
https://[1080:0:0:0:8:800:200C:417A]/index.html
https://[3ffe:2a00:100:7031::1]
https://[1080::8:800:200C:417A]/foo
https://[::192.9.5.5]/ipng
https://[::FFFF:129.144.52.38]:80/index.html
https://[2010:836B:4179::836B:4179]
```

3. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor HTTP seguro.
4. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
5. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.
6. En el campo **Número de hebras**, especifique el número de documentos que pueden procesarse simultáneamente. El valor predeterminado es 3.
7. En el campo **Validar IP de cliente**, seleccione **Sí**, si desea que la dirección IP del remitente se valide antes de procesar el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
8. En el campo **Validar certificado SSL de cliente**, seleccione **Sí** si desea que el certificado digital del socio remitente se valide contra el ID de empresa asociado con el documento. El valor predeterminado es **No**.
9. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si está a punto de producirse una anomalía de entrega porque que haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

   Cuando se selecciona **Cola automática**, todos los documentos permanecerán en la cola hasta que el destino se ponga en línea manualmente.
10. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
11. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 243. De lo contrario, pulse **Guardar**.

Configuración de un destino FTP

Acerca de esta tarea

Para crear un destino FTP, siga el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.

3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Nota: La modalidad de FTP pasiva no tiene soporte. Consulte el apartado "Configuración de un destino de FTP Scripting" en la página 239 para obtener información sobre soporte pasivo.

Detalles del destino

Acerca de esta tarea

Desde la página Detalles del destino, lleve a cabo los siguientes pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Se trata de un campo obligatorio.

   El formato es: ftp://<*nombre_servidor_ftp*>:<*núm_puerto*>

   Por ejemplo:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Si no especifica un número de puerto, se utilizará el puerto FTP estándar.

   Nota: Si está especificando una dirección IPv6, proporcione el formato numérico, no el nombre de máquina o el nombre de sistema principal.

   Ejemplos de direcciones IPv6 son:

   ```
   ftp://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:21
   ftp://[1080:0:0:0:8:800:200C:417A]:21
   ftp://[3ffe:2a00:100:7031::1]:21
   ftp://[1080::8:800:200C:417A]:21
   ftp://[::192.9.5.5]:21
   ftp://[::FFFF:129.144.52.38]:21
   ftp://[2010:836B:4179::836B:4179]:21
   ```
2. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor FTP.
3. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
4. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.

5. En el campo **Número de hebras**, especifique el número de documentos que pueden procesarse simultáneamente. El valor predeterminado es 3.
6. En el campo **Validar IP de cliente**, seleccione **Sí**, si desea que la dirección IP del remitente se valide antes de procesar el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
7. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si está a punto de producirse una anomalía de entrega porque que haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

   Cuando se selecciona **Cola automática**, todos los documentos permanecerán en la cola hasta que el destino se ponga en línea manualmente.
8. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
9. Si desea que el documento tenga su propio nombre cuando se envía a su destino, no seleccione **Utilizar nombre de archivo exclusivo**. De lo contrario, seleccione esta opción si desea que WebSphere Partner Gateway asigne un nombre al archivo.
10. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 243. De lo contrario, pulse **Guardar**.

Configuración de un destino SMTP

Acerca de esta tarea

Para crear un destino SMTP, utilice el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Detalles del destino

Acerca de esta tarea

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Se trata de un campo obligatorio.

   El formato es: mailto:<*usuario@nombre_servidor*>

   Por ejemplo:

   ```
   mailto:admin@anotherserver.ibm.com
   ```

2. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor SMTP.
3. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
4. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.
5. En el campo **Número de hebras**, especifique el número de documentos que pueden procesarse simultáneamente. El valor predeterminado es 3.
6. En el campo **Validar IP de cliente**, seleccione **Sí**, si desea que la dirección IP del remitente se valide antes de procesar el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
7. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si está a punto de producirse una anomalía de entrega porque que haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

   Cuando se selecciona **Cola automática**, todos los documentos permanecerán en la cola hasta que el destino se ponga en línea manualmente.
8. En el campo **Autenticación obligatoria**, indique si el documento proporciona un nombre de usuario y contraseña. El valor predeterminado es **No**.
9. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 243. De lo contrario, pulse **Guardar**.

Configuración de un destino JMS

Acerca de esta tarea

Para crear destinos JMS, siga el procedimiento siguiente.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Nota: Para obtener información sobre cómo configurar las bibliotecas de tiempo de ejecución para que los archivos jar de MQ necesarios sean visibles para WebSphere Partner Gateway, consulte el apartado "Configuración de bibliotecas de tiempo de ejecución" en la página 42.

Detalles del destino

Acerca de esta tarea

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. En el campo **Dirección**, especifique el URL en el que se entregará el documento. Se trata de un campo obligatorio.

   Para WebSphere MQ JMS, el formato del URL de destino es el siguiente:

   `file:///<vía_acceso_enlaces_JNDI_MQ_definidos_usuario>`

   Por ejemplo:

   ```
   file:///opt/JNDI-Directory en el caso de UNIX y
   file://c:/temp/ en caso de Windows.
   ```

   El directorio contiene el archivo ".enlaces" para el JNDI basado en archivos. Este archivo indica a WebSphere Partner Gateway cómo direccionar el documento al destino deseado.

   - Para un destino HMS interno (es decir, un destino al sistema de fondo), este valor debe coincidir con el valor que ha especificado (la vía de acceso del sistema de archivos) al configurar WebSphere Partner Gateway para JMS (paso 5 en la página 40). También puede especificar la subcarpeta para el contexto JMS como parte del URL del proveedor JMS.

     Por ejemplo, sin el contexto JMS, debería indicar `c:/temp/JMS`. Con el contexto JMS, debería indicar `c:/temp/JMS/JMS`.
   - Para destinos de socios, el socio probablemente proporcionará el archivo ".bindings" file.

   Este campo es necesario.
2. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder a la cola JMS.
3. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
4. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.

5. En el campo **Número de hebras**, especifique el número de documentos que pueden procesarse simultáneamente. El valor predeterminado es 3.
6. En el campo **Validar IP de cliente**, seleccione **Sí**, si desea que la dirección IP del remitente se valide antes de procesar el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
7. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si está a punto de producirse una anomalía de entrega porque que haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

   Cuando se selecciona **Cola automática**, todos los documentos permanecerán en la cola hasta que el destino se ponga en línea manualmente.
8. En el campo **Autenticación obligatoria**, indique si el documento proporciona un nombre de usuario y contraseña. El valor predeterminado es **No**.
9. En el campo **Nombre de fábrica JMS**, especifique el nombre de la clase Java que el proveedor JMS utiliza para conectarse a la cola JMS. Se trata de un campo obligatorio.

   Para destinos JMS internos, este nombre debe coincidir con el nombre especificado con el mandato `define qcf` al crear el archivo de enlaces (paso 4 en la página 41).

   Si ha especificado la subcarpeta para el contexto JMS en el paso 1 en la página 233, indique aquí sólo el nombre de fábrica (por ejemplo, `Hub`). Si no ha especificado la subcarpeta para el contexto JMS en el campo **Dirección**, especifique la subcarpeta antes que el nombre de fábrica (por ejemplo, `JMS/Hub`).
10. En el campo **Clase de mensaje JMS**, especifique la clase de mensaje. Puede seleccionar cualquier clase de mensaje JMS válida, como mensajes de texto o mensajes de bytes. Este campo es necesario.
11. En el campo **Tipo de mensaje JMS**, especifique el tipo de mensaje. Dado que el componente Receptor decide la correlación del tipo de mensaje JMS, el valor del tipo de mensaje JMS es opcional.
12. En el campo **Paquetes de URL del proveedor**, especifique el nombre de las clases (o archivo JAR) que utiliza Java para entender el URL del contexto de JMS. Este campo es opcional. Si no especifica un valor, se utiliza la vía de acceso del sistema de archivos al archivo de enlaces.
13. En el campo **Nombre de cola JMS**, especifique el nombre de la cola JMS a la que se enviarán los documentos. Se trata de un campo obligatorio.

    Para destinos JMS internos, este nombre debe coincidir con el nombre especificado con el mandato `define q` al crear el archivo de enlaces (paso 4 en la página 41).

    Si ha especificado la subcarpeta para el contexto JMS en el paso 1 en la página 233, indique aquí sólo el nombre de cola (por ejemplo, `outQ`). Si no ha especificado la subcarpeta para el contexto JMS en el URL del proveedor JMS, especifique la subcarpeta antes del nombre de fábrica (por ejemplo, `JMS/outQ`).
14. En el campo **Nombre de fábrica JMS JNDI**, especifique el nombre de fábrica utilizado para conectar con el servidor de nombres. Se trata de un campo obligatorio. El valor de com.sun.jndi.fscontext.RefFSContextFactory es probablemente el que se utilizará si se establece la configuración de JMS para WebSphere MQ tal como se describe en el apartado “Configuración del concentrador para el protocolo de transporte JMS” en la página 39.
15. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a “Configuración de manejadores” en la página 243. De lo contrario, pulse **Guardar**.

Configuración de un destino de directorio de archivos

Acerca de esta tarea

Para crear destinos de directorio de archivos, utilice el siguiente procedimiento.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Detalles del destino

Acerca de esta tarea

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Se trata de un campo obligatorio.

   El formato para los sistemas UNIX y Windows en los que el directorio de archivos se encuentra en la misma unidad en la que WebSphere Partner Gateway se encuentra instalado es: file://*<vía_acceso_a_directorio_destino>*

   Por ejemplo:

   ```
   file://dirarchlocal
   ```

   donde *localfiledir* es un directorio del directorio raíz.

   Si el destino de directorio de archivos se debe crear en cualquier unidad de Windows, DISTINTA de la unidad en la que está instalado WebSphere Partner Gateway, la vía de acceso es: file:///*<letra_unidad>*:/*<vía_acceso>*
2. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
3. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.
4. En el campo **Número de hebras**, escriba el número de documentos que se deben procesar simultáneamente. El valor predeterminado es 3.

5. En el campo **Validar IP de cliente**, seleccione **Sí**, si desea que la dirección IP del remitente se valide antes de procesar el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
6. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si está a punto de producirse una anomalía de entrega porque que haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

   Cuando se selecciona **Cola automática**, todos los documentos permanecerán en la cola hasta que el destino se ponga en línea manualmente.
7. Si desea que el documento tenga su propio nombre cuando se envía a su destino, no seleccione **Utilizar nombre de archivo exclusivo**. De lo contrario, seleccione esta opción si desea que WebSphere Partner Gateway asigne un nombre al archivo.
8. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores" en la página 243. De lo contrario, pulse **Guardar**.

Configuración de un destino FTPS

Acerca de esta tarea

Para crear destinos FTPS, utilice el siguiente procedimiento.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Nota: La modalidad de FTPS pasiva no tiene soporte. Consulte el apartado "Configuración de un destino de FTP Scripting" en la página 239 para obtener información sobre soporte pasivo.

Detalles del destino

Acerca de esta tarea

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. En el campo **Dirección**, especifique el URI en el que se entregará el documento. Se trata de un campo obligatorio.

   El formato es: ftp://<*nombre_servidor_ftp*>:<*núm_puerto*>

   Por ejemplo:

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Si no especifica un número de puerto, se utilizará el puerto FTP estándar.
2. Si lo desea, especifique un nombre de usuario y contraseña si son necesarios para acceder al servidor FTP seguro.
3. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
4. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.
5. En el campo **Número de hebras**, escriba el número de documentos que se deben procesar simultáneamente. El valor predeterminado es 3.
6. En el campo **Validar IP de cliente**, seleccione **Sí**, si desea que la dirección IP del remitente se valide antes de procesar el documento. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
7. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si está a punto de producirse una anomalía de entrega porque que haya agotado el número de reintentos. De lo contrario, seleccione **No**. El valor predeterminado es **No**.

   Cuando se selecciona **Cola automática**, todos los documentos permanecerán en la cola hasta que el destino se ponga en línea manualmente.
8. En el campo **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
9. Si desea que el documento tenga su propio nombre cuando se envía a su destino, no seleccione **Utilizar nombre de archivo exclusivo**. De lo contrario, seleccione esta opción si desea que WebSphere Partner Gateway asigne un nombre al archivo.
10. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a “Configuración de manejadores” en la página 243. De lo contrario, pulse **Guardar**.

Configuración de un destino SFTP

Acerca de esta tarea

Configure un destino SFTP para que puedan enviarse documentos desde el concentrador a la dirección IP del socio. El adaptador conecta al servidor SFTP y le envía el documento. Se proporcionan losdatos del documento al adaptador como una secuencia.

Para crear destinos SFTP, utilice el siguiente procedimiento.

1. Pulse **Administración de cuentas> Perfiles > Socio**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.

4. Pulse **Destinos**.
5. Pulse **Crear**.

Detalles del destino

Acerca de esta tarea

En la página Detalles del destino, lleve a cabo los siguientes pasos:

1. Especifique un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.
5. Seleccione **SFTP** en la lista **Transporte**.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. Introduzca **SFTP host IP / nombre de host**. Se aceptarán un máximo de 100 caracteres. También puede introducir direcciones de IP, IPv4 y direcciones IPv6.
2. Introduzca el **Número de puerto**. EL valor mínimo es 1 y el máximo es 65535. El valor predeterminado es 22.
3. Introduzca el **Directorio de salida**. Se aceptarán un máximo de 100 caracteres. Puede contener caracteres locales.
4. En **Tipo de autenticación**, seleccione el nombre de usuario y la contraseña o la autenticación de clave privada.
5. En el campo **Cola automática**, seleccione **Sí** si desea que el destino se sitúe fuera de línea (automáticamente) si se produce una anomalía de entrega. De lo contrario, seleccione **No**. El valor predeterminado es **No**.
6. Especifique el **Nombre de usuario** y la **Contraseña** del nombre de usuario/contraseña. Si el tipo de autenticación corresponde a una autenticación de clave privada, especifique el **Nombre de usuario**, el **Archivo de clave privada** y la **Frase de paso**. **Archivo de clave privada** es la vía de acceso al archivo de clave privada en formato OpenSSH.
7. Especifique **Recuento de reintentos**. Número de veces que el receptor intentará conectarse al servidor SFTP en caso de que la conexión no fuese satisfactoria.
8. Especifique **Intervalo de reintentos**. Tiempo de espera para el receptor entre reintentos.
9. Especifique el **Número de hebras**.
10. **Codificación EIS** es la codificación del servidor FTP. Utilice este valor para establecer la codificación de la conexión de control del servidor FTP.
11. Se puede **Habilitar autenticación de servidor** para autenticar el servidor con el que se establece la conexión. Si se ha habilitado la autenticación de servidor, especifique la vía de acceso del archivo de claves de host. El archivo de claves de host debe utilizar el formato OpenSSH.

12. Pulse **Guardar** para guardar la configuración.
13. Especifique la configuración del manejador y pulse **Guardar** para guardar los detalles de la configuración.

Nota: Reinicie el correspondiente servidor después de guardar la configuración:

- En la modalidad simple, reinicie el servidor bcgserver.
- En la modalidad distribuida simple, reinicie el clúster bcgserver.
- En la modalidad distribuida completa, reinicie el clúster BCGDocMgr.

Configuración de un destino de FTP Scripting

Un destino de FTP Scrtipting se ejecuta de acuerdo con una planificación establecida. El comportamiento de un destino de scripts FTP se controla mediante un script de mandatos FTP.

Nota: Si la base de datos está inactiva y el bloqueo de usuarios está establecido en "sí", es posible que el destino de FTP Scripting no funcione ya que no puede obtener el bloqueo de la base de datos.

Nota: En la plataforma AIX, utilice la modalidad pasiva para entregar documentos con volúmenes de transacción elevados. En la operación de transferencia de archivo, especifique la modalidad pasiva en el script que el destino de FTP Scripting utiliza. Se puede utilizar el mandato 'passive' o el mandato 'pasv' en el script. La utilización de la modalidad activa genera un error.

Creación de scripts FTP

Acerca de esta tarea

Para utilizar un destino de FTP Scripting, cree un archivo que incluya todos los mandatos FTP necesarios que puedan ser aceptados por el servidor FTP.

1. Cree un script para los destinos para indicar las acciones que desea realizar. En el siguiente script se muestra un ejemplo de cómo conectarse al servidor FTP especificado (con el nombre y la contraseña especificados), pasar al directorio especificado en el servidor FTP y enviar todos los archivos al directorio especificado en el servidor.

   ```
   open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
   cd %BCGOPTIONx%
   mput *
   quit
   ```

   Los indicadores de posición (por ejemplo, %BCGSERVERIP%) se sustituyen cuando el destino se pone en funcionamiento por los valores que se entran cuando se crea una instancia específica de un destino de scripts FTP, tal como se muestra en la tabla siguiente:

Tabla 30. Cómo correlacionar parámetros de script con entradas de campo de destino de FTP Scrtipting

Parámetro de script	**Entrada de campo de pasarela de scripts FTP**
%BCGSERVERIP%	IP de servidor
%BCGUSERID%	ID de usuario
%BCGPASSWORD%	Contraseña
%BCGOPTIONx%	Opción *x*, en **Atributos definidos por el usuario**

Puede haber hasta 10 opciones definidas por el usuario.

2. Guarde el archivo.

Mandatos de scripts FTP

Puede utilizar los siguientes mandatos al crear el script:

- ascii, binary, passive, epsv

  Estos mandatos no se envían al servidor FTP. Modifican la modalidad de transferencia (ascii, binary o passive) al servidor FTP.

- cd

  Este mandato le lleva al directorio especificado.

- delete

  Este mandato suprime un archivo del servidor FTP.

- mkdir

  Este mandato crea un directorio en el servidor FTP.

- mput

  Este mandato acepta un solo argumento, que especifica los archivos que deben transferirse al sistema remoto. Este argumento puede contener los caracteres comodín estándar para identificar varios archivos ('*' y '?')..

- mputren

  Este mandato toma tres argumentos: <source>, <temporary> y <target> donde un asterisco (*) representa el nombre de archivo que se está procesando actualmente.

  fuente El nombre del archivo que se va a colocar en el servidor FTP. El valor esperado es un asterisco (*).

  temporal
  El nombre de archivo temporal que se va a utilizar cuando se coloque el archivo <source> en el servidor FTP.

  destino
  El nombre de archivo que se va a utilizar para renombrar el archivo <temporary>. Cuando este archivo se haya renombrado, el archivo temporal dejará de existir.

  Ejemplos:

  `mputren * *.tmp *`
  En este ejemplo se coloca el archivo actual en el servidor del FTP con la extensión .tmp. Después de colocar el archivo en el servidor, el archivo se renombrará de nuevo con su nombre original.

  `mputren * *.tmp *.ready`
  En este ejemplo se coloca el archivo actual en el servidor del FTP con la extensión .tmp. Después de colocar el archivo en el servidor, el archivo se renombrará de nuevo su nombre original y con la extensión .ready.

  `mputren * *.tmp /complete/*`
  En este ejemplo se coloca el archivo actual en el servidor del FTP con la extensión .tmp. Después de colocar el archivo en el servidor, el archivo se renombrará con su nombre original pero estará ubicado en el directorio /complete. El archivo temporal *.tmp dejará de existir.

mputren * *.tmp /complete/*.final

En este ejemplo se coloca el archivo actual en el servidor del FTP con la extensión .tmp. Después de colocar el archivo en el servidor, el archivo se renombrará con su nombre original pero estará ubicado en el directorio /complete con la extensión .final. El archivo temporal *.tmp dejará de existir.

- open

  Este mandato acepta tres parámetros: la dirección IP del servidor FTP, el nombre de usuario y una contraseña. Estos parámetros se correlacionan con las variables %BCGSERVERIP%, %BCGUSERID% y %BCGPASSWORD%.

  La primera línea del script de destino de FTP Scrtipting debe, por lo tanto, ser:

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```

- quit

  Este mandato finaliza una conexión existente con un servidor FTP.

- quote

  Este mandato indica que todo lo que siga a QUOTE debe enviarse al sistema remoto como mandato. Esto permite enviar a un servidor FTP remoto mandatos que es posible que no estén definidos en el protocolo FTP estándar.

- rmdir

  Este mandato suprime un directorio del servidor FTP.

- site

  Este mandato puede utilizarse para emitir mandatos específicos del sitio al sistema remoto. El sistema remoto determina si el contenido de este mandato es válido.

Destinos de FTP Scripting

Acerca de esta tarea

Si va a utilizar destinos de FTP Scrtipting, lleve a cabo los siguientes pasos:

Para crear destinos de scripts FTP, utilice el siguiente procedimiento.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Crear**.

Detalles del destino

Acerca de esta tarea

En la página Lista de destinos, siga estos pasos:

1. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
2. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.
3. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
4. Si lo desea, especifique una descripción del destino.

Configuración del destino

Acerca de esta tarea

En el apartado **Configuración del destino** de la página, lleve a cabo los siguientes pasos:

1. Escriba la dirección IP del servidor FTP al que está enviando documentos. El valor aquí especificado sustituirá al valor %BCGSERVERIP% cuando se ejecute el script FTP.

   Nota: Si está especificando una dirección IPv6, proporcione el formato numérico, no el nombre de máquina o el nombre de sistema principal.

   Ejemplos de direcciones IPv6 son:

   ```
   FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
   1080:0:0:0:8:800:200C:417A
   3ffe:2a00:100:7031::1
   1080::8:800:200C:417A
   ::192.9.5.5
   ::FFFF:129.144.52.38
   2010:836B:4179::836B:4179
   ```

2. Escriba el ID de usuario y la contraseña necesarios para acceder al servidor FTP. Los valores aquí especificados sustituirán a %BCGUSERID% y %BCGPASSWORD% cuando se ejecuta el script FTP.
3. Si el destino está en modalidad segura, pulse **Sí** para **Modalidad FTPS**. De lo contrario, utilice el valor predeterminado **No**.
4. Suba el archivo script realizando los siguientes pasos:
   a. Pulse **Subir archivo de script**.
   b. Escriba el nombre del archivo que contiene el script para procesar documentos o utilice **Examinar** para desplazarse hasta el archivo.
   c. Seleccione el **Tipo de codificación del archivo de script**.
   d. Pulse **Cargar archivo** para cargar el archivo de script en el recuadro de texto **Archivo de script cargado actualmente**.
   e. Si el archivo de script es el que desea utilizar, pulse **Guardar**.
   f. Pulse **Cerrar ventana**.
5. En el campo **Recuento de reintentos**, especifique el número de veces que desea que el destino intente enviar un documento antes de fallar. El valor predeterminado es 3.
6. En el campo **Intervalo de reintentos**, especifique la cantidad de tiempo que debe esperar el destino antes de volver a intentar enviar el documento. El valor predeterminado es 300 segundos.
7. En **Tiempo de espera de conexión**, especifique el número de segundos que un socket permanecerá abierto sin tráfico. El valor predeterminado es 120 segundos.
8. En el campo **Bloquear usuario**, indique si el destino solicitará un bloqueo, para que ninguna otra instancia de un destino de scripts FTP pueda acceder al mismo directorio del servidor FTP a la vez.

Nota: los valores **Atributos globales de FTP Scripting** ya están rellenados y no se pueden editar en esta página. Para modificar estos valores, utilice la página Atributos de transporte global, como se describe en el apartado “Configuración de los valores de transporte global” en la página 224.

Atributos definidos por el usuario

Acerca de esta tarea

Si desea especificar atributos adicionales, realice los pasos siguientes. El valor que especifique para la opción sustituirá al valor %BCGOPTION*x*% cuando se ejecute el script FTP (donde *x* corresponde al número de la opción).

1. Pulse **Nuevo**.
2. Escriba un valor junto a la **Opción 1**.
3. Si va a especificar atributos adicionales, vuelva a pulsar **Nuevo** y escriba un valor.
4. Repita el paso 3 tantas veces como sea necesario para definir todos los atributos.

Por ejemplo, suponga que el script FTP es parecido al siguiente:

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mput *
          quit
```

En este caso %BCGOPTION% sería un nombre de directorio.

Planificación

Acerca de esta tarea

En el apartado Planificación de la página, realice los siguientes pasos:

1. Indique si desea la planificación basada en intervalos o la planificación basada en agenda.
   - Si elige **Planificación basada en intervalos**, seleccione el número de segundos que deben transcurrir antes de sondear el destino (o aceptar el valor predeterminado).
   - Si selecciona **Planificación basada en calendario**, elija el tipo de planificación (**Planificación diaria**, **Planificación semanal** o **Planificación personalizada**).
     - Si selecciona **Planificación diaria**, especifique la hora del día en que debe sondearse el destino.
     - Si elige **Planificación semanal**, seleccione uno o varios días de la semana además de la hora del día.
     - Si elige **Planificación personalizada**, seleccione la hora del día y luego **Rango** o **Días selectivos** para la semana y el mes. Con **Rango**, indique la fecha de inicio y la fecha de finalización. (Por ejemplo, pulse **Lunes** y **Viernes** si desea que el servidor se sondee a un determinada hora únicamente los días laborables). Con **Días selectivos** puede elegir los días concretos de la semana y del mes.
2. Si desea configurar el paso de preproceso o postproceso para el destino, acceda a "Configuración de manejadores". De lo contrario, pulse **Guardar**.

Configuración de manejadores

Acerca de esta tarea

Puede modificar dos puntos de proceso para un destino: el preproceso y el postproceso.

No se proporciona ningún manejador predeterminado para el paso de preproceso o postproceso y, por lo tanto, no se lista ningún manejador predeterminado en la **Lista disponible**. Si ha subido un manejador, puede seleccionarlo y moverlo a la **Lista configurada**.

Para aplicar un manejador escrito por el usuario para estos puntos de configuración, debe primero subir el manejador. Consulte la publicación *Guía de configuración del concentrador* para obtener paso acerca de cómo subir el cargador. A continuación, siga estos pasos:

1. Seleccione **preproceso** o **postproceso** en la lista **Manejadores de puntos de configuración**.
2. Seleccione el manejador en la **Lista disponible** y pulse **Añadir**.
3. Si desea cambiar los atributos del manejador, selecciónelo en la **Lista configurada** y pulse **Configurar**. Aparecerá una lista de atributos que pueden cambiarse. Haga los cambios necesarios y pulse **Establecer valores**.
4. Pulse **Guardar**.

Puede modificar más la **Lista configurada** como se indica a continuación:

- Elimine un manejador seleccionándolo en la **Lista configurada** y pulsando **Eliminar**. El manejador pasa a la **Lista disponible**.
- Para cambiar el orden en que se procesa el manejador, seleccione el manejador y pulse **Mover arriba** o **Mover abajo**.

Configuración de un destino para un transporte definido por el usuario

Acerca de esta tarea

Si desea subir un transporte definido por el usuario, realice los pasos siguientes.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Destinos**.
3. Pulse **Gestionar tipos de transporte**.
4. Especifique el nombre de un archivo XML que defina el transporte (o utilice **Examinar** para ir hasta el archivo).
5. Utilice el valor predeterminado **Sí** en **Confirmar en base de datos**. Seleccione **No** si está probando este transporte antes de implementarlo en un entorno de producción.
6. Indique si este archivo debe sustituir a un archivo con el mismo nombre que ya está en la base de datos.
7. Pulse **Subir**.

   Nota: en la página Gestionar tipos de transporte, también es posible borrar un tipo de transporte definido por el usuario. No es posible borrar un transporte proporcionado por WebSphere Partner Gateway. Además, no es posible suprimir un transporte definido por el usuario después de haber sido usado para crear un destino.
8. Pulse **Crear**
9. Escriba un nombre para identificar el destino. Se trata de un campo obligatorio.
10. Indicar opcionalmente el estado del destino. **Habilitado** es el valor predeterminado. Un destino que está habilitado está listo para enviar documentos. Un destino que está inhabilitado no puede enviar documentos.

11. Si lo desea, indique si el destino está En línea o Fuera de línea. El valor predeterminado es **En línea**.
12. Si lo desea, especifique una descripción del destino.
13. Complete los campos (que serán exclusivos para cada transporte definido por el usuario) y pulse **Guardar**.

Especificación de un destino predeterminado

Acerca de esta tarea

Después de crear destinos para el socio interno o para el socio, seleccione uno de los destinos como el destino predeterminado.

1. Pulse **Administración de cuentas > Perfiles>**.
2. Especifique los criterios de búsqueda y pulse **Buscar**, o bien pulse **Buscar** sin especificar ningún criterio de búsqueda para mostrar una lista de todos los socios.
3. Pulse el icono **Ver detalles** para mostrar el perfil del socio.
4. Pulse **Destinos**.
5. Pulse **Ver destinos predeterminados**.

   Aparecerá una lista de destinos definidos para el socio.
6. En la lista **Producción**, seleccione el destino que será el valor predeterminado para este socio. También puede establecer destinos predeterminadas para otros tipos de destinos, como **Prueba**.
7. Pulse **Guardar**.

Capítulo 12. Gestión de conexiones

Después de crear las funciones B2B de los socios y crear las interacciones, establezca conexiones entre los socios internos y los socios externos. Este capítulo incluye los siguientes temas:

- "Visión general de las conexiones"
- "Activación de conexiones de socio"
- "Especificación o cambio de atributos" en la página 248

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Visión general de las conexiones

Defina una conexión entre los socios para cada tipo de documento que será intercambiado. Por ejemplo, puede que tenga varias conexiones del socio interno al mismo socio, porque el empaquetado, protocolo, tipo de documento, acción o correlación puede que sean diferentes.

Cuando se activan conexiones, es posible especificar atributos para el socio de origen o destino. Cualquier atributo que establezca en el nivel de conexión tiene prioridad sobre los atributos que establezca en el nivel de funciones B2B (para un socio determinado) o en el nivel de definición de documentos.

Para los documentos EDI, XML y ROD, dispone de varias conexiones para cada intercambio, si éste implica la acción de ensobrado o transformación. Para definir más las conexiones para estos tipos de documentos, seleccione un conjunto de perfiles asociados con la conexión. Consulte el apartado "Perfiles de conexión" en la página 198 para obtener más información.

Configuración de varios socios internos

WebSphere Partner Gateway no tiene ninguna restricción en el número de socios internos. Es necesario configurar el socio interno predeterminado para que proporcione compatibilidad con versiones anteriores para los documentos binarios y de servicios web que se desplazan a través de las características de soporte de FTPScript. Para obtener más información sobre la configuración de documentos binarios y de servicios web para varios socios internos, consulte el capítulo Configuración de tipos de documento.

Activación de conexiones de socio

Acerca de esta tarea

Las conexiones de socio contienen la información necesaria para un intercambio adecuado de cada tipo de documentos. Un documento no puede ser direccionado a no ser que exista una conexión entre el Socio interno y uno de sus socios externos.

El sistema crea conexiones de forma automática entre los socios internos y los socios externos basadas en sus funciones e interacciones B2B.

Busque estas conexiones y, a continuación, actívelas.

Cuando seleccione un Origen y un Destino, asegúrese de que la fuente sea única.

Utilice el siguiente procedimiento para realizar una búsqueda básica de conexiones y, a continuación, activar las conexiones.

1. Pulse **Administración de cuentas > Conexiones**. Se mostrará la página Gestionar conexiones.
2. En **Origen**, seleccione un origen. Por ejemplo, si está definiendo un intercambio con origen en el socio interno, seleccione el Socio interno.
3. En **Destino**, seleccione un destino. Por ejemplo, si está definiendo un intercambio que será recibido por un socio, seleccione dicho socio.

   Nota: cuando cree una nueva conexión, el origen y el destino deben ser exclusivos.
4. Pulse **Buscar** para buscar las conexiones que coinciden con su criterio.

   Nota: puede también utilizar la página Búsqueda avanzada si desea especificar criterios de búsqueda detallados.
5. Para activar una conexión, pulse **Activar**. Se vuelve a visualizar la página Gestionar conexiones, esta vez con la conexión resaltada en verde. Esta página muestra el paquete, protocolo y tipo de documento del origen y destino. También proporciona botones que pueden pulsarse para ver y cambiar el estado y parámetros de la conexión de socios.
6. Para especificar atributos para el origen y socio o para seleccionar un perfil de conexión, consulte el apartado “Especificación o cambio de atributos”.

En el caso de un PIP de dos acciones, active la conexión en ambas direcciones para dar soporte a la segunda acción del PIP. Para ello, el origen y el destino de la segunda acción son los opuestos al origen y el destino de la primera acción.

En el caso de los documentos EDI, XML o ROD para los que se ha definido más de una interacción, asegúrese de activar todas las conexiones asociadas con las interacciones.

Especificación o cambio de atributos

Acerca de esta tarea

Cuando se activa la conexión, puede establecer atributos o modificar los que se han definido previamente. Para especificar o cambiar los atributos para esta conexión:

1. Pulse **Atributos** para ver o cambiar los valores de atributos.

   Por ejemplo, suponga que un socio interno está enviando un documento empaquetado como Ninguno a un socio. El socio recibirá el documento empaquetado como AS. Es posible que el socio interno tenga más de un ID de empresa asignado. Para indicar a WebSphere Partner Gateway el ID que se utilizará:
   a. Pulse **Atributos** en el lado Origen de la conexión.
   b. Cuando aparece la página Atributos de conexión, expanda la carpeta **Ninguno**.
   c. En la lista **Actualización** seleccione el ID de AS que desea enviar al socio.
   d. Pulse **Guardar**.

Nota: si anteriormente ha especificado un ID AS (por ejemplo, en la página de funciones B2B), el valor que se entra aquí alterará temporalmente el valor anterior.

Otro ejemplo del establecimiento de atributos es especificar un valor para la dirección MDN cuando esté recibiendo documentos empaquetados como AS de un socio. La dirección específica donde se entrega la MDN.

2. Pulse **Acciones** si desea ver o cambiar una acción o una correlación de transformación asociada a esta conexión. Cualquier cambio que realice altera temporalmente los demás valores establecidos para la acción o correlación.
3. Pulse **Destinos** si desea ver o cambiar el destino de origen o de destino.
4. Si aparece el botón **Añadir perfil de conexión** y aparece la lista **Perfiles activos**, puede asociar esta conexión a un perfil concreto que se ha definido previamente.

Los atributos que establezca en el nivel de conexión tienen prioridad sobre cualquier atributo que establezca en el nivel de protocolo o de tipo de documento.Si el atributo está asociado a nivel de tipo de documento, protocolo y paquete, el valor de tipo de documento prevalecerá sobre el establecido a nivel de protocolo y paquete.

Capítulo 13. Habilitación de la seguridad para intercambios de documentos

Con WebSphere Partner Gateway, puede instalar y utilizar varios tipos de certificados para asegurar las transacciones de entrada y de salida. Este capítulo incluye los siguientes temas:

Los certificados y protocolos de seguridad proporcionan las siguientes ventajas de seguridad en WebSphere Partner Gateway:

- Verificación sobre quién envía el documento
- Verificación que el documento no ha sido alterado durante el tránsito
- Prevención de que otros usuarios vean el contenido del documento
- Verificación de que la persona que envía el documento está realmente autorizada a hacerlo.

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Visión general de la seguridad

Mecanismos de seguridad y protocolos utilizados en WebSphere Partner Gateway

Dependiendo del protocolo empresarial, WebSphere Partner Gateway utiliza certificados para habilitar estos mecanismos para mantener los intercambios de documentos seguros:

Cifrado y descifrado

El cifrado es una manera de modificar los datos para que los datos no puedan ser leídos hasta que sean descifrados. WebSphere Partner Gateway utiliza un sistema criptográfico conocido como cifrado de clave pública para garantizar la seguridad de la comunicación entre los socios y el concentrador. Distintos protocolos como AS2 o RosettaNet tienen requisitos referentes al cifrado. SSL también utiliza cifrado. En este capítulo, a no ser que se indique lo contrario, la utilización del término *cifrado* se aplica a los protocolos empresariales.

El descifrado es una manera de descifrar los datos cifrados para que se puedan leer. El descifrado se lleva a cabo en documentos entrantes.

WebSphere Partner Gateway puede enviar datos cifrados de OpenPGP. El paquete de datos recibido se descifra mediante la clave privada. Si desea que el envío de documentos esté siempre cifrado, establezca el atributo **Cifrado necesario** en `Sí` en el lado de destino de la conexión. Si desea que los documentos cifrados contengan un paquete de código detección de modificaciones, establezca la **Detección de modificaciones** en `Verdadero` en el lado de destino de la conexión. Si recibe datos cifrados con protección de integridad, después del descifrado, se verifica la integridad de los datos mediante el paquete de código de detección de modificaciones. El último paquete descifrado de los datos descifrados tiene que se un paquete de código de detección de modificaciones. En este caso, los datos cifrados incluyen un paquete de datos de integridad protegida cifrados simétricamente para que se pueda verificar la integridad del mensaje. Debe definir los atributos de cifrado en el lado de destino de la conexión. Para el paquete OpenPGP, se soporta RFC 4880. Si necesita enviar datos cifrados con protección de integridad, establezca la **Detección de modificaciones** en `Verdadero` y seleccione las preferencias de algoritmo simétrico. Esta funcionalidad sólo se define en RFC 4880.

Compresión

Al enviar un documento, en el paso de empaquetado, los datos se deben comprimir según la preferencia de algoritmo de compresión establecida en la conexión del destino. Al recibir un mensaje comprimido, éste se descomprime. Si desea que el envío de documentos esté siempre comprimido, establezca el atributo **Compresión necesaria** en `Sí` en el lado de destino de la conexión. Para el paquete OpenPGP, se soporta RFCs 4880.

Cifrado y compresión

Cuando tenga que cifrar y comprimir un documento, establezca todos los atributos de objeto de direccionamiento para cifrado y compresión en el lado de destino de la conexión. El cifrado se realiza según RFC 4880. Cuando reciba un mensaje cifrado y comprimido, se realiza el descifrado. Después del descifrado, se obtiene un paquete de datos comprimido en el que se realiza la descompresión. Al enviar datos cifrados con protección de integridad, establezca el atributo de Detección de modificaciones en el lado de destino de la conexión.

Firma digital y verificación de firma digital

La firma digital es el mecanismo para verificar quién ha enviado un documento y que el documento no ha sido alterado durante su tránsito. Es también útil para asegurar que no se produce ningún rechazo. El no rechazo quiere decir que un socio no puede negar haber originado y enviado un mensaje. También asegura que el socio no puede negar haber recibido el mismo mensaje.

Nota: La información de no rechazo se obtiene de los parámetros de conexión del socio. Los parámetros de conexión del socio se obtienen después de una comprobación de conexión de socio satisfactoria. De forma predeterminada, el no rechazo está establecido en "Yes", que significa que si la información no está disponible desde la conexión del socio por algún motivo, el documento se colocará en el almacén de no rechazo.

SSL SSL es un protocolo utilizado frecuentemente para gestionar la seguridad a través de Internet. SSL proporciona conexiones seguras habilitando dos aplicaciones enlazadas a través de una conexión de red para verificar que cada una es de confianza y cifrando los datos para garantizar la confidencialidad. El cifrado es independiente del tipo de datos. SSL se utiliza en transportes como HTTP y FTP.

Autenticación básica

Cuando se envía cualquier mensaje entrante a través de HTTP o HTTPS, el receptor puede autenticar al socio emisor mediante las credenciales de autenticación básicas. El ID de usuario y la contraseña se pasan en la cabecera HTTP. Cuando también se envía la contraseña, debería utilizarse la autenticación básica con SSL/TLS para asegurarse de que las cabeceras estén cifradas. La autenticación se proporciona utilizando ID de empresa/nombre de usuario:contraseña o bien Nombre de usuario:contraseña en el formato de codificación Base64. El valor en la cabecera HTTP se tiene en cuenta sólo si **Habilitar autenticación básica** está establecido en verdadero. Seleccione Autenticación básica en la página de información del Receptor de la consola para establecerla en Verdadero.

Si la autenticación falla, se devolverá al emisor una respuesta indicando que la autenticación ha fallado. De lo contrario, el documento se envía para su posterior proceso. En caso de autenticación de cliente SSL, se identifican los ID de empresa del socio emisor. Cuando se recibe el documento, el receptor comprueba si el certificado está asociado con algún socio, y el documento falla si no hay ninguna coincidencia. Para mantener la compatibilidad con versiones anteriores, al enviar un mensaje SOAP con autenticación básica, establezca el distintivo **Habilitar autenticación básica** en "No" en el receptor. A menos que la autenticación del documento falle en el receptor, puede visualizar el documento en el Visor de documentos. La autenticación básica está soportada para los siguientes documentos:

- Documentos EDI/XML
- Documentos AS2 con carga binaria/EDI/XML
- Solicitud de servicios web
- Mensaje de Rosettanet
- Mensaje ebMS

La seguridad puede estar en el transporte o en el protocolo empresarial. La autenticación de los usuarios en el receptor soporta documentos binarios de socios

externos a través de HTTP. El socio emisor se identifica mediante las credenciales de autenticación básica o bien mediante las credenciales de autenticación de cliente SSL.

Certificados y mecanismos de seguridad

Los certificados forman la base de los tres enfoques de seguridad: cifrado, firmas digitales y SSL. Permiten que dichos enfoques funcionen en WebSphere Partner Gateway. La utilización de un certificado mantiene los documentos seguros durante una transmisión.

Cada socio tiene uno o más certificados para enviar o recibir documentos con WebSphere Partner Gateway y WebSphere Partner Gateway representado por el operador de concentrador tiene uno o más certificados para enviar o recibir documentos con el socio.

Nota: los mismos certificados utilizados para un socio o para el operador de concentrador se aplican a todos los documentos. Los certificados no varían por tipo de documento.

Certificados y cifrado

Un certificado contiene la parte de clave pública de un par de claves públicas/privadas relacionadas matemáticamente. La clave pública "bloquea" o cifra un documento antes de enviarlo y lo hace de tal manera que sólo la clave privada puede entonces "desbloquear" o descifrar un documento después de haberlo enviado. Una clave pública se denomina así porque se comparte con los socios que envían documentos cifrados mientras que la clave privada se guarda individualmente para poder descifrarla. Un certificado contiene la clave pública y la vincula a un Nombre de Asunto, que constituye el nombre de la entidad final a la que pertenece el certificado.

Los certificados son generados por el socio y suelen estar firmados automáticamente o emitidos por una CA. Un certificado emitido por una CA es un certificado que un socio ha solicitado utilizando una Solicitud de firma de certificado y recibido de una autoridad certificadora (CA). Un certificado emitido por una CA está firmado por la CA y no por el socio. Cada socio tiene al menos un certificado que utilizar para enviar o recibir documentos.

El cifrado de documentos empresariales sólo se aplica si el estándar empresarial da soporte al cifrado. No todos los estándares dan soporte al cifrado. Para aquellos estándares que sí dan soporte al cifrado éste será aplicado de diferente manera dependiendo de cada estándar. WebSphere Partner Gateway entiende las diferencias entre los estándares y cómo aplicar el cifrado.

Si WebSphere Partner Gateway está enviando un documento a un socio, se utilizará el certificado de los socios para cifrar el documento. De esta manera sólo el socio puede leer el contenido descifrando el documento con su propia clave privada. El certificado que se utilice será el certificado de cifrado cargado en WebSphere Partner Gateway para dicho socio.

Si un socio está enviando un documento a WebSphere Partner Gateway, el socio utiliza el certificado de los operadores del concentrador para cifrar dicho documento. De esta manera el operador de concentrador que tiene la clave privada puede leer el contenido descifrando el documento. La clave privada que se utiliza es la que se carga para el operador de concentrador en la opción Cargar PKCS12. Tenga en cuenta que el administrador debe proporcionar el certificado de Operador del concentrador al socio.

Notas:

1. WebSphere Partner Gateway da soporte a los algoritmos RC2 y TripleDES. No da soporte al algoritmo RC5. Si en un release anterior utilizaba el algoritmo RC5, sustitúyalo por uno de los algoritmos soportados.
2. WebSphere Partner Gateway también tiene soporte para los algoritmos siguientes:
   - AES, TripleDES y RC2: para documentos ebMS enviados y recibidos.
   - TripleDES y RC2: para documentos RNIF.
   - DES: para ebMS, pero se recomienda utilizar algoritmos más potentes como RC2, TripleDES o AES.

   Puede establecer estos algoritmos en la consola de WebSphere Partner Gateway en la vista Administración del sistema > Administración del Gestor de documentos > Seguridad con la API de SecurityService en Salidas de usuario. Consulte la publicación *Guía del administrador de WebSphere Partner Gateway* para obtener información acerca de las propiedades de seguridad. Consulte la publicación *WebSphere Partner Gateway Programmer Guide* para obtener información sobre SecurityService.

Procedimiento básico

Para recibir un documento cifrado, debe completar los siguientes pasos básicos. Para obtener el procedimiento completo, consulte el apartado "Utilización de certificados para habilitar el cifrado y el descifrado" en la página 263.

1. Obtenga un par de claves públicas/privadas generándolo o recibiendo una de una CA.
2. Suba la clave privada al servidor de WebSphere Partner Gateway en el Operador de concentrador (únicamente los socios internos pueden utilizar la clave) o socio Interno (únicamente ciertos socios internos podrán utilizar la clave), para que el servidor pueda descifrar los documentos entrantes.
3. Proporcione el certificado público al socio comercial para que pueda subir el certificado a ese servidor del socio y para que el socio pueda cifrar los documentos antes de enviarlos.

Una vez ha completado este procedimiento, este socio, utilizando el certificado, puede enviar documentos cifrados de tal manera que sólo el destinatario pueda descifrarlos. Para enviar documentos cifrados a los socios, deberá invertir este procedimiento, subiendo sus certificados y utilizando dichos certificados para cifrar los documentos que desee enviarles.

Certificados y firmas digitales

WebSphere Partner Gateway da soporte a las firmas digitales según los requisitos de los protocolos B2b. Puede utilizar certificados para firmar de un modo similar a los certificados de cifrado, excepto que en este caso se realiza a la inversa. Debe crear el certificado para enviar un documento con una firma digital a los socios y no viceversa.

Las firmas digitales se utilizan para verificar el remitente real del documento y para comprobar que el documento no ha sido alterado durante su tránsito. Sólo se aplican si el estándar empresarial da soporte a las firmas digitales. No todos los estándares dan soporte a firmas digitales. Para aquellos estándares que sí dan soporte a las firmas digitales éstas serán aplicadas de diferente manera dependiendo de cada estándar. WebSphere Partner Gateway entiende las diferencias entre los estándares y cómo aplicar las firmas digitales.

Si WebSphere Partner Gateway envía un documento a un socio, se utilizará la clave privada de los operadores de concentrador cargada en la opción PKCS12 para firmar el documento. El socio utiliza el certificado del operador de concentrador para verificar que WebSphere Partner Gateway es quien ha firmado el documento. Si la clave privada de los operadores del concentrador no ha sido utilizada para firmar el documento, el certificado de los operadores de concentrador que posee el socio no funcionará para verificar las firmas. Tenga en cuenta que el administrador debe proporcionar el certificado de Operador del concentrador al socio.

Si un socio envía un documento a WebSphere Partner Gateway, WebSphere Partner Gateway utiliza el certificado de firma digital del socio para verificar que dicho socio es quien ha firmado el documento. Si no se ha utilizado la clave privada del socio para firmar el documento, el certificado que WebSphere Partner Gateway posee para dicho socio no funcionará para verificar la firma.

Procedimientos básicos:

Para enviar un documento firmado digitalmente, deberá completar los siguientes pasos. Para obtener el procedimiento completo, consulte el apartado "Utilización de certificados para habilitar la firma digital" en la página 268.

1. Obtenga un par de claves públicas/privadas generándolo o recibiendo una de una CA.
2. Suba la clave privada al servidor de WebSphere Partner Gateway como operador de concentrador para que el servidor pueda firmar los documentos que se están enviando.
3. Proporcione el certificado público al socio comercial para que pueda subir el certificado al servidor del socio y para que el socio pueda verificar la procedencia de los documentos.

Una ves haya completado este procedimiento deberá, utilizando la clave privada, enviar documentos firmados digitalmente para que el socio sepa que nadie más puede haberlos enviado. Para recibir documentos de los socios firmados de manera similar, deberá invertir este procedimiento, subiendo sus certificados y utilizándolos para garantizar su origen.

Certificados y SSL/TLS

Cuando envíe documentos, puede utilizar SSL para cifrar documentos para que sólo el destinatario pueda leer dichos documentos y, por lo tanto, garantizando la confidencialidad de los datos.

Dentro de SSL se encuentra el concepto de un *cliente* y de un *servidor*. Un cliente se conecta a un servidor para enviar un documento al servidor. Cuando el cliente se conecta con el servidor, el servidor envía al cliente un certificado para utilizarse al cifrar el documento. Este certificado de servidor forma también parte de la autenticación del servidor, lo cual quiere decir que el servidor usa su certificado para autenticarse a sí mismo con los clientes. A veces el servidor también solicitará un certificado al cliente. Esto se conoce como Autenticación de cliente y el servidor la utiliza para verificar que el cliente es conocido para el servidor.

Cuando WebSphere Partner Gateway está enviando un documento a un socio, WebSphere Partner Gateway es el cliente y el socio es el servidor (es decir, el documento que se está enviando al servidor del socio).

Nota: el servidor del socio es el destino definido en WebSphere Partner Gateway para el socio.

Cuando el socio envía un documento a WebSphere Partner Gateway, el socio es el cliente y WebSphere Partner Gateway es el servidor.

Nota: este es el receptor y ha sido definido en WebSphere Partner Gateway.

Cuando un socio envía un documento a WebSphere Partner Gateway utilizando SSL, se desconoce la identidad real del socio. Si se utiliza la Autenticación de cliente, sigue sin conocerse la identidad del socio. No obstante, lo que sí se conoce es que este socio es de confianza para enviar documentos a WebSphere Partner Gateway. WebSphere Partner Gateway tiene también una característica adicional para identificar el socio a partir del certificado de Autenticación de cliente proporcionado por el socio.

Si WebSphere Partner Gateway está enviando un documento a un socio, el certificado de dicho socio se utiliza para cifrar el documento. Por lo tanto, sólo el socio puede leer el contenido descifrando el documento con la clave privada del socio. Como parte de SSL durante el tiempo de ejecución, el socio enviará dinámicamente el certificado para utilizarlo para cifrar en WebSphere Partner Gateway. WebSphere Partner Gateway verifica que el certificado sea válido generando y validando la vía de acceso a la certificación utilizando los certificados cargados como Raíz/Intermedios en el Operador del concentrador.

Hay una segunda parte opcional de SSL llamada Autenticación de cliente para validar el remitente en la que el socio solicita un certificado de WebSphere Partner Gateway. WebSphere Partner Gateway enviará el certificado de Autenticación de cliente cargado bajo el operador de concentrador. Tenga en cuenta que el certificado de Operador del concentrador para la Autenticación de cliente tiene que ser proporcionado al socio por parte del administrador. Si el certificado de Autenticación de Cliente es un certificado autofirmado, dicho certificado debe entregarse al socio. Si el certificado de Autenticación de Cliente es un certificado CA, dicho certificado puede que deba entregarse al socio, si no dispone con anterioridad del certificado CA.

Si un *socio* está enviando un documento a WebSphere Partner Gateway utilizando SSL, el certificado de WebSphere Partner Gateway se utilizará para cifrar el documento. Por lo tanto, sólo WebSphere Partner Gateway puede leer el contenido descifrando el documento con su propia clave privada. Como parte de SSL durante el tiempo de ejecución, WebSphere Partner Gateway enviará dinámicamente el certificado para que el socio lo utilice para el cifrado. El socio verifica que el certificado es válido comparándolo con el certificado que el Administrador haya proporcionado anteriormente al socio. Hay una segunda parte opcional de SSL llamada Autenticación de cliente para validar el remitente en la que WebSphere Partner Gateway solicita un certificado del socio. El socio enviará el certificado de autenticación a WebSphere Partner Gateway y este certificado será verificado con el certificado que el socio haya proporcionado anteriormente al administrador.

Nota: para recibir documentos de socios utilizando SSL, WebSphere Partner Gateway utiliza los recursos subyacentes de WebSphere Application Server. Por lo tanto, los certificados utilizados durante el tiempo de ejecución no se suben utilizando la consola de WebSphere Partner Gateway sino que le cargan en el almacén de claves y almacén de confianza de WebSphere Application.

Con la Autenticación de cliente hay una identificación de socio adicional que WebSphere Partner Gateway realiza fuera del transporte SSL. El certificado de

Autenticación de Cliente proporcionado por el socio se pasará a WebSphere Partner Gateway, que lo comparará con el certificado cargado para el Cliente SSL de dicho socio para poder identificarlo.

Una conexión SSL basada en HTTP siempre es iniciada por el cliente utilizando un URL que comienza por https:// en lugar de http://. Una conexión SSL empieza con un reconocimiento. Durante esta etapa, las aplicaciones intercambian certificados, acuerdan los algoritmos de cifrado que utilizar y generar las claves de cifrado utilizadas durante el resto de la sesión.

Procedimientos básicos

Para *enviar* un documento utilizando SSL, deberá completar los siguientes pasos básicos. Para obtener el procedimiento completo, consulte el apartado "Utilización de certificados para habilitar SSL" en la página 272.

1. Obtenga un certificado del socio y cárguelo en el almacén de confianza de WebSphere Application Server.
2. Para la Autenticación de cliente para el socio, obtenga un par de claves públicas/privadas generándolo o recibiéndolo de una CA.
3. Suba la clave privada y certificado público al almacén de claves WebSphere Application Server.
4. Proporcione el certificado público al socio empresarial para que ese socio pueda subir el certificado al servidor del socio y para que pueda verificar que se ha recibido el certificado de cliente de autenticación durante la comunicación de tiempo de ejecución de SSL.

Para *recibir* un documento utilizando SSL, deberá completar los siguientes pasos. Para obtener el procedimiento completo, consulte el apartado "Utilización de certificados para habilitar SSL" en la página 272.

1. Obtenga un par de claves públicas/privadas generándolo o recibiendo una de una CA.
2. Suba la clave privada y certificado público al almacén de claves WebSphere Application Server.
3. Proporcione el certificado público al socio empresarial para que ese socio pueda subir el certificado al servidor del socio y para que pueda verificar que se ha recibido el certificado del servidor durante la comunicación de tiempo de ejecución de SSL.
4. Para la Autenticación de cliente obtenga un certificado del socio y cárguelo en el almacén de confianza de WebSphere Application Server. Este será utilizado durante la comunicación de tiempo de ejecución de SSL.
5. Para identificar el socio a partir del certificado de Autenticación de cliente en la consola de WebSphere Partner Gateway, suba el certificado del socio bajo la Autenticación de cliente del socio.

Almacenamiento de certificados en almacenes de claves y almacenes de confianza

WebSphere Partner Gateway tiene dos maneras de almacenar certificados. Para aquellos documentos enviados por un socio a WebSphere Partner Gateway utilizando SSL, los certificados se almacenan en el almacén de claves y almacén de confianza de WebSphere Application Server. Los almacenes de confianza se utilizan para almacenar certificados de confianza que, por su parte, se utilizan para validar que un certificado recibido de un socio es válido. Los almacenes de claves se utilizan para almacenar la clave pública y privada del operador de concentrador de WebSphere Partner Gateway. Los certificados que se utilizan para la seguridad

de documentos de empresa se almacenan cargándolos a través de la consola de WebSphere Partner Gateway. Este apartado describe el almacén de claves y el almacén de confianza utilizados con WebSphere Application Server. Cuando se instala WebSphere Partner Gateway, se crean un almacén de claves y un almacén de confianza para la instancia de WebSphere Application Server en que el receptor y la consola estén instalados.

- Un almacén de claves es un archivo que contiene las claves públicas y privadas.
- Un almacén de confianza es un archivo de base de datos de claves que contiene las claves públicas para los certificados autofirmados y de CA. La clave pública se almacena como el certificado de un firmante. En las CA comerciales se añade el certificado raíz de la CA. Debido a que el archivo de almacén de confianza no contiene la clave privada, el archivo del almacén de confianza puede tener un acceso más público que el archivo del almacén de claves.
- El programa iKeyman se utiliza para administrar el almacén de claves y el almacén de confianza. Este programa de utilidad se describe en aquellos apartados que necesiten su utilización.

  Nota: La consola administrativa de WebSphere Application Server también puede utilizarse para gestionar certificados, almacenes de claves y almacenes de confianza del Receptor y la Consola. Consulte el artículo del Information Center de WebSphere Application Server titulado "Securing applications and their environment" para obtener detalles sobre cómo gestionar certificados y almacenes de claves utilizando la consola administrativa de WebSphere Application Server.

De forma predeterminada, se crea un almacén de claves y un almacén de confianza en el directorio *<DirProducto>*`/common/security/keystore`. Sus nombres son:

- bcgSecurity.jks
- bcgSecurityTrust.jks

Cambio de la contraseña predeterminada

La contraseña predeterminada para acceder a los almacenes es WebAS. WebSphere Application Server está configurado para utilizar estos almacenes. Puede utilizar el programa de utilidad iKeyman para cambiar la contraseña. Como alternativa, puede utilizar el mandato de herramienta de claves para modificar la contraseña del archivo de almacén de claves. En UNIX, el mandato es el siguiente:

```
/<WAS_Installation_Dir>/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
 -storepass $CURRENT_PASSWORD$ -storetype JKS
```

En Windows, utilice el mandato anterior pero utilizando barras invertidas y nombres de unidad.

Si se modifican las contraseñas del almacén de claves, también deberá cambiarse la configuración de las instancias de WebSphere Application Server. Para ello se utilizará el `bcgChgPassword.jacl`. Para la instancia de la consola, navegue al directorio siguiente:

```
/<ProductDir>/bin
```

y ejecute el siguiente mandato:

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/
bcgChgPassword.jacl -conntype NONE
```

Repita este mandato para las instancias de WebSphere Application Server del receptor y el Gestor de documentos.

Nota: en instalaciones en Windows, utilice `bcgwsadmin.bat` en lugar de `./bcgwsadmin.sh`.

Se le solicitará la nueva contraseña.

Sustitución de un certificado caducado

Cuando venza un certificado de un almacén de confianza, deberá añadir un certificado nuevo para sustituirlo mediante el procedimiento siguiente:

1. Inicie iKeyman si no está ya en ejecución.
2. Abra el archivo de almacén de confianza.
3. Escriba la contraseña y pulse **Aceptar**.
4. Seleccione en el menú **Certificados del firmante**.
5. Pulse **Añadir**.
6. Pulse **Tipo de datos** y seleccione un tipo de datos, como datos ASCII codificados con Base64.

   Este tipo de datos debe coincidir con el tipo de datos del certificado de importación.
7. Escriba un nombre y ubicación para el archivo de certificados para el certificado digital raíz de la CA o pulse **Examinar** para seleccionar el nombre y la ubicación.
8. Pulse **Aceptar**.
9. Escriba una etiqueta para el certificado de importación.
10. Pulse **Aceptar**.

Utilización de cadenas de certificados

Una cadena de certificados se compone un certificado de un socio y de cualquier certificado utilizado para autenticar el certificado del socio. Por ejemplo, si se ha utilizado una CA para crear el certificado del socio, es posible que la misma CA haya sido certificada por otra CA. La cadena de confianza empieza en la CA *raíz* (el ancla de confianza). El certificado digital de la CA raíz es autofirmado; es decir, la autoridad certificadora utiliza su propia clave privada para firmar el certificado digital. Cualquier certificado entre el ancla de confianza y el certificado del socio (el certificado de destino) son certificados *intermedios*.

Para todos los certificados emitidos por CA, deben añadirse todos los certificados de la cadena. Por ejemplo, en una cadena de certificados en la que A (el ancla de confianza) es el emisor de B y B es el emisor de C (certificado de destino), los certificados A y B deben subirse como certificados de CA.

WebSphere Partner Gateway trata todos los certificados autofirmados como anclas de confianza. El certificado autofirmado puede ser de una CA (autoridad certificadora) o puede ser un certificado autofirmado generado por el socio.

Para SSL entrante, todos los certificados (ancla de confianza) raíz y certificados intermedios se guardan en el almacén de confianza de WebSphere Application Server Trust como se ha descrito anteriormente. Todos certificados de socios que sus certificados raíz (ancla de confianza) y certificados intermedios se suben bajo el operador de concentrador.

Utilización de certificados primarios y secundarios

Puede crear más de un certificado de un tipo concreto y designar uno como certificado primario y otro como certificado secundario. Si el certificado primario caduca o no se puede utilizar, WebSphere Partner Gateway pasa a usar el certificado secundario.

Nota: Este dispositivo puede utilizarse para realizar la transición desde un certificado antiguo a un certificado nuevo sin tener que detener el servidor. Especifique en la Consola de comunidad qué certificado es el primario y cuál es el secundario.

La capacidad de proporcionar certificados primario y secundario está disponible para los siguientes certificados:

- Certificado de cifrado de un socio
- Certificado de firma del operador de concentrador
- Certificado de cliente SSL del operador de concentrador

Cambio de la complejidad criptográfica

Java Runtime Environment (JRE), que se entrega con WebSphere Partner Gateway, impone limitaciones respecto a los algoritmos criptográficos y la máxima complejidad criptográfica que se puede utilizar. Por ejemplo, una política restringida especifica límites en la longitud permitida y, como resultado, la complejidad de las claves de cifrado. Estas restricciones se especifican en archivos denominados *archivos de política de jurisdicción*. La longitud máxima permitida es de 2048 bytes.

Si desea dar soporte a certificados con un tamaño de clave mayor que 2048 bytes, utilice la versión de complejidad sin restricción o sin límite de los archivos de política de jurisdicción. Puede especificar que desea utilizar una política sin restricciones más enérgica instalando nuevos archivos de política en un subdirectorio del JRE instalado.

Hay también restricciones de cifrado en los algoritmos de claves simétricas, como 3DES. Si necesita un algoritmo de claves simétricas fuerte, si sustituye los archivos de política también se eliminarán las restricciones para las claves simétricas. Por ejemplo, si está utilizando el algoritmo AES, se necesitan archivos de política de criptografía sin restricción. Consulte en el enlace http://www.ibm.com/developerworks/java/jdk/security/50 para obtener detalles.

No obstante, debido a la importación de restricciones de control, los archivos de política sin restricciones enviados con IBM SDK para Java 5 Development Kit permiten utilizar criptografía **fuerte** pero limitada. La tabla siguiente proporciona los tamaños máximos de clave permitidos por esta versión **fuerte** de los archivos de política de jurisdicción:

Tabla 31. Tamaño máximo de clave de algoritmos utilizado en archivos de política de jurisdicción fuertes

Algoritmo	Tamaño máximo de clave
DES	64
DESede	112 (efectiva) o 168 (efectiva)
RC2	128
RSA	2048
* (todos los demás)	128

Nota: Se produce una excepción 'Anomalía de cifrado XMLEncryptionException' al cifrar un mensaje ebMS direccionado con los siguientes parámetros:

- Algoritmo de cifrado:aes-192-cbc o aes-256-cbc
- Protocolo de cifrado: Cifrado Xml

Para resolver este problema, si legalmente se permite, instale los archivos de política criptográfica sin restricciones.

Instrucciones de instalación para los sistemas operativos Windows, Linux y AIX

Para instalar los archivos de política de jurisdicción ilimitada en WebSphere Partner Gateway, realice los pasos siguientes:

1. Descargue los archivos de política de jurisdicción ilimitada utilizando el enlace **IBM SDK Policy files** en el siguiente sitio web: http://www.ibm.com/developerworks/java/jdk/security/50/.
2. Descomprima del archivo descargado en una carpeta temporal.
3. Copie local_policy.jar y US_export_policy.jar de la carpeta temporal.
4. Detenga todos los servidores que aloje la instancia de WebSphere Application Server que está configurando.
5. Vaya a la carpeta *<Dir_instalación_WAS>*\java\jre\lib\security.
6. Cambie el nombre de los archivos existentes local_policy.jar y US_export_policy.jar por local_policy.jar.bak y US_export_policy.jar.bak.
7. Pegue los archivos jar copiados en el paso 3 en la carpeta *<Dir_instalación_WAS>*\was\java\jre\lib\security.
8. Detenga todos los servidores que aloje la instancia de WebSphere Application Server que acaba de reconfigurar.

Estos pasos se aplican a todas las instalaciones de WebSphere Application Server en que tengan instaladas aplicaciones de WebSphere Partner Gateway.

Instrucciones de instalación para los sistemas operativos HP-UX y Solaris

Para las plataformas HP-UX y Solaris, se aplicarán las instrucciones siguientes:

1. Descargue los archivos de política de jurisdicción ilimitada utilizando el enlace **IBM SDK Policy files** en el siguiente sitio web: http://www.ibm.com/developerworks/java/jdk/security/50/.
2. Descomprima del archivo descargado en una carpeta temporal.
3. Detenga todos los servidores que aloje la instancia de WebSphere Application Server que está configurando.
4. Vaya a la carpeta *<Dir_instalación_WAS>*\java\jre\lib\security.
5. Cambie el nombre de los archivos existentes local_policy.jar y US_export_policy.jar por local_policy.jar.bak y US_export_policy.jar.bak.
6. Copie los archivos local_policy.jar y US_export_policy.jar de la carpeta temporal a la carpeta *<Dir_instalación_WAS>*\java\jre\lib\security.
7. Reinicie los servidores que aloje la instancia de WebSphere Application Server que acaba de reconfigurar.

Estos pasos se aplican a todas las instalaciones de WebSphere Application Server en que tengan instaladas aplicaciones de WebSphere Partner Gateway.

SSL con configuración de Autenticación de Cliente

El cliente enviará documentos utilizando un protocolo de transporte con SSL con Autenticación de Cliente, con lo que debe realizarse un cambio adicional en el proveedor JSSE utilizado. Consulte el apartado "Troubleshooting "SSL handshake fails due to no certificate received" del capítulo 14 de la publicación *WebSphere Partner Gateway Administrator Guide* para obtener información adicional.

Caducidad del certificado

Sólo se inhabilitan al caducar los certificados utilizados para el cifrado, la firma digital y SSL. Estos certificados deben ser de entidad final y no certificados CA. Los certificados CA no se inhabilitan cuando caducan.

Si los certificados de raíz o de intermediario caducan entre dos reinicios del servidor, estos certificados no se incluirán en la lista de certificados fiables. Esto significa que si la vía de acceso de certificación creada no es satisfactoria porque no se ha encontrado el certificado CA, podría deberse a que el certificado CA ha caducado. Si un certificado de raíz o de intermediario caduca en tiempo de ejecución, la creación de la vía de acceso de la certificación no será satisfactoria y el certificado correspondiente de la entidad final no se utilizará en la transacción empresarial. Puede comprobar el período de validez y el estado del certificado utilizando la vista Lista de certificados de la consola de WebSphere Partner Gateway. La fecha de validez de los certificados caducados aparece en rojo en esta vista.

Si un certificado CA ha caducado, puede obtener un certificado nuevo de la CA que lo haya expedido. Cargue el certificado CA nuevo mediante el uso de la consola de WebSphere Partner Gateway. Consulte los apartados “Utilización de certificados para habilitar el cifrado y el descifrado”, “Utilización de certificados para habilitar la firma digital” en la página 268 y “Utilización de certificados para habilitar SSL” en la página 272 para obtener información sobre cómo cargar certificados.

Utilización de certificados para habilitar el cifrado y el descifrado

En este apartado se describen los certificados de cifrado y de descifrado.

Creación e instalación de certificados de descifrado entrantes

Este certificado es utilizado por el concentrador para descifrar archivos cifrados recibidos de los socios. El concentrador utiliza la clave privada para descifrar los documentos. El cifrado se utiliza para evitar que otros (a excepción del remitente y el destinatario) puedan ver los documentos en tránsito.

Tenga en cuenta la siguiente restricción importante acerca de recibir mensajes AS2 cifrados de los socios. Si un socio envía un mensaje AS2 cifrado pero utiliza el certificado equivocado, no será posible descifrar. Sin embargo, no se devuelve ninguna MDN al socio para indicar la anomalía. Para que el socio reciba MDN en esta situación, cree una conexión con el socio con la siguiente definición de documento:

- Paquete: **AS** a Paquete: **Ninguno**
- Protocolo: **Binario** a Protocolo **Binario**
- Tipo de documento: **Binario** a Tipo de documento: **Binario**

La conexión creada debe ser una conexión AS a Ninguno, es decir, crea una conexión activando la posibilidad AS B2B en un socio y posibilidad Ninguno B2B en el otro. Asegúrese de que la pasarela de origen en el lado AS es una pasarela

SMTP (en caso de AS1), pasarela HTTP (en caso de AS2) o pasarela FTP (en caso de AS3), que se configura con la dirección de MDN. Así pues, el error de descifrado de MDN se devuelve a la conexión de Ninguno Binario a través de esta AS.

Paso 1: obtención de un certificado
Acerca de esta tarea

Generación de un certificado autofirmado: Si va a utilizar el descifrado, utilice el procedimiento siguiente.

1. Inicie el programa de utilidad iKeyman.
2. Utilice iKeyman para generar un certificado autofirmado y un par de claves.
3. Utilice iKeyman para extraer a un archivo el certificado que contendrá la clave pública.
4. Distribuya el certificado a los socios. Deberán importar el archivo en su producto B2B para utilizarlo como certificado de cifrado. Aconséjelos utilizarlo cuando deseen enviar archivos cifrados al socio interno. Si el certificado está firmado por una CA, proporcione también el certificado de la CA.
5. Utilice el programa iKeyman para guardar la pareja certificado autofirmado y clave privada con el formato de un archivo PKCS12.
6. Vaya a **Perfil** > **{Operador de concentrador/socio interno}** > **certificados** > **Cargar certificado**.
7. En la lista desplegable **¿A qué socio pertenece este certificado?**, seleccione el socio al que se asociará el Certificado recién subido.
8. Pulse **Buscar** para buscar unos socios específicos o un subconjunto de ellos.
9. Pulse **Examinar** al lado de **Ubicación de certificado** para subir el certificado.
10. Pulse **Siguiente**.
11. En Proporcione los detalles del certificado, especifique la siguiente información del certificado: **Certificado sin secundarios**, **Certificado CA raíz** o **Certificado CA intermedio**.
12. Asocie este certificado al **Descifrado**.
13. En **Utilización de certificado**, seleccione **Primario** o **Secundario**.
14. Seleccione **habilitado** o **inhabilitado** en el **Estado** en función de si desea habilitar o inhabilitar el certificado después de subirlo.
15. Seleccione la **Modalidad de funcionamiento**.
16. Pulse **Finalizar** para guardar los cambios y cerrar el asistente.

Utilización de un certificado firmado por una CA: Si piensa utilizar un certificado firmado por una CA, utilice el siguiente procedimiento:

1. Inicie el programa de utilidad iKeyman.
2. Utilice iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
3. Envíe una Solicitud de firma de certificado (CSR) a la CA.
4. Cuando reciba el certificado firmado de la CA, utilice iKeyman para colocar el certificado firmado en el almacén de claves.

Paso 2: distribución del certificado
Acerca de esta tarea

Distribuya el certificado CA firmante a todos los socios.

Instalación de certificados de cifrado salientes

El certificado de cifrado de salida se utiliza cuando el concentrador envía documentos cifrados a los socios. WebSphere Partner Gateway cifra documentos con las claves privadas de los socios y los socios descifran los documentos con sus claves privadas.

El socio puede tener más de un certificado de cifrado. Uno es el certificado primario, que es el que se utiliza de manera predeterminada. El otro es un certificado secundario, que se utiliza si el certificado primario caduca.

Paso 1: obtención de un certificado de socio

Acerca de esta tarea

Obtenga el certificado de cifrado del socio. El certificado debe estar en formato X.509 DER. Recuerde que WebSphere Partner Gateway sólo da soporte a certificados X5.09.

Paso 2: instalación del certificado del socio

Acerca de esta tarea

Instale el certificado mediante la consola de comunidad bajo el perfil del socio realizando el procedimiento siguiente:

1. Vaya a **Perfil** > **Socio externo** > **Certificados** > **Cargar certificado**.
2. En la página **Seleccionar socio, Ubicación de archivo, Contraseña** del asistente, especifique los siguientes valores:
   - En **A qué socio pertenece este certificado o certificados**, seleccione el socio al que asociará el certificado recién cargado. Pulse Buscar para buscar un socio o subconjunto de socios determinados. Si el socio es un Operador de concentrador o un Socio interno, especifique la ubicación del certificado, la ubicación de la clave privada y la contraseña (OR) Proporcione el almacén de confianza o el almacén de claves con la contraseña. Como Socio externo, especifique la ubicación de certificado (OR) proporciona la ubicación del almacén de confianza que contiene la cadena de certificados.
   - **Ubicación de certificado**: Pulse **Examinar** para seleccionar la ubicación del certificado público.
3. Pulse **Siguiente** para ir a la página **Detalles de certificado** del asistente.
4. En la página **Detalles de certificado** del asistente, escriba los siguientes detalles del certificado:
   - **Nombre de certificado sin secundarios** - Nombre del certificado sin secundarios. El nombre de campo depende de si el certificado es un certificado sin secundarios, un certificado CA raíz o un certificado CA intermedio.
   - **Descripción**: Descripción del certificado sin secundarios.
   - **Tipo de certificado** - Asocie este certificado al cifrado.
   - **Utilización de certificado**: Asocie una utilización al certificado. Los valores son Primario y Secundario.
   - **Modalidad de funcionamiento:** especifique la modalidad de funcionamiento.
   - **Estado** - Seleccione habilitado o inhabilitado en función de si desea habilitar o inhabilitar un certificado después de la carga. El botón Siguiente sólo se habilita si se habilita el certificado.

- **Gestión de conjuntos**- Puede asociar un certificado a un conjunto existente o crear un conjunto nuevo. Si el certificado es un certificado secundario, sólo se puede asociar a un conjunto existente. Puede asociar el certificado a cualquier conjunto para un socio interno con tipo cifrado o para un socio externo con tipo SSL (autorización de cliente entrante) o Firma (Verificar).

5. Pulse **Siguiente** para ir a la página Conjunto del asistente. Si el certificado es primario, no tiene que crear conjuntos y asociar el certificado a un conjunto y una conexión participante. Si ha marcado el recuadro de selección **Crear nuevo conjunto**, se abrirá la página **Crear nuevo conjunto** del asistente. De lo contrario, se abrirá la página **Añadir a existente** del asistente. Si el archivo contiene una clave privada del socio interno o el certificado público del socio externo utilizado para SSL / Firma digital, puede pulsar **Finalizar**.
6. En la página **Crear nuevo conjunto** del asistente, especifique los detalles del nuevo conjunto. Para los certificados primarios, no tiene que crear conjuntos y asociar un certificado a ellos. Especifique los siguientes valores:
   - **Nombre de conjunto** - El nombre del conjunto.
   - **Descripción** - La descripción del conjunto.
   - **Estado**: Seleccione habilitado o inhabilitado. Si está inhabilitado, no se habilitará el botón **Siguiente**.
   - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
7. En la página **Añadir a conjunto existente** del asistente, seleccione los conjuntos que se añadirán al certificado. Especifique los siguientes valores:
   - **Seleccionar de la lista de conjuntos disponibles para el tipo de certificado seleccionado** - En la lista, seleccione uno o varios conjuntos para añadir el certificado.
   - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
8. En **Crear nuevo conjunto** o **Añadir al conjunto existente**, pulse **Siguiente** para ir a la página **Valores predeterminados** del asistente. El botón **Siguiente** sólo estará habilitado si el estado del conjunto es habilitado.
9. Seleccione **habilitado** o **inhabilitado** en el **Estado** en función de si desea habilitar o inhabilitar el certificado después de subirlo.

   Nota: Si ha marcado el recuadro de selección **Establecer como conjunto predeterminado** en la página anterior (Crear nuevo conjunto o Añadir a conjunto existente), deberá asociar el conjunto a una modalidad de funcionamiento. Se visualizarán las utilizaciones de certificado según las modalidades de operación. El cifrado se inhabilitará para socios internos. Cliente SSL y Firma digital se inhabilitarán para socios externos.
10. Pulse **Siguiente** para ir a la página de Configuración del asistente. En el caso de que pulse **Siguiente** y de que falten algunos certificados CA raíces o intermedios, se le solicitará que los suba. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** si desea realizar la subida más tarde.
11. En la página Configuración del asistente, especifique los valores siguientes:

    Nota: La página Configuración muestra una lista de utilizaciones de (conjunto de) certificados respecto a las modalidades de operación. El nombre de conjunto actual se lleva previamente para todos, pero puede restablecerlo.
    - **Socio de origen** - Este campo estará rellenado con el valor del socio interno.

- **Socio de destino** - Esta lista desplegable estará rellenada con la lista de socios externos. También puede seleccionar el valor "Todos" para incluir todos los socios externos.
- **De paquete** - En la lista desplegable, seleccione el paquete de objetos de definiciones de flujo de documentos del socio interno.
- **A paquete** - En la lista, seleccione el paquete de objetos de definiciones de flujo de documentos del socio externo.

12. Pulse **Añadir más conexiones** si desea asociar el conjunto a otras conexiones de participantes.
13. Pulse **Añadir certificado secundario** para añadir un certificado secundario al conjunto actual.
14. Pulse **Finalizar** para subir el certificado. En caso de que falten certificados raíz o CA intermedios, se le solicitará que los cargue. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** en la ventana de solicitud si desea realizar la subida más tarde.

Repita este paso si el socio tiene un segundo certificado de cifrado.

Paso 3: instalación de cualquier certificado emitido por una CA

Acerca de esta tarea

Si el certificado ha sido firmado por una CA y el certificado raíz de CA y cualquier otro certificado que forma parte de la cadena de certificados no están ya instalados en el perfil del operador de concentrador, instale ahora los certificados siguiendo este procedimiento:

Nota: No tiene que realizar este paso si el certificado emitido por la CA ya está instalado.

1. Vaya a **Perfil**> **<Hub Operator> usuario**> **certificados** > **Cargar certificado**.
2. En la lista desplegable **¿A qué socio pertenece este certificado?**, seleccione el socio al que se asociará el Certificado recién subido.
3. Pulse **Buscar** para buscar unos socios específicos o un subconjunto de ellos.
4. Pulse **Examinar** al lado de la **Ubicación del almacén de confianza (o) almacén de claves**.
5. Tanto para el Certificado como para el Almacén de claves, escriba la **Contraseña**.
6. Si se trata del almacén de confianza, especifique el **Tipo de almacén de claves** y pulse **Siguiente**.
7. En la página **Seleccionar certificado de entidad de destino para subir** del asistente, seleccione un certificado para subir.

   Nota: Cuando cargue certificados con un almacén de confianza que tenga más de un certificado, **Seleccionar la lista de certificados CA raíces e intermedios para subir** estará rellenado con todos los certificados. También puede cargar varios certificados.
8. Pulse **Finalizar**.

Paso 4: habilitación del cifrado

Acerca de esta tarea

Habilite el cifrado en el nivel de paquete (nivel superior), socio o de conexión (nivel inferior). Su valor puede prevalecer sobre otros valores en el nivel de conexión. El resumen de la conexión le indicará si falta algún atributo necesario.

Por ejemplo, para alterar los atributos de una conexión de socio, pulse **Administración de cuenta > Conexiones > Conexiones de socios** y seleccione los socios. Pulse **Atributos** y edite el atributo (por ejemplo, **AS cifrado**).

Cuando aparece el mensaje `No se ha encontrado ningún certificado de cifrado válido`, no son válidos ni el certificado primario ni el secundario. Puede que los certificados hayan caducado o se hayan revocado. Si los certificados han caducado o se han revocado, también podrá verse el suceso correspondiente (`Certificado caducado o revocado`) en el Visor de sucesos. Tenga en cuenta que estos dos sucesos pueden estar separados por otros sucesos.

Para mostrar el Visor de sucesos, lleve a cabo los siguientes pasos:

1. Pulse **Visores > Visor de sucesos**.
2. Seleccione los criterios de búsqueda adecuados.
3. Pulse **Buscar**.

Consulte la publicación *Guía del administrador de WebSphere Partner Gateway* para obtener más información sobre la utilización del Visor de sucesos.

Utilización de certificados para habilitar la firma digital

Creación de un certificado de firma saliente

El Gestor de documentos utiliza este certificado cuando envía documentos salientes y firmados a los socios. El mismo certificado y clave se utilizan para todos los puertos y protocolos.

Puede haber más de un certificado de firma digital. Uno es el certificado primario, que es el que se utiliza de manera predeterminada. El otro es un certificado secundario, que se utiliza si el certificado primario caduca.

Generación de un certificado autofirmado

Acerca de esta tarea

Si va a utilizar un certificado autofirmado, utilice el siguiente procedimiento.

1. Inicie el programa de utilidad iKeyman.
2. Utilice iKeyman para generar un certificado autofirmado y un par de claves.
3. Utilice iKeyman para extraer a un archivo el certificado que contendrá la clave pública.
4. Distribuya el certificado a los socios. El método preferente de distribución consiste en enviar el certificado por correo electrónico en un archivo comprimido protegido mediante contraseña. Los socios deberán llamarle y solicitarle la contraseña para el archivo comprimido.
5. Utilice la herramienta iKeyman para exportar el par de certificado autofirmado y clave privada con el formato de un archivo PKCS12.

Instalación de un certificado autofirmado saliente

Acerca de esta tarea

1. Vaya a **Perfil** > {**Operador de concentrado/Socio interno**} > **certificados**> **Cargar certificado**.
2. En la página **Seleccionar socio, Ubicación de archivo, Contraseña** del asistente, especifique los siguientes valores:
   - En **A qué socio pertenece este certificado o certificados**, seleccione el socio al que asociará el certificado recién cargado. Pulse **Buscar** para buscar un

socio o subconjunto de socios determinados. Si el socio es un Operador de concentrador o un Socio interno, especifique la ubicación del certificado, la ubicación de la clave privada y la contraseña (OR) Proporcione el almacén de confianza o el almacén de claves con la contraseña. Como Socio externo, especifique la ubicación de certificado (OR) proporciona la ubicación del almacén de confianza que contiene la cadena de certificados.

- **Clave privada:** Pulse **Examinar** para seleccionar la clave privada del certificado.
- **Contraseña:** Si el certificado tiene una contraseña, indique la contraseña.
- **Ubicación del almacén de confianza (o) almacén de claves:** Pulse **Examinar** para seleccionar la Ubicación del almacén de claves. El almacén de claves es un conjunto de claves privadas junto con la raíz de confianza y certificados de CA.
- **Contraseña:** Especifique la contraseña para la ubicación del almacén de claves.
- **Tipo:** seleccione el tipo de almacén de confianza (o) almacén de claves. Los valores disponibles en la lista desplegable son: JKS, JCEKS y PKCS12.

Nota: En WebSphere Partner Gateway, al crear una base de datos de claves (almacén de claves) de tipo CMS con iKeyman, se muestra el siguiente error:

```
No se ha encontrado la biblioteca nativa de java CMS. Asegúrese de que el
 componente SSL que necesita su producto está instalado y la vía de acceso a biblioteca
se ha definido correctamente
```

. Dado que WebSphere Application Server y WebSphere Partner Gateway no utilizan almacenes de claves CMS, utilice el tipo de almacén de claves soportado, JKS (predeterminado), PKCS12 o JCEKS.

3. Pulse **Siguiente** para ir a la página **Detalles del certificado** del asistente. La página **Seleccionar certificados CA y de entidad de destino** se abrirá cuando cargue certificados a través de un almacén de confianza que tenga más de un certificado. Se mostrará la lista de certificados disponibles en el almacén de confianza.
4. En la **Seleccionar certificados CA y de entidad de destino** del asistente, especifique los siguientes valores:
   - **El almacén de claves contiene más de un certificado de entidad final. Seleccione el certificado que desee cargar** - La lista desplegable tiene una lista de todos los certificados de entidad final. Seleccione el certificado que desee cargar
   - **Contraseña** - Si el almacén de claves tiene una contraseña, marque este recuadro de selección y escriba la contraseña en el recuadro de texto.
   - **Seleccione la lista de certificados CA raíz e intermedios que desee subir** - En el recuadro de lista, seleccione los certificados CA raíz e intermedios que se subirán.
5. Pulse **Siguiente** para ir a la página **Detalles de certificado** del asistente.
6. En la página **Detalles de certificado** del asistente, escriba los siguientes detalles del certificado:
   - **Nombre de certificado sin secundarios** - Nombre del certificado sin secundarios. El nombre de campo depende de si el certificado es un certificado sin secundarios, un certificado CA raíz o un certificado CA intermedio.
   - **Descripción**: Descripción del certificado sin secundarios.
   - **Tipo de certificado** - Asocie este certificado al cifrado.

- **Utilización de certificado**: Asocie una utilización al certificado. Los valores son Primario y Secundario.
- **Modalidad de funcionamiento:** especifique la modalidad de funcionamiento.
- **Estado** - Seleccione habilitado o inhabilitado en función de si desea habilitar o inhabilitar un certificado después de la carga. El botón Siguiente sólo se habilita si se habilita el certificado.
- **Gestión de conjuntos**- Puede asociar un certificado a un conjunto existente o crear un conjunto nuevo. Si el certificado es un certificado secundario, sólo se puede asociar a un conjunto existente. Puede asociar el certificado a cualquier conjunto para un socio interno con tipo cifrado o para un socio externo con tipo SSL (autorización de cliente entrante) o Firma (Verificar).

  Nota: Para el operador de concentrador, no habrá gestión de conjuntos. Los certificados se asociarán al conjunto predeterminado que se cree.

7. Pulse **Siguiente** para ir a la página Conjunto del asistente. Si el certificado es primario, no tiene que crear conjuntos y asociar el certificado a un conjunto y una conexión participante. Si ha marcado el recuadro de selección **Crear nuevo conjunto**, se abrirá la página **Crear nuevo conjunto** del asistente. De lo contrario, se abrirá la página **Añadir a existente** del asistente. Si el archivo contiene una clave privada del socio interno o el certificado público del socio externo utilizado para SSL / Firma digital, puede pulsar **Finalizar**.
8. En la página **Crear nuevo conjunto** del asistente, especifique los detalles del nuevo conjunto. Para los certificados primarios, no tiene que crear conjuntos y asociar un certificado a ellos. Especifique los siguientes valores:
   - **Nombre de conjunto** - El nombre del conjunto.
   - **Descripción** - La descripción del conjunto.
   - **Estado**: Seleccione habilitado o inhabilitado. Si está inhabilitado, no se habilitará el botón **Siguiente**.
   - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
9. En la página **Añadir a conjunto existente** del asistente, seleccione los conjuntos que se añadirán al certificado. Especifique los siguientes valores:
   - **Seleccionar de la lista de conjuntos disponibles para el tipo de certificado seleccionado** - En la lista, seleccione uno o varios conjuntos para añadir el certificado.
   - **Establecer valores predeterminados** - Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.
10. En **Crear nuevo conjunto** o **Añadir al conjunto existente**, pulse **Siguiente** para ir a la página **Valores predeterminados** del asistente. El botón **Siguiente** sólo estará habilitado si el estado del conjunto es habilitado.
11. Seleccione **habilitado** o **inhabilitado** en el **Estado** en función de si desea habilitar o inhabilitar el certificado después de subirlo.

    Nota: Si ha marcado el recuadro de selección **Establecer como conjunto predeterminado** en la página anterior (Crear nuevo conjunto o Añadir a conjunto existente), deberá asociar el conjunto a una modalidad de funcionamiento. Se visualizarán las utilizaciones de certificado según las modalidades de operación. El cifrado se inhabilitará para socios internos. Cliente SSL y Firma digital se inhabilitarán para socios externos.
12. Pulse **Siguiente** para ir a la página de Configuración del asistente. En el caso de que pulse **Siguiente** y de que falten algunos certificados CA raíces o

intermedios, se le solicitará que los suba. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** si desea realizar la subida más tarde.

13. En la página Configuración del asistente, especifique los valores siguientes:

    Nota: La página Configuración muestra una lista de utilizaciones de (conjunto de) certificados respecto a las modalidades de operación. El nombre de conjunto actual se lleva previamente para todos, pero puede restablecerlo.

    - **Socio de origen** - Este campo estará rellenado con el valor del socio interno.
    - **Socio de destino** - Esta lista desplegable estará rellenada con la lista de socios externos. También puede seleccionar el valor "Todos" para incluir todos los socios externos.
    - **De paquete** - En la lista desplegable, seleccione el paquete de objetos de definiciones de flujo de documentos del socio interno.
    - **A paquete** - En la lista, seleccione el paquete de objetos de definiciones de flujo de documentos del socio externo.
14. Pulse **Añadir más conexiones** si desea asociar el conjunto a otras conexiones de participantes.
15. Pulse **Añadir certificado secundario** para añadir un certificado secundario al conjunto actual.
16. Pulse **Finalizar** para subir el certificado. En caso de que falten certificados raíz o CA intermedios, se le solicitará que los cargue. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** en la ventana de solicitud si desea realizar la subida más tarde.

Si está subiendo los certificados primario y secundario para la Autenticación de cliente SSL y la firma digital y está subiendo los certificados primarios como dos entradas separadas, asegúrese de que los correspondientes certificados secundarios se suban como dos entradas distintas.

Obtención de un certificado firmado por una CA

Acerca de esta tarea

Si piensa utilizar un certificado firmado por una CA, utilice el siguiente procedimiento:

1. Inicie el programa de utilidad iKeyman.
2. Utilice iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
3. Envíe una Solicitud de firma de certificado (CSR) a la CA.
4. Cuando reciba el certificado firmado de la CA, utilice iKeyman para colocar el certificado firmado en el almacén de claves.
5. Distribuya el certificado CA firmante a todos los socios.

Instalación de un certificado de verificaión de firma digital entrante

Acerca de esta tarea

El Gestor de documentos utiliza el certificado firmado por el socio para verificar la firma del remitente cuando reciba documentos. Los socios le envían sus certificados de firma autofirmados en el formato X.509 DER. A su vez, instale los certificados de los socios mediante la consola de comunidad bajo el perfil del socio correspondiente.

Para instalar el certificado, utilice el procedimiento siguiente.

1. Reciba el certificado de firma X.509 del socio en formato DER.
2. Vaya a **Perfil**> **Socio externo**> **Certificados** > **Cargar certificado**.
3. Pulse **Buscar** para buscar unos socios específicos o un subconjunto de ellos.
4. Pulse **Examinar** al lado de **Ubicación de certificado** para subir el certificado.
5. Pulse **Siguiente** para ir a la página **Detalles del certificado** del asistente.
6. Asocie este certificado a la **Verificación de firma digital**.
7. Seleccione **habilitado** o **inhabilitado** en el **Estado** en función de si desea habilitar o inhabilitar el certificado después de subirlo.
8. Seleccione la **Modalidad de funcionamiento**. Si es un operador de concentrador, no tiene la opción de seleccionar la **Modalidad de funcionamiento**.
9. Pulse **Finalizar** para guardar los cambios y cerrar el asistente.
10. Si una CA firma el certificado y tanto el certificado raíz de CA como cualquier otro certificado que forme parte de la cadena de certificados no están instalados ya en el perfil de Operador de concentrador, instale los certificados ahora. Esto sólo es aplicable al almacén de confianza o al almacén de claves.
    a. Pulse **Administración de concentrador > Perfil de socio de concentrador > Certificados** para visualizar la página Lista de certificados.

       Asegúrese de que ha iniciado la sesión en la Consola de comunidad como operador de concentrador e instale el certificado en su propio perfil.
    b. Pulse **Cargar certificado**.
    c. Seleccione **Raíz e intermedio**.
    d. Escriba una descripción del certificado (que es necesario).
    e. Cambie el estado por **Habilitado**.
    f. Pulse **Examinar** y vaya al directorio en el que se ha guardado el certificado.
    g. Seleccione el certificado y pulse **Abrir**.
    h. Pulse **Subir** y, a continuación, **Guardar**.

    Nota: si el certificado de la CA ya está instalado, no es necesario que realice el paso anterior.
11. Habilite la firma en el nivel de paquete (nivel superior), socio o de conexión (nivel inferior). Su valor puede prevalecer sobre otros valores en el nivel de conexión. El resumen de la conexión le indicará si falta algún atributo necesario.

    Por ejemplo, para alterar los atributos de una conexión de socio, pulse **Administración de cuenta > Conexiones** y seleccione los socios. Pulse **Atributos** y edite el atributo (por ejemplo, **AS firmado**).

Utilización de certificados para habilitar SSL

En los apartados siguientes se describe cómo crear e instalar certificados SSL para utilizarlos con WebSphere Partner Gateway. También se incluye una visión general de reconocimiento SSL. Si la comunidad no está utilizando SSL, ni usted ni el socio necesitan un certificado SSL entrante o saliente.

Reconocimiento SSL

Acerca de esta tarea

Cada sesión SSL empieza con reconocimiento.

Cuando un cliente (el socio o socio interno) inicia un intercambio de mensajes, se producen los siguientes pasos:

1. El cliente envía un mensaje "hola" de cliente que lista las posibilidades criptográficas del cliente (clasificadas por orden de preferencia del cliente), como la versión de SSL, los juegos de cifrado admitidos por el cliente y los métodos de compresión de datos admitidos por el cliente. El mensaje también contiene un número aleatorio de 28 bytes.
2. El servidor responde con un mensaje "hello done" de servidor que contiene el método criptográfico (juego de cifrado) y el método de compresión de datos seleccionado por el servidor, el ID de sesión y otro número aleatorio.

   Nota: el cliente y el servidor deben dar soporte a cómo mínimo un juego de cifrado común, si no el reconocimiento falla. El servidor en general elige el juego de cifrado común más sólido.
3. El servidor envía su certificado digital.

   La autenticación de servidor se realiza en este paso.
4. El servidor envía un mensaje de "solicitud de certificado digital". En el mensaje de "solicitud de certificado digital", el servidor envía una lista de tipos de certificados digitales soportados y los nombres distinguidos de autoridades certificadoras que se pueden aceptar.
5. El servidor envía un mensaje "hello done" de servidor y espera a recibir una respuesta del cliente.
6. Cuando se recibe el mensaje "hello done" del servidor, el cliente verifica la validez del certificado digital del servidor y comprueba que los parámetros "hello" del servidor sean aceptables.
7. Si el servidor ha solicitado un certificado digital de cliente, el cliente envía un certificado digital o, si no hay disponible ningún certificado digital apropiado el cliente envía una alerta "no hay ningún certificado digital". Esta alerta sólo es un aviso, pero la aplicación del servidor puede terminar la sesión si la Autenticación de cliente es obligatoria.
8. El cliente envía un mensaje de "intercambio de claves de cliente". Este mensaje consta del secreto de preparación de copia maestra, un número aleatorio de 46 bytes que se utiliza en la generación de claves de cifrado simétrico y las claves de código de autenticación de mensajes (MAC), cifrado con la clave pública del servidor.
9. Si el cliente ha enviado un certificado digital al servidor, el cliente envía un mensaje de "verificación de certificado digital" firmado con la clave privada del cliente. Si verifica la firma de este mensaje, el servidor puede verificar de forma explícita la propiedad del certificado digital del cliente.

   Nota: no es necesario ningún proceso adicional para verificar el certificado digital del servidor. Si el servidor no tiene la clave privada que pertenece al certificado digital, no podrá descifrar el secreto de preparación de copia maestra ni crear las claves correctas para el algoritmo de cifrado simétrico y el reconocimiento fallará.
10. El cliente utiliza una serie de operaciones criptográficas para convertir el secreto de preparación de copia maestra en un secreto maestro, del que se deriva todo el material clave necesario para el cifrado y la autenticación de mensajes. A continuación, el cliente envía un mensaje de "cambio de especificación de cifrado" para que el servidor pase a utilizar el juego de cifrado recién negociado. El mensaje siguiente enviado por el cliente (el mensaje "terminado") es el primer mensaje cifrado con este método y estas claves.

11. El servidor responde con un mensaje de "cambio de especificación de cifrado" y un mensaje de "terminado" propio.

La Autenticación de cliente requiere efectuar los pasos 4 en la página 273, 7 en la página 273 y 9 en la página 273.

El reconocimiento SSL finaliza y los datos de aplicación cifrados pueden enviarse.

Configuración de los certificados SSL entrantes

Este apartado describe cómo configurar la autenticación de servidor y la Autenticación de cliente para solicitudes de conexión entrantes de socios.

Una solicitud de socio es cuando el socio está enviando un documento a WebSphere Partner Gateway. Si su comunidad no utiliza SSL, no necesita un certificado SSL entrante o saliente.

Nota: para FTPS entrante WebSphere Partner Gateway utiliza un servidor FTP proporcionado por el cliente, por lo que cualquier configuración SSL entrante es para ese producto de servidor FTP que el cliente está utilizando.

Paso 1: obtención de un certificado SSL

Acerca de esta tarea

WebSphere Application Server utiliza el certificado SSL cuando recibe solicitudes de conexión de los socios a través de SSL. Es el certificado que el receptor presenta para identificar al concentrador ante el socio. Este certificado de servidor puede ser autofirmado o puede estar firmado por una CA. En la mayoría de los casos, se utilizará un certificado CA para mayor seguridad. Quizás podría utilizarse un certificado autofirmado en un entorno de prueba. Utilice iKeyman o la consola administrativa de WebSphere Application Server para generar una pareja de certificado y clave. Consulte la documentación disponible de IBM para obtener más información sobre la utilización de iKeyman o de la consola administrativa de WebSphere Application Server.

Después de generar el par de certificado y clave, utilice el certificado para el tráfico SSL entrante para todos los socios. Si posee múltiples receptores o consolas, copie el almacén de claves resultante en cada instancia. Si se genera el certificado utilizando la consola administrativa de WebSphere Application Server, la clave y el certificado pueden importarse en otro almacén de claves de otro servidor utilizando la consola administrativa de WebSphere Application Server. Si el certificado es autofirmado, proporcione este certificado a los socios. Para obtener este certificado, utilice iKeyman para extraer el certificado público en un archivo.

Generación de un certificado autofirmado: Si se dispone a utilizar certificados de servidor autofirmados, utilice el procedimiento siguiente.

1. Inicie el programa de utilidad iKeyman, que se encuentra en /<*Dir_instalación_WAS*>/bin. Si es la primera vez que utiliza iKeyman, suprima el certificado “ficticio” que reside en el almacén de claves.
2. Utilice iKeyman para abrir el Receptor o el Almacén de claves de la consola, y para generar un certificado autofirmado y una pareja de claves para el Almacén de claves de la consola o el Receptor.
3. Utilice iKeyman para extraer a un archivo el certificado que contendrá la clave pública.

   Guarde el almacén de claves en un archivo JKS, PKCS12 o JCEKS.

4. Distribuya el certificado a los socios. El método preferente de distribución consiste en enviar el certificado por correo electrónico en un archivo comprimido protegido mediante contraseña. Los socios deberán llamarle y solicitarle la contraseña para el archivo comprimido.
5. Mediante la consola administrativa de WebSphere Application Server, establezca el nuevo certificado en la configuración SSL y en los parámetros del receptor y de la consola. Puede hacerlo seleccionando el alias del nuevo certificado en el almacén de claves de la configuración de cada nodo o servidor.

Obtención de un certificado generado por CA: Si piensa utilizar un certificado firmado por una CA, utilice el siguiente procedimiento.

1. Inicie el programa de utilidad iKeyman, que se encuentra en el directorio */<Dir_instalación_WAS>*/bin.
2. Utilice iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
3. Envíe una Solicitud de firma de certificado (CSR) a la CA.
4. Cuando reciba el certificado firmado de la CA, utilice iKeyman para colocar el certificado firmado en el almacén de claves.
5. Distribuya el certificado CA a todos los socios si es necesario.
6. Mediante la consola administrativa de WebSphere Application Server, establezca el nuevo certificado en la configuración SSL y en los parámetros del receptor y de la consola. Puede hacerlo seleccionando el alias del nuevo certificado en el almacén de claves de la configuración de cada nodo o servidor.

   Nota: La consola administrativa de WebSphere Application Server también puede utilizarse para completar los pasos anteriores.

Paso 2: autenticación de clientes
Acerca de esta tarea

Si desea autenticar socios que envíen documentos, lleve a cabo los pasos descritos en este apartado.

Instalación del certificado de cliente:
Acerca de esta tarea

Para la autenticación del cliente, emplee el procedimiento siguiente:

1. Obtenga el certificado del socio.
2. Si el certificado es autofirmado, instálelo en el almacén de confianza utilizando el programa iKeyman o la consola administrativa de WebSphere Application Server.
3. Si la CA ha emitido el certificado, añada los certificados CA relacionados en el almacén de confianza utilizando el programa iKeyman o la consola administrativa de WebSphere Application Server.

Nota: Cuando añada más socios a la comunidad del concentrador, puede utilizar iKeyman o la consola administrativa de WebSphere Application Server para añadir los certificados al almacén de confianza. Si un socio deja la comunidad, puede utilizar iKeyman o la consola administrativa de WebSphere Application Server para eliminar los certificados del socio del almacén de confianza.

Configuración de autenticación de cliente:

Acerca de esta tarea

Después de instalar el certificado o los certificados, configure WebSphere Application Server de forma que emplee la Autenticación de cliente ejecutando el script del programa de utilidad bcgClientAuth.jacl.

1. Acceda al directorio siguiente: <*ProductDir*>/bin
2. Para activar la Autenticación de cliente, invoque el script del siguiente modo:

   ```
   ./bcgwsadmin.sh -f /<DirProducto>/scripts/bcgClientAuth.jacl
      -conntype NONE set
   ```

   Nota: para desactivar la autenticación del cliente, invoque el script del siguiente modo:

   ```
   ./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/bcgClientAuth.jacl
     -conntype NONE clear
   ```

Debe reiniciar el servidor bcgreceiver para que estos cambios entren en vigor. La Autenticación de cliente también se puede habilitar utilizando la consola administrativa de WebSphere Application Server. Un valor "Soportado" significa que el servidor solicitará el certificado de cliente pero, si éste no está disponible, el reconocimiento de SSL aún puede establecerse. Un valor de "Necesario" significa que el certificado de cliente debe enviarse. De lo contrario, el reconocimiento SSL fallará.

Validación del certificado del cliente:
Acerca de esta tarea

Existe una función adicional que puede utilizarse con la autenticación SSL de cliente. Esta función se habilita a través de la Consola de comunidad. Para HTTPS, WebSphere Partner Gateway verifica los certificados frente a los ID de empresa en los documentos de entrada. Para utilizar esta característica, cree el perfil del socio, importe el certificado del cliente y márquelo como SSL.

1. Importe el certificado de cliente.
   a. Pulse **Administración de cuentas > Perfiles > socio** y busque el perfil del socio.
   b. Pulse **Certificados**.
   c. Pulse **Cargar certificado**.
   d. Pulse **Examinar** y vaya al directorio en el que se ha guardado el certificado.
   e. Seleccione **Cliente SSL** como tipo de certificado.
   f. Escriba una descripción del certificado (que es necesario).
   g. Cambie el estado por **Habilitado**.
   h. Si desea seleccionar una modalidad de operación distinta de **Producción** (el valor predeterminado), selecciónelo de la lista.
   i. Pulse **Finalizar**.
2. Actualice el destino del cliente.
   a. Pulse **Administración de cuentas > Perfiles > socio** y busque el perfil del socio.
   b. Pulse **Destinos**.
   c. Seleccione el destino HTTPS que ha creado anteriormente. Si aún no ha creado el destino HTTPS, consulte “Configuración de un destino HTTPS” en la página 228.
   d. Pulse el icono **Editar** para editar el destino.
   e. Seleccione **Sí** para **Validar certificado de cliente SSL**.

f. Pulse **Guardar**.

Configuración de un almacén de claves y un almacén de confianza distintos para el receptor y la consola

De forma predeterminada, WebSphere Partner Gateway utiliza un almacén de claves y un almacén de confianza para el receptor y la consola. Sin embargo, puede configurar un almacén de claves y un almacén de confianza separados para receptor y consola en la instalación de modalidad distribuida.

Para configurar el almacén de claves y el almacén de confianza, cree y establezca un almacén de claves y un almacén de confianza separados para receptor y consola. Además, cree configuraciones de SSL por separado. Las configuraciones de SSL pueden establecerse en el nivel de clúster o de servidor. Es más sencillo establecer la configuración de SSL en el nivel de clúster, ya que la configuración es aplicable a todos los servidores de ese clúster, y no necesita configurar cada servidor por separado.

Establecimiento de la configuración SSL en el nivel clúster: Mientras se establece la configuración de SSL con un nuevo almacén de claves y un almacén de confianza en el nivel de clúster, no debe establecerse ninguna configuración de SSL en el nivel de servidor. Si se ha establecido una configuración de SSL en el nivel de servidor, no se utilizará la configuración de SSL en el nivel de clúster, sino que se utilizará el establecido para el servidor.

Siga estos pasos para establecer la configuración de SSL para bcgconsoleCluster:

1. Cree un almacén de claves para el clúster de consola. El almacén de claves debe crearse en el ámbito del clúster bcgconsole navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.
2. Cree un almacén de confianza para el clúster de consola. El almacén de confianza debe crearse en el ámbito del clúster bcgconsole navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.
3. Cree una configuración de SSL para el clúster de consola en el ámbito de clúster de consola navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Configuraciones de SSL**. Establezca el almacén de claves y el almacén de confianza que se crearon en los pasos anteriores. Actualice los alias de certificado en la lista de alias de certificado pulsando **Obtener alias de certificado** y seleccione los alias necesarios a utilizar para la autenticación del servidor. Establezca el gestor de confianza en **IbmPKIX**.
4. Establezca esta configuración de SSL en bcgconsoleCluster alterando temporalmente la configuración de SSL heredada. Actualice los alias de certificado pulsando **Actualizar los alias de certificado** y establezca los alias a utilizar para la autenticación del servidor.
5. Reinicie bcgconsoleCluster.

Siga estos pasos para establecer la configuración de SSL para bcgreceiverCluster:

1. Cree un almacén de claves para el clúster de receptor. El almacén de claves debe crearse en el ámbito del clúster bcgreceiver navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.
2. Cree un almacén de confianza para el clúster de receptor. El almacén de confianza debe crearse en el ámbito del clúster bcgconsole navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Almacenes de claves y certificados**.

3. Cree una configuración de SSL para el clúster de receptor en el ámbito de clúster de receptor navegando hasta **Seguridad > Certificado de SSL y gestión de claves > Configuraciones de SSL**, y establezca el almacén de claves y el almacén de confianza que se crearon en los pasos anteriores. Obtenga los alias de certificado pulsando **Obtener alias de certificado** y seleccione el alias necesario a utilizar para la autenticación del servidor. Establezca el gestor de confianza en **IbmPKIX**.
4. Establezca esta configuración de SSL en bcgreceiverCluster alterando temporalmente la configuración de SSL heredada. Actualice los alias de certificado pulsando **Actualizar los alias de certificado** y establezca los alias a utilizar para la autenticación del servidor.
5. Reinicie bcgreceiverCluster.

Para obtener más información acerca de cómo trabajar con almacenes de claves, almacenes de confianza, configuración SSL y configuraciones de punto final, consulte la sección *Securing applications and their environment of WebSphere Application Server Documentation.*

Establecimiento de NodeDefaultTrustStore en NodeDefaultSSLSetting en modalidad distribuida: Este valor debe establecerse para la modalidad simple distribuida. Sin embargo, esto también es aplicable para la modalidad completamente distribuida si deben utilizarse un almacén de claves y un almacén de confianza comunes para el receptor y la consola. Si se federa un nodo en una célula, los certificados de firmante de nodo se añaden a CellDefaultTrustStore. De forma predeterminada, NodeDefaultSSLSetting hace referencia a CellDefaultTrustStore como almacén de confianza. Para el receptor y la consola de WebSphere Partner Gateway, puede que no sea deseable utilizar certificados de firmantes de otros nodos. Para utilizar un almacén de confianza dedicado para los nodos en que está instalado WebSphere Partner Gateway, NodeDefaultTrustStore puede establecerse en NodeDefaultSSLSettings como almacén de confianza.

Los pasos para realizar este cambio son:

1. En la consola administrativa de WebSphere Application Server, vaya a **Seguridad > Certificado de SSL y gestión de claves > Gestionar configuraciones de seguridad > <node_name> > SSL configurations > NodeDefaultSSLSettings**.
2. En el campo Nombre de almacén de confianza, seleccione **NodeDefaultTrustStore**.

   Nota: Asegúrese de que NodeDefaultTrustStore se configura para el almacén de confianza que desea utilizar; por ejemplo, bcgSecurityTrust.jks.
3. Pulse **Aplicar**.
4. En la página siguiente de la consola, pulse **Guardar** para actualizar los cambios en la configuración maestra.
5. Reinicie los servidores en ese nodo.

Nota: Para la modalidad completamente distribuida, los cambios antedichos deben realizarse para todos los nodos que contengan los servidores bcgreceiver y bcgconsole. Para la modalidad simple distribuida, estos cambios deben realizarse para todos los nodos que contengan bcgserver.

Adición de Certificados de firmante en trust.p12 si NodeDefaultTrustStore está establecido para el nodo que contiene los servidores de WebSphere Partner

Gateway: Actualmente, NodeDefaultTrustStore hace referencia a trust.p12. Si NodeDefaultTrustStore se establece para el nodo que contiene servidores de WebSphere Partner Gateway, no se utilizará bcgSecurityTrust.jks. Los certificados de firmante de bcgSecurityTrust.jks tiene que añadirse a trust.p12 como sea necesario.

Configuración de certificados SSL salientes

Una solicitud saliente es cuando WebSphere Partner Gateway está enviando un documento a un socio. Si la comunidad no está utilizando SSL, no necesita un certificado SSL entrante o saliente.

Paso 1: autenticación del servidor

Acerca de esta tarea

Cuando se utiliza SSL para enviar documentos salientes a los socios, WebSphere Partner Gateway solicita un certificado de servidor de los socios. El mismo certificado CA puede ser utilizado para varios socios. El certificado debe estar en formato X.509 DER.

Nota: puede convertir el formato con el programa de utilidad iKeyman. Para utilizar iKeyman para convertir el formato, siga estos pasos:

1. Inicie iKeyman.
2. Cree un nuevo almacén de claves vacío o abra un almacén de claves existente.
3. En Contenido de base de datos de claves, seleccione **Certificados de firmante**.
4. Añada el certificado de ARM utilizando la opción **Añadir**.
5. Extraiga el mismo certificado como datos DER binarios mediante la opción **Extraer**.
6. Cierre iKeyman.

Instale el certificado autofirmado del socio en el perfil de Operador de concentrador. Si el certificado estaba firmado por una CA y el certificado raíz de la CA y todos los demás certificados que forman parte de la cadena de certificados todavía no están instalados en el perfil del operador de concentrador, instale los certificados en el perfil del operador de concentrador.

1. Pulse **Administración de cuentas > Perfiles > Certificados** para visualizar la página Lista de certificados.

   Asegúrese de que ha iniciado la sesión en la consola de comunidad como operador de concentrador o socio interno.
2. Pulse **Cargar PKCS12**.

   Nota: El archivo PKCS12 que se sube sólo debe contener una clave privada y el certificado asociado. También puede cargar el certificado y la clave privada formateada con PKCS#8 por separado.
3. Seleccione **Cliente SSL** como tipo de certificado.
4. Escriba una descripción del certificado (que es necesario).
5. Cambie el estado por **Habilitado**.
6. Pulse **Examinar** y vaya al directorio en el que se ha guardado el certificado.
7. Seleccione el certificado y pulse **Abrir**.
8. Escriba la contraseña.
9. Si desea seleccionar una modalidad de operación distinta de **Producción** (el valor predeterminado), selecciónelo de la lista.

10. Si dispone de dos certificados SSL, indique si éste es el certificado primario o secundario seleccionando **Primario** o **Secundario** en la lista **Utilización de certificado**.
11. Pulse **Subir** y, a continuación, **Guardar**.

Nota: si el certificado de la CA ya está instalado, no es necesario que realice los pasos anteriores.

Paso 2: autenticación de clientes

Acerca de esta tarea

Si se requiere la Autenticación de cliente SSL, el socio, por su parte, solicitará un certificado del concentrador. Utilice la Consola de comunidad para importar su certificado a WebSphere Partner Gateway. Puede generar el certificado mediante iKeyman. Si el certificado es un certificado autofirmado, deberá proporcionarse al socio. Si es un certificado firmado por una CA, el certificado raíz de la CA deberá ser proporcionado a los socios, para que puedan añadirlo a sus certificados de confianza.

Puede haber más de un certificado SSL. Uno es el certificado primario, que es el que se utiliza de manera predeterminada. El otro es un certificado secundario, que se utiliza si el certificado primario caduca.

Utilización de un certificado autofirmado:
Acerca de esta tarea

Si va a utilizar un certificado autofirmado, utilice el siguiente procedimiento.

1. Inicie el programa de utilidad iKeyman.
2. Utilice iKeyman para generar un certificado autofirmado y un par de claves.
3. Utilice iKeyman para extraer a un archivo el certificado que contendrá la clave pública.
4. Distribuya el certificado a los socios. El método preferente de distribución consiste en enviar el certificado por correo electrónico en un archivo comprimido protegido mediante contraseña. Los socios deberán llamarle y solicitarle la contraseña para el archivo comprimido.
5. Utilice la herramienta iKeyman para exportar el par de certificado autofirmado y clave privada con el formato de un archivo PKCS12.
6. Instale el certificado autofirmado y la clave mediante la Consola de comunidad.
   a. Pulse **Administración de cuentas > Perfiles > Certificados** para visualizar la página Lista de certificados.

      Asegúrese de que ha iniciado la sesión en la Consola de comunidad como operador de concentrador.
   b. Pulse **Cargar PKCS12**.

      Nota: El archivo PKCS12 que se sube sólo debe contener una clave privada y el certificado asociado. También puede cargar el certificado y la clave privada formateada con PKCS#8 por separado.
   c. Seleccione **Cliente SSL** como tipo de certificado.
   d. Escriba una descripción del certificado (que es necesario).
   e. Cambie el estado por **Habilitado**.
   f. Pulse **Examinar** y vaya al directorio en el que se ha guardado el certificado.
   g. Seleccione el certificado y pulse **Abrir**.

h. Escriba la contraseña.
i. Si desea seleccionar una modalidad de operación distinta de **Producción** (el valor predeterminado), selecciónelo de la lista.
j. Si dispone de dos certificados SSL, indique si éste es el certificado primario o secundario seleccionando **Primario** o **Secundario** en la lista **Utilización de certificado**.
k. Pulse **Subir** y, a continuación, **Guardar**.

Si está subiendo los certificados primario y secundario para la Autenticación de cliente SSL y la firma digital y está subiendo los certificados primarios como dos entradas separadas, asegúrese de que los correspondientes certificados secundarios se suban como dos entradas distintas.

Utilización de un certificado firmado por una CA:
Acerca de esta tarea

Si piensa utilizar un certificado firmado por una CA, utilice el siguiente procedimiento:

1. Utilice iKeyman para generar una solicitud de certificado y un par de claves para el receptor.
2. Envíe una Solicitud de firma de certificado (CSR) a la CA.
3. Cuando reciba el certificado firmado de la CA, utilice iKeyman para colocar el certificado firmado en el almacén de claves.
4. Distribuya el certificado CA firmante a todos los socios.

Adición de CRL (Lista de revocación de certificados)

WebSphere Partner Gateway incluye una característica de Lista de revocación de certificados (CRL). La CRL, emitida por una autoridad de certificación (CA), identifica los socios que hayan revocado certificados antes de su fecha de caducidad planificada. A los socios con certificados revocados se les denegará el acceso a WebSphere Partner Gateway.

En la CRL, los certificados revocados se identifican mediante el número de serie del certificado. El Gestor de documentos explora la CRL cada 60 segundos y rechaza un certificado si está contenido en la lista CRL. No obstante, puede configurar el intervalo de tiempo en el que el directorio CRL se explora. El intervalo de tiempo se especifica para la propiedad de configuración bcg.rosettanet.encrypt.CertDbRefreshInterval.

De forma predeterminada, las CRL se guardan en la siguiente ubicación: /<*directorio_datos_compartidos*>/security/crl. WebSphere Partner Gateway utiliza el valor bcg.CRLDir en Consola > Administración del sistema > Administración del gestor de documentos > Seguridad para identificar la ubicación del directorio CRL.

Coloque los CRL en el directorio CRL.

Configuración de CRLDP

Acerca de esta tarea

Configurar el CRLDP cambiando la configuración de Java Virtual Machine, es decir, establecer el valor de -Dcom.ibm.security.enableCRLDP = Verdadero.

En la modalidad distribuida completa, esta configuración se debe realizar para bcgdocmgr, bcgreceiver y bcgconsole. En el caso de la modalidad distribuida simple y la modalidad simple, lleve a cabo esta configuración para bcgserver.

Los pasos para realizarlo son los siguientes:

1. Inicie la sesión en la consola administrativa de WebSphere Application Server.
2. Vaya a **Servidores > Servidores de aplicación** y seleccione **Servidor**.
3. Consulte la propiedad mediante el proceso siguiente:
   a. Seleccione el servidor (bcgdocmgr, bcgreceiver o bcgconsole).
   b. En la página de **Configuración** , expanda **Java y Gestión de procesos** en el apartado **Infraestructura del servidor** de la página y seleccione **Definición del proceso**.
   c. En la página **Configuración de la definición del proceso**, seleccione **Java Virtual Machine** en el apartado **Propiedades adicionales**.
   d. Añada lo siguiente al valor existente (si existe) en el campo de argumentos JVM genéricos: -Dcom.ibm.security.enableCRLDP=true.
4. Pulse **Aplicar** y a continuación Guardar para completar esta configuración.
5. Reinicie el servidor.
6. Establezca esta propiedad en todos los servidores del clúster.

Configuración de SSL entrante para la Consola de comunidad y el componente Receptor

Los almacenes de claves de WebSphere Partner Gateway están configurados previamente en WebSphere Application Server. Este apartado sólo es válido si se están utilizando diferentes almacenes de claves.

Para configurar SSL para la Consola de comunidad y componente Receptor en WebSphere Partner Gateway, utilice el siguiente procedimiento.

1. Obtenga la siguiente información:
   - Los nombres completos de vía de acceso del archivo de claves y el archivo de confianza; por ejemplo, para el Receptor: *<DirProducto>*/common/security/keystore/bcgSecurity.jks y *<DirProducto>*/common/security/skeystore/bcgSecurityTrust.jks

     Debe especificar estos nombres correctamente. En el entorno UNIX, estos nombres son sensibles a las mayúsculas y minúsculas.
   - Las nuevas contraseñas para cada archivo.
   - El formato de cada archivo. Se debe seleccionar uno de los valores siguientes: JKS, JCEKS o PKCS12. Especifique este valor en mayúsculas exactamente como se indica.
   - La vía de acceso al archivo de script con el nombre bcgssl.jacl.
2. Abra una ventana de la Consola de comunidad y vaya a */<DirProducto>*/bin. No es necesario que el servidor esté en ejecución para cambiar las contraseñas.
3. Especifique el mandato siguiente, sustituyendo los valores que se incluyen entre <>. Deben especificarse todos los valores.

```
./bcgwsadmin.sh -f /<DirProducto>/
scripts/bcgssl.jacl -conntype NONE install
<archivoClaves_nombrevíaacceso>
<contraseña_archivoClaves> <formato_archivoClaves> <nombrevíaacceso_archivoClaves>
<archivodeConfianza_contraseña> <archivodeConfianza_formato>
```

4. Inicie el servidor. Si el servidor no arranca, podría ser debido a un error durante la ejecución de bcgssl.jacl. Si comete un error, puede volver a ejecutar el script para corregirlo.
5. Si utilizó bcgClientAuth.jacl para establecer la propiedad SSL de clientAuthentication, restáurela después de utilizar bcgssl.jacl. Esto se debe a que bcgssl.jacl sobrescribe todos los valores que pueden haberse establecido para la Autenticación de cliente con el valor false.

Nota:

1. repita estos pasos para la consola, sustituyendo **consola** por **receptor** en el nombre de la vía de acceso.
2. La configuración de SSL, del almacén de claves y del almacén de confianza también puede realizarse utilizando la consola administrativa de WebSphere Application Server.

De manera predeterminada, WebSphere Partner Gateway da soporte a un almacén de clave y un almacén de confianza para el receptor y la consola. No obstante, puede utilizar un almacén de claves y un almacén de confianza distintos para el receptor y la consola en Modalidad distribuida completa. Para utilizar un almacén de claves y un almacén de confianza independientes, realice la siguiente configuración utilizando la Consola administrativa de WAS del Receptor:

1. Cree un almacén de claves para el almacén de claves del receptor. Consulte el apartado sobre cómo crear una configuración de almacén de claves en la documentación de WAS.
2. Cree un almacén de confianza para el almacén de confianza del receptor. Consulte el apartado <*Creating a keystore configuration* del documento de WAS <*Securing applications and their environment*.
3. Cree una configuración SSL para el receptor y establezca el almacén de claves y el almacén de confianza anteriores en dicha configuración. Seleccione el alias necesario que se utilizarán para la autenticación de servidor en el almacén de claves. Establezca el gestor de confianza en **IbmPKIX**. Consulte el apartado *Creating a Secure Socket Layer configuration* del documento de WAS *Securing applications and their environment.*
4. Establezca esta configuración SSL en cada servidor de bcgreceiver sobrescribiendo la configuración SSL heredada. Establezca el alias que se utilizará para la autenticación del servidor.
5. Reinicie todos los servidores de bcgreceiver.

Los pasos son parecidos para la configuración de la consola. Consulte los apartados adecuados del documento de WAS *Securing applications and their environment.*

1. Cree un almacén de claves para el almacén de claves de la consola.
2. Cree un almacén de confianza para el almacén de confianza de la consola.
3. Cree una configuración SSL para la consola y establezca el almacén de claves y el almacén de confianza anteriores en dicha configuración. Seleccione el alias necesario que se utilizarán para la autenticación de servidor en el almacén de claves. Establezca el gestor de confianza en **IbmPKIX**.
4. Establezca esta configuración SSL en cada servidor de bcgconsole sobrescribiendo la configuración SSL heredada. Establezca el alias que se utilizará para la autenticación del servidor.
5. Reinicie todos los servidores de bcgconsole.

Para obtener más información sobre cómo trabajar con almacenes de claves, almacenes de confianza, configuración SSL y configuraciones de punto final, consulte el documento de WAS *Securing applications and their environment*.

Nota: Actualmente, NodeDefaultTrustStore hace referencia a trust.p12. Si NodeDefaultTrustStore se establece para el nodo bcg, bcgSecurityTrust.jks no se utilizará. Debe añadir los certificados de firmante necesarios de bcgSecurityTrust.jks a trust.p12.

Cómo subir certificados con el asistente

Acerca de esta tarea

Como operador de concentrador, puede subir certificados para socios internos o externos:

- Subir claves privadas y certificados para socios internos.
- Subir certificados públicos para socios externos.
- Subir certificados raíces e intermedios.

  Importante: Esta funcionalidad sólo está disponible para certificados X.509.
- Subir una cadena de certificados desde un almacén de confianza.

  Importante: Esta funcionalidad sólo está disponible para certificados X.509.

Certifique un asistente de subida para subir certificados. Con el certificado, puede definir el uso del certificado (Firma / verificación / Cifrado / descifrado /cliente SSL / servidor FTPS /servidor SFTP), asociarlo con una o varias modalidades de funcionamiento, añadirlo a un conjunto (ya sea uno existente o uno nuevo), seleccionar el certificado para que sea el predeterminado para todas las conexiones de participantes o seleccionar una conexión determinada en la que se utilice este conjunto de certificados. La opción de asociar el certificado a la conexión no aparecerá si el certificado no está asociado a un conjunto. Cuando suba el certificado, asegúrese de que el certificado no haya caducado.

En OpenPGP, también se puede utilizar un paquete de clave pública para subir la clave pública y el certificado de un socio externo. El socio externo puede exportar la clave del conjunto de claves, almacenarla en un archivo y enviarla al operador de concentrador. El operador de concentrador puede subir el certificado recibido del socio externo. El archivo de clave pública puede estar en formato binario o blindaje ASCII.

Pasos para subir certificados para socios (internos o externos) con el asistente:

1. Seleccione el socio y pulse **Administración de cuentas** > **Perfil** > **Certificados**.
2. Pulse **Cargar certificado**.
3. En la página **Seleccionar socio, Ubicación de archivo, Contraseña** del asistente, especifique los siguientes valores:
   - En **A qué socio pertenece este certificado o certificados**, seleccione el socio al que asociará el certificado recién cargado. Pulse **Buscar** para buscar un socio o subconjunto de socios determinados. Si el socio es un Operador de concentrador o un Socio interno, especifique la ubicación del certificado, la ubicación de la clave privada y la contraseña (O) Proporcione el almacén de confianza o el almacén de claves con la contraseña. Como Socio externo, especifique la ubicación de certificado (O) proporcione la ubicación del almacén de confianza que contiene la cadena de certificados.

Nota: Si pulsa **Cargar certificado** sin seleccionar un perfil de socio, no aparece el campo **A qué socio pertenece este certificado o certificados**. El certificado se sube para el perfil de socio seleccionado automaticamente.

- **¿Es un certificado raíz e intermedio?**: Marque este recuadro de selección si se trata de un certificado raíz e intermedio.

  Nota: El tipo de certificado Raíz e intermedio sólo es aplicable al perfil de administrador de concentrador, de modo que el recuadro de selección de Certificado raíz e intermedio sólo es visible cuando el socio seleccionado es el administrador de concentrador. Asimismo, para los perfiles de administrador de concentrador, el recuadro de selección de Certificado raíz e intermedio sólo está disponible si se selecciona Cargar certificado.
- **Ubicación de certificado**: Pulse **Examinar** para seleccionar la ubicación de certificado (pública/privada).
- **Clave privada:** Pulse **Examinar** para seleccionar la clave privada del certificado.

  Nota: Esto sólo es aplicable para un socio interno.
- **Contraseña:** Si el certificado tiene una contraseña, indique la contraseña.
- **Ubicación de almacén de confianza (o) Ubicación de almacén de claves o Ubicación de conjunto de claves:** Pulse **Examinar** para seleccionar el Almacén de confianza (o) la Ubicación del almacén de claves o la ubicación del conjunto de claves. El almacén de confianza es un archivo que contiene un conjunto de certificados raíz y de CA fiables. El almacén de claves es un conjunto de claves privadas junto con la raíz de confianza y certificados de CA. El conjunto de claves es una colección de certificados en formato OpenPGP. Pulse **Examinar** para seleccionar el archivo en el diálogo Archivo desde la vía de acceso del archivo de conjunto de claves/almacén de claves/almacén de confianza, o escriba la vía de acceso en el campo de texto. Si sube un certificado para un socio interno de tipo conjunto de claves de OpenPGP, indique la vía de acceso del archivo de conjunto de claves secreto. Para un socio externo, indique la vía de acceso del archivo de conjunto de claves público.
- **Contraseña:** Si la Ubicación del almacén de confianza (o) almacén de claves tiene contraseña, especifique el valor. En el caso de conjunto de claves, no se necesita la contraseña.
- **Tipo:** Seleccione el tipo de Almacén de confianza (o) Almacén de claves o ubicación de conjunto de claves. Los valores disponibles en la lista son: JKS, JCEKS, PKCS12 y OpenPGP.

4. Pulse **Siguiente**.
5. La página **Certificados CA y de entidad de destino** se abrirá cuando cargue certificados a través de un almacén de confianza que tenga más de un certificado. Se mostrará la lista de certificados disponibles en el almacén de confianza. La página **Seleccione las Certificaciones/Claves OpenPGP a cargar** se muestra al seleccionar un conjunto de claves de tipo OpenPGP en la página **Seleccionar socio, Ubicación de archivo, Contraseña** del asistente.
   - Seleccione un certificado en la página **Certificado de entidad de destino para subir** del asistente. Si el almacén de claves tiene varias claves privadas, junto con la clave privada debe especificar la contraseña para la clave si es distinta. En la página **Certificados CA y de entidad de destino** del asistente, especifique los siguientes valores:

- **El almacén de claves contiene más de un certificado de entidad final. Seleccione el certificado que desee cargar**- tiene una lista de todos los certificados de entidad final. Seleccione el certificado que desee cargar
- **Contraseña**: Si el almacén de claves tiene una contraseña, marque este recuadro de selección y escriba la contraseña en el recuadro de texto.
- **Seleccionar la lista de y certificados CA raíces e intermedios para subir**: En el recuadro de lista, seleccione los certificados de CA raíz e intermedios para subir.

- En la página **Seleccione las Certificaciones/Claves OpenPGP a cargar** del asistente, los certificados asociados al conjunto de claves seleccionado aparecen en la lista.

  Nota: Puede pulsar **Ver detalles** para ver los detalles del certificado seleccionado. En caso de un certificado cuyo ID de clave e ID de emisor sea el mismo, éste será un certificado propio.
  - Seleccione una clave de nivel superior de la lista.
  - Escriba la contraseña de la clave de nivel superior si desea cargar la clave de nivel superior.

    Nota: Si hay subclaves en la clave de nivel superior, todas las subclaves aparecen en la lista **Seleccione la subclave a cargar**.

    Importante: Esto no es aplicable cuando se cargan certificados públicos para cifrado.
  - Seleccione la subclave si es necesario.
  - Escriba la contraseña de la subclave.

  Importante: Esto no es aplicable cuando se cargan certificados públicos para cifrado.

  Recuerde: Si carga el certificado para un socio externo, no es necesaria la contraseña de nivel superior y la subclave.

6. Pulse **Siguiente** para ir a la página **Detalles del certificado** del asistente.
7. En la página **Detalles de certificado** del asistente, escriba los siguientes detalles del certificado:
   - **Nombre de certificado sin secundarios**: Nombre del certificado sin secundarios. El nombre de campo depende de si el certificado es un certificado sin secundarios, un certificado CA raíz o un certificado CA intermedio.
   - **Descripción**: Descripción del certificado sin secundarios.
   - **¿Es un certificado de autenticación del servidor FTP?**: Seleccione este recuadro de selección si el certificado cargado es para autenticación del servidor FTP.
   - **¿Es un certificado de autenticación del servidor SFTP?**: Seleccione este recuadro de selección si el certificado cargado es para autenticación del servidor SFTP.

     Importante: La autenticación del servidor SFTP y del servidor FTP no se aplica para certificados OpenPGP.
   - **Tipo de certificado**: Asocie este certificado a un tipo de certificado. Los diferentes tipos soportados son Firma digital, Verificación de firma digital, Cifrado, Descifrado, Servidor SSL y Cliente SSL.

Recuerde:

– La opción de cifrado es para un socio externo y la opción de descifrado es para un socio interno.

– No se soporta el cliente SSL para el tipo de certificado OpenPGP.

- **Utilización de certificado**: Asocie una utilización al certificado. Los valores son Primario y Secundario.

  Importante: Esto no es aplicable para descifrado, verificación de firmas y certificado de servidor SSL.

- **Modalidad de funcionamiento**: Seleccione una modalidad de funcionamiento para cifrado, firma y certificados de cliente SSL.

  Importante: La modalidad de funcionamiento no es aplicable para cifrado y verificación de firmas.

- **Estado**: Seleccione habilitado o inhabilitado según si desea habilitar o inhabilitar un certificado después de subirlo. El botón **Siguiente** sólo se habilita si se habilita el certificado.

- **Gestión de conjuntos**: Puede asociar un certificado a un conjunto existente o bien crear uno nuevo. Si el certificado es un certificado secundario, sólo se puede asociar a un conjunto existente. Puede asociar el certificado a cualquier conjunto para un socio interno con tipo cifrado o para un socio externo con tipo SSL (autorización de cliente entrante) o Firma (Verificar).

  Nota: Si carga un certificado OpenPGP para un socio interno, Gestión de conjuntos no es aplicable. En caso de cifrado para un socio externo y firma o certificado de cliente SSL para un socio interno, seleccione **Añadir nuevo conjunto** o **Actualizar conjunto existente**. Esto sólo es aplicable si decide utilizar conjuntos. De lo contrario, pulse **Finalizar**.

8. Pulse **Siguiente** para ir a la página Conjunto del asistente. Si el certificado es primario, no tiene que crear conjuntos y asociar el certificado a un conjunto y una conexión participante. Si ha marcado el recuadro de selección **Crear nuevo conjunto**, se abrirá la página **Crear nuevo conjunto** del asistente. De lo contrario, se abrirá la página **Añadir a existente** del asistente. Si el archivo contiene una clave privada del socio interno o el certificado público del socio externo utilizado para SSL / Firma digital, puede pulsar **Finalizar**.

   Importante: No se soporta la transición de secundario a primario para certificados OpenPGP.

9. En la página **Crear nuevo conjunto** del asistente, especifique los detalles del nuevo conjunto. Para los certificados primarios, no tiene que crear conjuntos y asociar un certificado a ellos. Especifique los siguientes valores:

   - **Nombre de conjunto**: El nombre del conjunto.
   - **Descripción** - La descripción del conjunto.
   - **Estado**: Seleccione habilitado o inhabilitado. Si está inhabilitado, no se habilitará el botón **Siguiente**.
   - **Establecer valores predeterminados**: Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.

10. En la página **Añadir a conjunto existente** del asistente, seleccione los conjuntos que se añadirán al certificado. Especifique los siguientes valores:

    - **Seleccionar de la lista de conjuntos disponibles para el tipo de certificado seleccionado**: En la lista, seleccione uno o varios conjuntos para añadir el certificado.

- **Establecer valores predeterminados**: Seleccione este recuadro de selección si desea que este conjunto sea el predeterminado.

11. En **Crear nuevo conjunto** o **Añadir al conjunto existente**, pulse **Siguiente** para ir a la página **Valores predeterminados** del asistente. El botón **Siguiente** sólo estará habilitado si el estado del conjunto es habilitado.
12. Seleccione **habilitado** o **inhabilitado** en el **Estado** en función de si desea habilitar o inhabilitar el certificado después de subirlo.

    Nota: Si ha marcado el recuadro de selección **Establecer como conjunto predeterminado** en la página anterior (Crear nuevo conjunto o Añadir a conjunto existente), deberá asociar el conjunto a una modalidad de funcionamiento. Se visualizarán las utilizaciones de certificado según las modalidades de operación. El cifrado se inhabilitará para socios internos. Cliente SSL y Firma digital se inhabilitarán para socios externos.
13. Pulse **Siguiente** para ir a la página de Configuración del asistente. En el caso de que pulse **Siguiente** y de que falten algunos certificados CA raíces o intermedios, se le solicitará que los suba. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** si desea realizar la subida más tarde.
14. En la página Configuración del asistente, especifique los valores siguientes:

    Nota: La página Configuración muestra una lista de utilizaciones de (conjunto de) certificados respecto a las modalidades de operación. El nombre de conjunto actual se lleva previamente para todos, pero puede restablecerlo.
    - **Socio de origen**: Este campo estará rellenado con el valor del socio interno.
    - **Socio de destino**: Esta lista estará rellenada con la lista de socios externos. También puede seleccionar el valor "Todos" para incluir todos los socios externos.
    - **Paquete de origen**: En la lista, seleccione los objetos de Definiciones de flujo de documentos de paquete del socio interno.
    - **A paquete**: En la lista, seleccione el paquete de objetos de definiciones de flujo de documentos del socio externo.
15. Pulse **Añadir más conexiones** si desea asociar el conjunto a otras conexiones de participantes.
16. Pulse **Añadir certificado secundario** para añadir un certificado secundario al conjunto actual.
17. Pulse **Finalizar** para subir el certificado. En caso de que falten certificados raíz o CA intermedios, se le solicitará que los cargue. Si pulsa "Sí" en la ventana de solicitud, se abrirá la primera página del asistente. Pulse **Cancelar** en la ventana de solicitud si desea realizar la subida más tarde.

Nota: En el caso de OpenPGP, si se produce un error en la carga del certificado a pesar de cargar el certificado correcto, reinicie el servidor.

Creación de conjuntos de certificados

Acerca de esta tarea

El Conjunto de certificados se introduce para las siguientes funciones de seguridad:

- Autenticación de cliente SSL de los mensajes salientes del socio interno al socio externo.
- Adición de firma digital a los mensajes salientes del socio interno al socio externo.

- Cifrado de los mensajes salientes del socio interno al socio externo.
- Los conjuntos no se utilizan para situaciones de tráfico entrante, como la verificación del certificado de autenticación del cliente SSL del socio externo en el almacén de confianza de WebSphere Partner Gateway, la verificación de la firma digital del socio externo, o el descifrado de los mensajes cifrados dirigidos al socio interno.

Para crear un nuevo conjunto de certificados, siga este procedimiento:

1. En la consola, vaya a **Perfil** > **Socio** > **Lista de certificados** > **Lista de conjunto de certificados**> **crear conjunto**.
2. Pulse**Certificado > Conjuntos de certificados> Crear conjunto**.
3. Escriba el **Nombre de conjunto** y la **Descripción** del nuevo conjunto de certificados.
4. Establezca el **Tipo de certificado**.
5. Marque el recuadro de selección **Habilitado** o **Inhabilitado** para habilitar o inhabilitar el **Conjunto de certificados**.
6. Pulse **Cargar certificado**

   Nota: .Las listas **Certificado primario** y **Certificado secundario** se rellenan en función del **Tipo de certificado** seleccionado. Si hay certificados ya creados y no asociados a ningún conjunto, puede añadir estos certificados al conjunto que se está creando. Si la lista de certificados está vacía, habrá una lista desplegable vacía.
7. Seleccione el **Certificado primario** y el **Certificado secundario** de la lista.
8. Pulse **Guardar**.

Supresión de un conjunto de certificados

Acerca de esta tarea

1. En la Consola, vaya a **Perfil** > **Socio** > **Lista de conjuntos de certificados**. En esta vista se muestra una lista con todos los certificados creados para el socio.
2. Pulse el icono **Suprimir**. Antes de la operación de supresión, compruebe que ha modificado todas las referencias a este conjunto en la conexión.
3. Si una o varias conexiones utilizan este conjunto, aparecerá un mensaje de aviso. Para comprobar si se utiliza un certificado determinado, consulte el apartado “Dónde se utiliza el certificado”.
4. En la ventana del mensaje de aviso, pulse **Aceptar** para suprimir o pulse **Cancelar** para anular la supresión del conjunto de certificados.

Dónde se utiliza el certificado

En la consola, vaya a **Perfil** > **{Socio}** > **Lista de certificados** > **Lista de conjunto de certificados**> **Donde se utiliza**. La vista resultante muestra los siguientes detalles:

- Socio de origen
- Socio de destino
- Paquete de origen
- Paquete de destino
- Cliente SSL
- Firma digital
- Verificación de firma digital

- Cifrado
- Descifrar
- Validez

Nota: El certificado podría no ser válido por los siguientes motivos: que no hay certificado primario, que el certificado primario está inhabilitado, que el primario ha caducado y no hay secundario o que tanto el primario como el secundario han caducado.

Configuración de SSL para el receptor/destino de FTP Scripting

Para el receptor de FTP Scripting, el certificado de autenticación de cliente SSL se carga al perfil del operador de concentrador. Aunque los certificados se carguen para el socio interno, no se sobrescribirán los valores globales.

Cómo proporcionar un conjunto de certificados predeterminados para todos los socios internos

Como WebSphere Partner Gateway soporta varios socios internos, cada socio tiene que subir las claves privadas. Si una organización desea compartir un certificado con sus unidades organizativas, deberá subir el certificado para cada socio interno. Para simplificar esta operación, puede proporcionar una opción predeterminada para que un determinado certificado se utilice para todos los socios internos.

En la Consola, vaya a **Certificados** > **Subir certificados**. Suba los certificados y proporcione los detalles acerca del tipo de certificado, la utilización y la modalidad de funcionamiento. Cuando guarde la información especificada, el certificado/claves se cargarán en el nivel de operador de concentrador. Durante el tiempo de ejecución, el valor predeterminado proporcionado en el nivel de operador de concentrador se utiliza si falta algún certificado.

Resumen de certificado

La Tabla 32 muestra un resumen del uso de los certificados en WebSphere Partner Gateway. Las ubicaciones de certificados se muestran entre paréntesis "( )".

Tabla 32. Información de resumen de certificados

Método de entrega de mensajes (ver nota 1)	Certificado de operador de concentrador	Obtención de un certificado y CA de socio	CA (ver nota 2)	Otorgar certificado al socio (consulte la nota 3)	Comentarios
SSL entrante	Instalar en SSL del servidor WebSphere Application Server. (Colocar en almacén de claves de WebSphere Application Server).	Certificado autofirmado del socio.	Sólo es necesario si se utiliza la Autenticación de cliente. (Coloque el certificado autofirmado o de CA en el almacén de confianza de WebSphere Application Server).	Certificado de operador del concentrador, si es autofirmado, o certificado raíz de CA, en caso necesario, si es autenticado por CA.	

Tabla 32. Información de resumen de certificados (continuación)

Método de entrega de mensajes (ver nota 1)	Certificado de operador de concentrador	Obtención de un certificado y CA de socio	CA (ver nota 2)	Otorgar certificado al socio (consulte la nota 3)	Comentarios
SSL de salida	Si se utiliza la Autenticación de cliente. (WebSphere Partner Gateway)	Certificado del servidor de socio o certificado raíz de CA, si es autenticado por la CA.	WebSphere Partner Gateway	Certificado de operador del concentrador, si es autofirmado o certificado CA, si está firmado por terceros.	
Descifrado entrante	Clave privada (WebSphere Partner Gateway)	N/D	Si el certificado está firmado por CA, los certificados CA deben cargarse como certificados Raíz/ Intermediarios.	Certificado de operador de concentrador	Para descifrar el mensaje
Verificación de firma digital entrante	N/D	Certificado para validar el certificado utilizado para la firma digital. (WebSphere Partner Gateway)	WebSphere Partner Gateway	ND	Para verificación y no rechazo
Cifrado saliente	N/D	Utilice el certificado obtenido por el socio. (El certificado está instalado en el perfil del socio)	Cadena de certificados CA para certificado cliente si no está autofirmado	N/D	Para descifrar mensajes de salida
Firma saliente	Clave privada y certificado (WebSphere Partner Gateway)	N/D	Cadena de certificados CA	Opcional, en función del socio; proporcione el certificado de WebSphere Partner Gateway	
Certificado para validación de ID de empresa	N/D	Cargar en perfil de socio			Valida que este certificado es para este ID de empresa cuando se realiza la comprobación del cliente de SSL

Notas:

1. Un mensaje entrante es uno que llega a WebSphere Partner Gateway desde un socio. Un mensaje saliente es uno que sale de WebSphere Partner Gateway hacia un socio.
2. Si el certificado es emitido por CA, se debe obtener y almacenar el certificado de CA emisora. Esto se aplica al certificado del operador de concentrador o al certificado del socio.

3. Si hay una clave privada implicada, este certificado corresponde a la clave privada.

Utlización de claves y certificados formateados con PEM con WebSphere Partner Gateway

En esta sección se proporciona información sobre la utilización de los certificados y claves codificados con PEM.

Utilización de claves privadas con formato PEM

Si se posee una clave privada en formato PEM y desea subirla a WebSphere Partner Gateway, no podrá subirla a no ser que la clave privada se convierta a formato PKCS#8.

Esto se puede realizar con la herramienta OpenSSL.

Utilice este mandato para convertir una clave con formato PEM a formato PKCS#8:

```
openssl pkcs8 -topk8 -in usr.key -out usr.p8 -outform DER
```

Este mandato funciona con claves que se han creado con OpenSSL.

OpenSSL está disponible en distribuciones Linux y también se puede descargar del sitio web http://www.openssl.org.

Utilización de certificados con formato PEM

El certificado se puede subir en WebSphere Partner Gateway en formato PEM. Funciona con certificados con formato PEM que se han generado con OpenSSL.

Certificado codificado con PKCS#7 con WebSphere Partner Gateway

Acerca de esta tarea

En Windows, si se tienen certificados codificados con formato PKCS#7 (archivos .p7b), siga los siguientes pasos para extraer los certificados del archivo .p7b:

1. Efectúe una doble pulsación en el archivo .p7b.
2. En el panel de navegación, expanda el árbol de carpetas y pulse **Certificados**. En el lado derecho aparecerá la lista de certificados que contiene el archivo.
3. Si desea copiar un certificado en el sistema de archivos, efectúe una doble pulsación en el certificado. Se visualizarán los detalles del certificado.
4. En los detalles del certificado, pulse el separador **Detalles**.
5. Pulse **Copiar a archivo** para copiar el archivo en el sistema de archivos.
6. Exporte el certificado como un archivo codificado con DER.

Carga de claves SFTP

Pasos para cargar claves SFTP.

Acerca de esta tarea

Para subir claves SFTP, realice los pasos siguientes:

1. Vaya a **Administración de cuentas** > **Perfiles** > **Certificados**.

2. Pulse **Cargar claves SFTP**.
3. En la página **Cargar claves SFTP**, pulse **Examinar** y seleccione el archivo de claves desde su local. El archivo subido se utilizará para la autenticación basada en claves. El icono de **datos contenidos** indica que una Clave ya está subida.

Conformidad con FIPS

WebSphere Partner Gateway cumple el estándar FIPS (Estándar Federal de Proceso de Información) FIPS 140-2. **IBMJCEFIPS** es el proveedor de JCE compatible con FIPS. El proveedor **IBMJSSE2 JSSE** utiliza **IBM JCE** y no contiene código para cifrado, de modo que no es necesario estar certificado para la conformidad con FIPS. Aunque el proveedor **IBMJSSEFIPS JSSE** es compatible con FIPS, utilice el proveedor **IBMJSSE2** en WebSphere Partner Gateway. **IBMJSSE2** es el proveedor más reciente y soporta más algoritmos y ha mejorado la capacidad de servicio. El producto se puede ejecutar en modalidad FIPS o no FIPS. Si se configura la modalidad FIPS y se utiliza un algoritmo aprobado como no FIPS, se generará un suceso de error y se detendrá la transacción de documentos. El algoritmo PKCS#12 no está aprobado por FIPS, de modo que no se pueden subir archivos PKCS#12 en modalidad FIPS. Para configurar WebSphere Partner Gateway para ejecutarse en modalidad FIPS o en modalidad predeterminada, es necesario ser administrador. Para la modalidad FIPS, PKCS#12 se puede subir a la consola de WebSphere Partner Gateway en formato JCEKS o JKS mediante iKeyman.

La modalidad FIPS soporta almacenes de claves JKS, JCEKS y OpenPGP, pero no da soporte a los almacenes de claves PKCS#12. Desde la Consola puede subir un certificado y una clave en formato JKS, JCEKS o OpenPGP. En la pantalla **Subida de almacén de claves**, seleccione el formato en la lista **Formato del almacén de claves**. Los valores disponibles en la lista **Formato de almacén de claves** son: PKCS#12, JKS, JCEKS y OpenPGP.

Configuración de WebSphere Partner Gateway para ejecutarse en modalidad FIPS

Acerca de esta tarea

Para configurar WebSphere Partner Gateway para que se ejecute en modalidad FIPS, utilice el siguiente procedimiento:

1. Establezca los proveedores de FIPS en el archivo **java.security**.
2. Establezca la propiedad del sistema **bcg.FIPSMode** a "verdadero" en la consola de WebSphere Partner Gateway.
3. Establezca el proveedor IBMJCEFIPS antes del proveedor IBMJCE en el archivo java.security. El archivo java.security se encuentra en el directorio <Instalación de WAS>/java/jre/lib/security.
4. Establezca las clases de la fábrica de sockets habilitadas para FIPS para la fábrica de sockets JSSE y la fábrica de sockets de servidor.
5. Reinicie todos los servidores.

   Nota: Se genera un suceso informativo para indicar que el producto se ejecuta en modalidad FIPS.

Configuración de WebSphere Partner Gateway para ejecutarse en modalidad predeterminada

Acerca de esta tarea

Para configurar WebSphere Partner Gateway para que se ejecute en modalidad predeterminada, utilice el siguiente procedimiento:

1. En la Consola de WebSphere Partner Gateway, establezca la propiedad del sistema **bcg.FIPSMode** en "Falso".
2. Restablezca los valores de la fábrica de sockets de JSSE, la fábrica de sockets de servidor y los proveedores del archivo **java.security** como se describe a continuación:
   a. Elimine la propiedad del sistema **com.ibm.jsse2.JSSEFIPS=true** de los Argumentos JVM genéricos para cada servidor.
   b. Restablezca los valores de las propiedades siguientes a sus valores originales:
      - ssl.SocketFactory.provider
      - ssl.SocketFactory.provider
   c. Para cada instalación de WAS, comente el proveedor IBMJCEFIPS y vuelva a numerar los proveedores, empezando desde 1, en el archivo **java.security**.
3. Reinicie los servidores.

   Nota: Se genera un suceso informativo para indicar la modalidad. En modalidad predeterminada, se pueden utilizar todos los algoritmos soportados, incluidos los algoritmos aprobados no FIPS.

Configuración de los proveedores IBM JSSE para la modalidad FIPS

Acerca de esta tarea

Para configurar los proveedores IBM JSSE para la modalidad FIPS, utilice el siguiente procedimiento:

1. Establezca la propiedad del sistema **com.ibm.jsse2.JSSEFIPS** en "Verdadero". Esto se realiza estableciendo las propiedades del sistema JVM para el servidor de aplicaciones mediante la Consola administrativa de WAS. Vaya a la página <Servidor>/Java y Gestión de procesos/Definición/Java Virtual Machine y especifique la propiedad **-Dcom.ibm.jsse2.JSSEFIPS=true**. Esta configuración se debe realizar para cada servidor.
2. Establezca las siguientes propiedades de seguridad para que el proveedor IBMJSSE2 maneje todas las solicitudes de JSEE:
   - ssl.SocketFactory.provider = com.ibm.jsse2.SSLSocketFactoryImpl
   - ssl.ServerSocketFactory.provider = com.ibm.jsse2.SSLServerSocketFactoryImpl
3. Añada el proveedor IBMJCEFIPS, com.ibm.crypto.fips.provider.IBMJCEFIPS, a la lista de proveedores antes del proveedor IBMJCE. No elimine el proveedor IBMJCE, ya que es necesario para el soporte del almacén de claves.

   Nota: Cuando IBMJSSE2 está en modalidad FIPS, sólo se da soporte al protocolo TLS.

Algoritmos soportados en modalidad FIPS y no FIPS

Los siguientes algoritmos están soportados en FIPS:

- Diffie-Hellman
- RSA, DSA
- SHA-1, SHA-384, SHA-224, SHA-512
- AES, DES, TDES (Triple DES)
- FIPS 186-2 – Algoritmo para la generación de números pseudoaleatorios (PRNG)
- Seguridad de capa de transporte: TLSv1
- Formato de almacén de claves: JKS, JCEKS

Los siguientes algoritmos están soportados en WebSphere Partner Gateway:

- Cifrado asimétrico: RSA, DSA
- Función hash: SHA-1, MD5, SHA-384, SHA-224, SHA-512, RIPEMD/160.
- Cifrado simétrico: AES, DES, 3DES, RC2 (todos con modalidad CBC), CAST5, Blowfish, Twofish.
- PRNG: IBMSecureRandom
- Algoritmo de firma: dsa-sha1, rsa-sha1
- Seguridad de capa de transporte: SSLv3, TLSv1
- Formato de almacén de claves: PKCS#12, JKS, JCEKS, OpenPGP
- Algoritmos de claves simétricas: AES y TripleDES con detección de modificaciones.

  Restricción: Sólo se pueden utilizar los algoritmos TripleDES y AES cuando se hayan definido las dos modalidades de Detección de modificaciones y FIPS.

Los siguientes algoritmos no están soportados en FIPS pero sí lo están en WebSphere Partner Gateway:

- Función hash: MD5. RIPEMD160
- Cifrado simétrico: RC2, CAST5, Blowfish, Twofish
- Proveedor PRNG IBMSecureRandom (todos los casos de WebSphere Partner Gateway).
- Seguridad de capa de transporte: SSLv3
- Formato de almacén de claves: PKCS#12

Capítulo 14. Gestión de alertas

Las alertas de WebSphere Partner Gateway se utilizan para notificar al personal clave de fluctuaciones inusuales en el volumen de las transmisiones que se reciban o cuando se producen errores de proceso de documentos de empresa.

Una opción complementaria del módulo Visor, Visor de sucesos, le ayuda a identificar mejor los errores y a resolver errores de procesos.

Visión general de las alertas

Una alerta consiste en un mensaje de correo electrónico basado en texto dirigido a los contactos suscritos o a una lista de distribución de personal clave. Las alertas se basan en la ocurrencia de un suceso del sistema (alerta basada en sucesos) o en un volumen de flujo de documentos esperado (alerta basada en volúmenes).

- Utilice una **alerta basada en volúmenes** para recibir notificaciones de un aumento o reducción en el volumen de las transmisiones.

  Por ejemplo, si es un socio externo, puede crear una alerta basada en volúmenes que le notifique si no recibe ninguna transmisión del socio interno en un día laborable cualquiera (establezca el Volumen en Volumen cero, establezca la frecuencia en Diaria y seleccione De lunes a viernes en la opción Días de la semana). Esta alerta puede resaltar dificultades en las transmisiones de red del socio interno.

  Si es un socio externo, también puede crear una alerta basada en volúmenes que le avise cuando el número de transmisiones del socio interno excede la tasa normal. Por ejemplo, si recibe normalmente unas 1000 transmisiones al día, puede establecer el Volumen esperado en 1000 y la Desviación de porcentaje en 25%. La alerta le notificará cuando reciba más de 1250 transmisiones por día (también le notificará cuando el volumen de transmisiones caiga por debajo de 750). Esta alerta puede identificar una demanda creciente por parte del socio interno, lo cual, en algún momento, le podría suponer tener que añadir más servidores al su entorno. Para obtener más información sobre las alertas basadas en volúmenes, consulte el apartado “ Creación de una alerta basada en volúmenes” en la página 301.

  Nota:

  1. Las alertas basadas en volúmenes supervisan el volumen con respecto al tipo de documento que haya seleccionado al crear la alerta. WebSphere Partner Gateway sólo mira los documentos que contengan el tipo de documento seleccionado en la alerta y genera alertas sólo cuando se cumplen todos los criterios de la alerta.
  2. El socio externo sólo puede crear una alerta basada en volúmenes en el volumen de documentos enviados al socio interno. Para que el socio externo establezca una alerta basada en volúmenes sobre el volumen de documentos entrantes enviados desde el socio interno, el socio externo debe solicitar al administrador del concentrador que configure una alerta basada en volúmenes en nombre del socio externo, especificando al socio externo como propietario de la alerta. Un socio interno también puede crear alertas basada en volumen para enviar a socios externos.

- Utilice una **alerta basada en sucesos** para recibir notificaciones cuando se produzcan errores en el proceso de documentos. Por ejemplo, puede que desee

crear una alerta que le notifique si los documentos no pueden procesarse debido a errores de validación o porque se han recibido documentos duplicados. También puede crear alertas que le permitan conocer cuándo un certificado está a punto de caducar.

Utilizará los códigos de suceso predefinidos de WebSphere Partner Gateway para crear alertas basadas en sucesos. Existen cinco tipo de evento: Depuración, Información, Aviso, Error, Crítico. Dentro de cada tipo de suceso hay muchos sucesos. Puede ver y seleccionar los sucesos predefinidos en la página Alerta: Sucesos. Por ejemplo, 240601 Anomalía en reintento de AS o 108001 No un certificado. Para obtener más información sobre las alertas basadas en sucesos, consulte el apartado " Creación de una alerta basada en sucesos" en la página 303.

Sugerencia:

- Utilice una alerta basada en volúmenes para recibir notificaciones si el volumen de transmisiones esperado del socio externo o del socio interno caen por debajo de los límites operativos. Esta alerta puede resaltar dificultades en las transmisiones de red del socio externo o del socio interno.
- Utilice una alerta basada en sucesos para recibir notificaciones sobre errores en el proceso de documento. Por ejemplo, puede crear una alerta basada en sucesos que le notifique si los documentos no pueden procesarse debido a errores de validación.

Nota: para enviar alertas, deberá configurar un servidor de correo electrónico para que envíe las alertas. Las alertas se configuran en la página Atributos del motor de alertas que se encuentra pulsando **Administración del sistema** > **Administración del Gestor de documentos** > **Motor de alertas**. Para obtener más información acerca de la configuración del servidor de correo electrónico de alertas, consulte el apartado "Updating alert mail addresses" en la publicación *Guía del socio de WebSphere Partner Gateway*.

Visualización o edición de detalles de alerta y contactos

Acerca de esta tarea

El socio interno puede ver todas las alertas, independientemente de quién sea su propietario (el creador de la alerta).

1. Pulse **Administración de cuentas** > **Alertas**. El sistema mostrará la página Búsqueda de alertas.
2. Seleccione el criterio de búsqueda en las listas desplegables; especifique el Nombre de alerta. También puede pulsar el botón **Buscar** sin seleccionar ningún criterio de búsqueda (el sistema mostrará todas las alertas).
3. Pulse **Buscar**. El sistema mostrará la página Resultados de la búsqueda de alerta.
4. Pulse el icono Ver detalles para ver los detalles de una alerta.
5. Pulse el icono Editar para editar los detalles de las alertas.
6. Edite la información si es necesario.
7. Pulse la pestaña **Notificar**.
8. Seleccione un socio (sólo socio interno o administrador de concentrador). El socio interno puede ver todas las alertas independientemente de su propietario.
9. Edite los contactos de esta alerta, si así lo desea.
10. Pulse **Guardar**.

Búsqueda de alertas

Acerca de esta tarea

1. Pulse **Administración de cuentas** > **Alertas**. El sistema mostrará la página Búsqueda de alertas.
2. Seleccione el criterio de búsqueda en las listas desplegables; especifique el Nombre de alerta. También puede pulsar el botón **Buscar** sin seleccionar ningún criterio de búsqueda (el sistema mostrará todas las alertas).

Tabla 33. Criterios de búsqueda de alertas para socios

Valor	Descripción
Tipo de alerta	Volumen, suceso o todos los tipos de alerta.
Nombre de alerta	Nombre de la alerta.
Estado de alerta	Alertas que están habilitadas, inhabilitadas o ambas.
Contactos suscritos	Contactos asignados por alertas. Las selecciones son Tiene suscriptores, Sin suscriptores o Todo.
Resultados por página	Controla cuántos resultados de búsqueda aparecen.

Tabla 34. Criterios de búsqueda de alertas del socio interno y del administrador del concentrador

Valor	Descripción
Propietario de alerta	Creador de la alerta.
Socio de alerta	Socio al que se aplica la alerta.
Tipo de alerta	Volumen, suceso o todos los tipos de alerta.
Nombre de alerta	Nombre de la alerta.
Estado de alerta	Alertas que están habilitadas, inhabilitadas o ambas.
Contactos suscritos	Contactos asignados por alertas. Las selecciones son Tiene suscriptores, Sin suscriptores o Todo.
Resultados por página	Controla cuántos resultados de búsqueda aparecen.

3. Pulse **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.

Inhabilitación o habilitación de una alerta

Procedimiento

1. Pulse **Administración de cuentas** > **Alertas**. El sistema mostrará la página Búsqueda de alertas.
2. Seleccione los criterios de búsqueda en las listas desplegables y especifique el nombre de alerta.
3. Pulse **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.
4. Localice la alerta y pulse el botón **Inhabilitado** o **Habilitado** bajo Estado. Sólo el administrador del concentrador y el propietario de la alerta (creador de la alerta) tienen permiso para editar el estado de la alerta.

Eliminación de una alerta

Procedimiento

1. Pulse **Administración de cuentas** > **Alertas**. El sistema mostrará la página Búsqueda de alertas.

2. Seleccione los criterios de búsqueda en las listas desplegables y especifique el **Nombre de alerta**.
3. Pulse **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.
4. Localice la alerta y pulse el icono Suprimir para suprimirla. Sólo el administrador del concentrador y el propietario de la alerta (el creador de la alerta) pueden eliminarla.

Adición de un nuevo contacto a una alerta existente

Acerca de esta tarea

1. Pulse **Administración de cuentas** > **Alertas**. El sistema mostrará la página Búsqueda de alertas.
2. Especifique el criterio de búsqueda en las listas desplegables; especifique el Nombre de alerta.
3. Pulse **Buscar**. El sistema muestra una lista de las alertas que coinciden con los criterios de la búsqueda, en caso de haberlas.
4. Pulse el icono Ver alertas para ver los detalles de la alerta.
5. Pulse el icono Editar para editar los detalles de las alertas.
6. Pulse la pestaña **Notificar**.
7. Seleccione un socio (sólo socio interno y administrador de concentrador).
8. Si el contacto que desea añadir aparece en la lista del recuadro de texto Contactos, seleccione el contacto y pulse el botón **Suscribir**. Vaya a 13.

   Si el contacto que desea añadir no aparece listado en el recuadro de texto Contactos, pulse **Añadir nueva entrada a contactos**. El sistema muestra la ventana emergente Crear nuevo contacto.

   Observe que el enlace Añadir nueva entrada a contactos únicamente está disponible si el socio es un operador de concentrador.
9. Especifique el nombre, la dirección de correo electrónico, y los números de teléfono y de fax del contacto.
10. Seleccione el estado de alerta del contacto.
    - Seleccione **Habilitado** para iniciar el envío de mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
    - Seleccione **Inhabilitado** si no desea enviar mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
11. Seleccione la visibilidad del contacto.
    - Seleccione **Local** para hacer que el contacto sólo sea visible para su organización.
    - Seleccione **Global** para que el contacto sea visible al administrador de concentrador y al socio interno. Ambos usuarios pueden suscribir el contacto a las alertas.
12. Pulse **Guardar** para guardar el contacto. Pulse el botón **Guardar y suscribir** para guardar el contacto y añadir el contacto a la lista de contactos de esta alerta.
13. Pulse **Guardar.**

Creación de una alerta basada en volúmenes

Acerca de esta tarea

1. Pulse **Administración de cuentas** > **Alertas**. El sistema mostrará la página Búsqueda de alertas.
2. Pulse **Crear** en la esquina superior derecha de la página. El sistema muestra la pestaña Definición de alertas.
3. Seleccione **Alerta de volumen** para **Tipo de alerta** (se trata del valor predeterminado). El sistema mostrará los recuadros de texto apropiados para una alerta de volumen.
4. Escriba un **Nombre de alerta** para la alerta.
5. Escriba **texto empresarial personalizado**. Cuando se genere el suceso de alerta, se enviará este mensaje junto con dicho suceso.
6. Seleccione un **Propietario de alerta** para la alerta.
7. Seleccione un **Socio** con derechos para crear una alerta basada en volumen (sólo socio interno y administrador de concentrador).
8. Seleccione **Paquete**, **Protocolo**, y **Tipo de documento** en las listas desplegables. El Paquete, Protocolo y Tipo de documento seleccionados deben coincidir con el Paquete, Protocolo y Tipo de documento del socio externo de origen.
9. Seleccione una de las tres opciones de volumen (Esperado, Rango o Volumen cero y, a continuación, siga con el punto 10 en la página 302:
   - **Esperado** - Seleccione Esperado si desea que se genere una alerta cuando el volumen del tipo de documento se desvía de una cantidad exacta. Siga los pasos siguientes para crear una alerta en un volumen de tipo de documento esperado:
     a. En el recuadro de texto de Volumen, especifique el número de tipos de documento que espera recibir en un margen de tiempo seleccionado en el punto 10 en la página 302. Especifique sólo un número positivo; la alerta no funcionará si especifica un número negativo.
     b. En el recuadro de texto Desviación de porcentaje, especifique un número que defina el límite que el volumen de tipo de documento puede desviarse antes de activarse la alarma. Por ejemplo:
        – Si el Volumen = 20 y la Desviación de porcentaje = 10, un flujo de documentos inferior a 18 o mayor que 22 desencadenará una alerta.
        – Si el Volumen = 20 y la Desviación de porcentaje = 0, cualquier volumen de flujo distinto de 20 desencadenará una alerta.
   - **Rango**. Seleccione Rango para generar una alerta si el volumen de flujo de documentos queda fuera de un rango mínimo-máximo. Lleve a cabo los siguientes pasos para crear una alerta basada en un rango de valores:
     a. En el recuadro de texto Mínimo, especifique el número mínimo de flujos de documento que espera recibir dentro de un intervalo temporal especificado en el paso 10 en la página 302. Sólo se desencadenará una alerta si el volumen de flujo de documento cae por debajo de dicha cantidad.
     b. En el recuadro de texto Máximo, especifique el número máximo de flujos de documento que espera recibir dentro de un intervalo temporal seleccionado en el apartado 10 en la página 302.

        Nota: ambos valores de los recuadros de texto Mínimo y Máximo deben estar rellenados al crear una alerta basada en el rango de volúmenes.

- **Volumen cero**. seleccione Volumen cero para activar una alerta si no se produce ningún proceso dentro del intervalo de tiempo seleccionado en el paso 10.

10. Seleccione Diario o Rango para la trama de tiempo (Frecuencia) que el sistema utilizará para supervisar el volumen de flujo de documentos para la generación de alertas.
    - **Diario**. Seleccione Diario para supervisar el volumen de flujo de documentos uno o más días reales de la semana o el mes. Por ejemplo, seleccione Diario si desea supervisar el volumen de flujo de documento sólo uno o más días determinados de la semana (por ejemplo, los lunes o los lunes y jueves), o del mes (por ejemplo, el día 1 y el 15).
    - **Rango**. Seleccione Rango para supervisar el volumen de flujo de documentos entre dos días de la semana o del mes. Por ejemplo, seleccione Rango para supervisar el volumen de flujo de documento todos los días entre el lunes y el viernes, o todos los días entre los días 5 y 20 de cada mes.
11. Seleccione la hora de **inicio** y la **hora final** (en formato de 24 horas) durante las cuales el sistema supervisará el volumen de procesos para los días seleccionados en el siguiente paso. Tenga en cuenta que cuando se selecciona una frecuencia Rango, el volumen de flujo de documentos se supervisa desde la hora de inicio del primer día del rango hasta la hora de finalización del último día del rango.
12. Seleccione los días adecuados de la semana o el mes en que se realizará la supervisión de dicha alerta. Si ha seleccionado Diario como frecuencia, seleccione los días reales de la semana o los días del mes para la supervisión de la alerta. Si ha seleccionado Rango como frecuencia, seleccione dos días de la semana o dos días del mes entre los que se sitúe la supervisión de la alerta.
13. Seleccione el **Estado de alerta** de esta alerta como Habilitado o Inhabilitado.
14. Pulse **Guardar**.
15. Pulse la pestaña **Notificar**.
16. Pulse el icono **Editar**.
17. Seleccione un **socio** (sólo el socio interno o el administrador del concentrador).
18. Si el contacto que desea añadir aparece en la lista del recuadro de texto Contactos, seleccione el contacto y pulse el botón **Suscribir**. Vaya a 23 en la página 303.

    Si el contacto que desea añadir no aparece listado en el recuadro de texto Contactos, pulse **Añadir nueva entrada a contactos**. El sistema muestra la ventana emergente Crear nuevo contacto.

    Tenga en cuenta que la opción Añadir nueva entrada a contactos sólo está presente en el Propietario de alertas para crear contactos asociados con éste. Esta función no permite al Propietario de alertas añadir contactos para los Socios de alertas.
19. Especifique el **nombre**, la **dirección de correo electrónico**, y los números de **teléfono** y de **fax** del contacto.
20. Seleccione el **estado de alerta** del contacto.
    - Seleccione **Habilitado** para iniciar el envío de mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
    - Seleccione **Inhabilitado** si no desea enviar mensajes de correo electrónico a este contacto cuando el sistema genere esta alerta.
21. Seleccione la visibilidad del contacto.

- Seleccione **Local** para hacer que el contacto sólo sea visible para su organización.
- Seleccione **Global** para que el contacto sea visible al administrador de concentrador y al socio interno. Ambos usuarios pueden suscribir el contacto a las alertas.

22. Pulse **Guardar** para guardar el contacto; pulse **Guardar & Suscribir** para añadir el contacto a la lista de contactos de esta alerta.
23. Pulse **Guardar**.

Nota: los cambios que se efectúen a las alertas basadas en volúmenes, después del periodo original de supervisión, pasan a ser efectivas el día siguiente del periodo de supervisión. Por ejemplo, una alerta supervisa el periodo 1-3 PM los miércoles y jueves. El miércoles a las 4 PM, la alerta se cambia para supervisar de 5-7 PM. La alerta no realizará la supervisión dos veces el miércoles; el cambio se volverá efectivo el jueves.

Creación de una alerta basada en sucesos

Acerca de esta tarea

1. Pulse **Administración de cuentas** > **Alertas**. El sistema mostrará la página Búsqueda de alertas.
2. Pulse **Crear** en la esquina superior derecha de la página. El sistema muestra la pestaña Definición de alertas.
3. Seleccione **Alerta de suceso** en **Tipo de alerta**. El sistema mostrará los recuadros de texto apropiados para una alerta basada en suceso.
4. Escriba un **Nombre de alerta** para la alerta.
5. Escriba **texto empresarial personalizado**. Cuando se genere el suceso de alerta, se enviará este mensaje junto con dicho suceso.
6. Seleccione un **Propietario de alerta** para la alerta.
7. Seleccione un **Socio** que active la alerta (esta opción sólo está disponible para el socio interno y el administrador de concentrador). Seleccione la opción Cualquier socio para asociar la alerta a todos los socios del sistema. Cuando realice la búsqueda de una alerta y seleccione Cualquier socio como Socio de alerta, el sistema mostrará todas las alertas que no estén asociadas a un socio específico.
8. Seleccione **Tipo de suceso**: Depuración, Información, Aviso, Error, Crítico o Todos.
9. Seleccione el **Nombre de suceso** que activará la alerta, por ejemplo, BCG240601 Anomalía de reintento de AS o 108001 No un certificado. Para crear una alerta que le notifique cuándo un certificado está a punto de caducar, seleccione una de las siguientes opciones:
   - BCG108005 Caducidad de certificado en 60 días
   - BCG108006 Caducidad de certificado en 30 días
   - BCG108007 Caducidad de certificado en 15 días
   - BCG108008 Caducidad de certificado en 7 días
   - BCG108009 Caducidad de certificado en 2 días

   Nota: para que un suceso se liste aquí, debe poder generar una alerta. Para que un suceso pueda generar una alerta, consulte el apartado “Especificación de sucesos alertables” en la página 312.
10. Seleccione el estado de esta alerta: Habilitado o Inhabilitado.

11. Pulse **Guardar**.
12. Pulse la pestaña **Notificar**.
13. Seleccione la **Modalidad de notificación**: Notificar a todas las partes relacionadas o Notificar sólo a los contactos suscritos. Los contactos suscritos se notifican por la modalidad ***Notificar sólo a los contactos suscritos***. Mientras se crean alertas, si se selecciona la modalidad de notificación de alertas como ***Notificar a todas las partes relacionadas***, la notificación se enviará a todas las partes relacionadas a este suceso para el que se ha definido la alerta. Las partes relacionadas para el suceso son los contactos combinados de Participante de origen, Participante de destino y el Propietario de la alerta.
14. Seleccione un **Socio** (sólo el socio interno o el administrador del concentrador).
15. En los contactos listados en el recuadro de texto **Contactos**, seleccione el contacto al que desea notificar y pulse **Suscribir**.
16. Seleccione la modalidad de entrega:
    - **Enviar alertas inmediatamente**. Si selecciona esta opción, el sistema enviará notificaciones de alerta al contacto cuando se produzca la alerta. Utilice esta opción para alertas críticas.
    - **Alertas de lote por**. Si selecciona esta opción, puede especificar cuándo desea que el contacto reciba las notificaciones de alerta. Utilice esta opción para alertas no críticas.

      Las dos opciones de esta sección, Número y Tiempo, no son mutuamente excluyentes.

      Si selecciona la opción **Recuento**, deberá siempre seleccionar la opción Tiempo.

      – Si se alcanza el número de alertas (Número) durante el límite temporal que ha seleccionado (Tiempo), el sistema generará una notificación de alerta.
      – Si se produce una alerta pero no se alcanza el número de alertas (Número) durante el límite temporal seleccionado (Tiempo), el sistema generará una notificación de alerta al terminar el límite temporal.

      La opción **Tiempo** pueden utilizarse sin la opción Número, pero la opción Número debe siempre estar asociada con un límite temporal (Tiempo).

      – **Recuento**. Debe también utilizar la opción Tiempo cuando seleccione esta opción. Especifique un número (n). Se trata del número de alertas que deben producirse durante el periodo de tiempo seleccionado (Tiempo), antes de que el sistema envía una notificación de alerta al contacto de la alerta.

        He aquí un ejemplo de cómo funcionan juntas estas dos opciones:

        En nuestro ejemplo, las opciones de Alertas de lote por se establecen en 10 para Número (10 alertas) y en 2 para Tiempo (periodo de 2 horas). El sistema retiene todas las notificaciones para esta alerta hasta que se producen 10 en un periodo de dos horas o hasta que se alcanza el final del periodo de tiempo.

        Cuando el número de alertas alcanza 10 en un periodo de 2 horas, el sistema envía todas las notificaciones de alerta para esta alerta al contacto.

        Si se produce una alerta pero no se producen 10 alertas durante el límite de tiempo (dos horas), el sistema envía una notificación de alerta al contacto de la alerta al final del límite de tiempo.

- **Hora**. Seleccione el número de horas (n). El sistema retiene la notificación de alerta durante n horas. Cada n horas, el sistema envía todas las notificaciones de alerta retenidas al contacto.

  Por ejemplo, si especifica 2, el sistema retendrá todas las notificaciones para esta alerta que se produzcan en cada intervalo de dos horas. Cuando caduque el intervalo de dos horas, el sistema enviará todas las notificaciones de alerta para esta alerta al contacto.

17. Pulse **Guardar**.

Capítulo 15. Cómo iniciar el flujo de errores

En WebSphere Partner Gateway, como administrador, puede supervisar los sucesos fallidos que se producen al procesar documentos. Un documento puede fallar en el receptor o en el gestor de documentos. Para un documento fallido, se registra el error o suceso grave correspondiente en el Motor de sucesos. Se pueden crear alertas para enviar una notificación por correo electrónico a uno o varios suscriptores.

Asimismo, un administrador puede iniciar un flujo de documentos de error para los socios internos, externos, o ambos. Este flujo de documentos de error se iniciará para un documento fallido en función del error o del suceso crítico. Este flujo de documentos de error puede estar en formato de WebSphere Partner Gateway o en formato de servicio web. Puede configurar el formato en la configuración de flujos de errores de un suceso.

Configuración de documentos de flujo de errores

Acerca de esta tarea

La pestaña Flujo de errores de la consola permite al operador establecer la invocación del Flujo de errores o Servicio web para determinados sucesos de error:

1. Vaya a **Administración de cuentas** > pestaña **Flujo de error**. La lista de flujos de errores tiene iconos visualizar y suprimir para cada flujo de errores.
2. Pulse el icono **Ver** para iniciar la pantalla de configuración de flujo de errores en modalidad de sólo lectura.
3. En la configuración de vista, pulse el icono **Editar** para editar la configuración de flujo de error.
4. En la modalidad de edición, hay los siguientes valores de configuración disponibles:
   - **Nombre** - nombre de configuración del documento del flujo de errores.
   - **Socio remitente** - pulse en la búsqueda de socio y seleccione el nombre de socio. El socio puede ser interno o externo.
   - **Tipo de socio** - seleccione en el desplegable el tipo de socio.
   - **Suceso de error** - en este desplegable únicamente se muestran los sucesos que son de tipo *Error* o *Crítico*.
   - **Tipo de flujo de errores** - puede ser *Documento de flujo de errores* o *Invocar un servicio web*.
   - **Enviar a** - Seleccione los destinatarios del documento fallido. Puede ser *Remitente*, *Receptor* o *Ambos*.
5. Pulse **Guardar**.
6. Pulse **Cancelar** para cancelar.
7. Habilite las funciones de B2B para el flujo de errores configurado.
8. Si se invoca el servicio web, cree la interacción y active la conexión del participante.

Las definiciones de documentos de flujo de errores para XML y servicio web se subirán de forma predeterminada a WebSphere Partner Gateway. Puede habilitarlas para los socios y crear las siguientes conexiones:

- Conexión XML ErrorFlowDocument.
- ErrorFlowDocument sobre servicios web para estilo de documento.
- ErrorFlowDocument sobre servicios web para estilo RPC.

Limitaciones y restricciones

1. El documento de flujo de errores sobre servicios web tiene las limitaciones siguientes:
   - La solicitud de servicios web debe ser una solicitud unidireccional.
   - Si el estilo de enlace es **documento**, el tipo de parámetro de entrada es de elemento **ErrorFlowDocument** que está definido en BCGErrorFlowSchema.xsd.
   - Si el estilo de enlace es **rpc**, el tipo de parámetro de entrada será **Cadena** y el número de parámetros de entrada es uno.
2. El Direccionamiento de flujo de errores no funcionará en caso de ID de empresa erróneos. Si se solicita un documento de flujo de errores para un suceso concreto e incluso si el documento de empresa que tiene los ID inapropiados falla con el mismo suceso configurado, el direccionamiento de documento de flujo de errores no funcionará, ya que los ID de empresa especificados no son válidos.

Capítulo 16. Finalización de la configuración

En este capítulo se describen las tareas adicionales que puede realizar para configurar el concentrador. Incluye los siguientes temas:

Nota: debe siempre utilizar la misma instancia de navegador con la que ha iniciado sesión en la Consola de comunidad para efectuar cambios de configuración en WebSphere Partner Gateway. Si utiliza más de una instancia de navegador al mismo tiempo puede acabar anulando los cambios de configuración.

Soporte de archivos grandes para documentos AS

El soporte de archivos grandes con un orden de tamaño en GB se ha ampliado para AS2 y AS3. El tamaño máximo de archivo procesado mediante matrices de bytes es configurable. Cuando la cantidad de memoria asignada es superior al tamaño de almacenamiento dinámico disponible, se produce un error de falta de memoria. Si el tamaño de datos es inferior a la memoria disponible, es posible que siga produciéndose un error de falta de memoria si la memoria asignada aumenta la memoria disponible. En tiempo de ejecución se determina si el tamaño de archivo configurado se puede soportar en función de la memoria de almacenamiento dinámico disponible. Puede especificar el tamaño máximo de archivo que se puede utilizar con matrices de bytes mediante la propiedad **bcg.maximumFileSizeForByteArrays**. El valor de la propiedad bcg.maximumFileSizeForByteArrays está en MB. Si el tamaño de archivo es superior al valor de esta propiedad, se procesa mediante secuencias. Si el tamaño de archivo es inferior al valor de esta propiedad, y si no hay suficiente memoria disponible, se generará un suceso de error BCG210050.

Cuando inicie sesión como operador de concentrador, vaya a la pestaña **Administrador del sistema** > **Propiedades comunes**. Sobrescriba el valor predeterminado de la propiedad **bcg.maximumFileSizeForByteArrays** para especificar el tamaño de archivo máximo que se utilizará con las matrices de bytes. Aumente el valor de esta propiedad para mejorar el rendimiento.

Habilitación del uso de API

Acerca de esta tarea

WebSphere Partner Gateway proporciona un conjunto de API que pueden utilizarse para acceder a ciertas funciones que habitualmente se realizan en la Consola de comunidad. Estas API se describen en la publicación *WebSphere Partner Gateway Programmer Guide*.

Utilice este procedimiento para habilitar el uso de las API basadas en XML para que los socios puedan hacer llamadas a la API para el servidor WebSphere Partner Gateway.

Procedimiento

1. En el menú principal, pulse **Administración de sistema > Administración de características > API administrativa**.
2. Pulse el icono **Editar** situado junto a **Habilitar la API basada en XML**.
3. Seleccione el recuadro para habilitar el uso de la API basada en XML.
4. Pulse **Guardar**.

Resultados

Nota: La API administrativa basada en XML está en desuso.

También existe la posibilidad de utilizar el programa de utilidad de migración en lugar de la API administrativa para realizar las tareas de creación y actualización. El archivo de importación de migración tiene información nueva o actualizada.

El archivo de importación se describe mediante el esquema XML que se proporciona con el programa de utilidad de migración. Puede utilizar una herramienta de desarrollo como Rational Application Developer para producir un archivo XML de importación que cumpla con el esquema. Al importar este archivo con el programa de utilidad de migración, puede cargar las nuevas definiciones de los socios incluidos los ID de empresa y los contactos de los socios. También puede actualizar las definiciones de socios existentes al importarlas con el programa de utilidad de migración. La API administrativa también le permite crear una lista con algunos de los artefactos de configuración de un sistema. Una exportación completa del sistema utilizando el programa de utilidad de migración proporciona listados de funciones de socios, conexiones de socio y destinatarios (destinos) en el archivo XML exportado.

El a archivo de proceso por lotes **bcgmigrate.bat/bcgmigrate.sh** se utiliza para iniciar el proceso de migración. Mientras se ejecuta el mandato bcgmigrate, asegúrese de que tiene permiso de archivo de **Ejecución** para (bcgmigrate.bat/ bcgmigrate.sh). Esto es más aplicable para plataformas UNIX.

Especificación de las colas que se utilizan para sucesos

Acerca de esta tarea

El concentrador puede configurarse de forma que envíe sucesos a una cola externa configurada utilizando la configuración JMS.

La configuración JMS predeterminada se establece cuando se instala el concentrador. En la página de Propiedades de publicación de sucesos aparecen algunos de estos valores.

Para apuntar a una configuración JMS diferente, proporcione los valores de configuración adecuados para publicar los sucesos en las colas de mensajería de WebSphere Partner Gateway / WAS u otros servidores de mensajería. Además, cambie el nombre de cola para hacer coincidir el nombre de la cola donde se publiquen los sucesos.

Para indicar dónde deben entregarse los sucesos:

1. En el menú principal, pulse **Administración del sistema> Administración de DocMgr > Motor administrativo> Sucesos externos**.
2. Pulse el icono **Editar** situado junto a **Habilitar entrega de sucesos**.
3. Seleccione el recuadro de selección **Habilitar entrega de sucesos** para activar la publicación de sucesos.
4. Si los valores predeterminados son correctos para su instalación, déjelos tal como aparecen. Los valores predeterminados admiten la entrega de sucesos a la cola DeliveryQ facilitada por el servidor JMS configurado en el momento de la instalación.

   Si desea modificar el lugar en el que se entregan los sucesos, actualice los campos utilizando la siguiente información como referencia:

   - Especifique valores para **ID de usuario** y **Contraseña**, si son necesarios para acceder a la cola.
   - En **Nombre de fábrica de la cola JMS**, especifique el nombre de la fábrica de conexiones de la cola JMS del archivo de enlaces JMS que está utilizando.

     Nota: en algunas versiones de Windows (anteriores a XP), es posible que sea necesario cambiar el valor predeterminado del campo **Nombre de fábrica de cola JMS** si desea emplear la característica de entrega de sucesos predeterminada. Será necesario cambiar el valor de **Nombre de fábrica de cola** `WBIC/QCF` por `WBIC\\QCF`.
   - En **Tipo de mensaje JMS**, especifique el tipo de mensaje que se entregará. Las opciones son byte o texto. Dado que el componente Receptor decide la correlación del tipo de mensaje JMS, el valor del tipo de mensaje JMS es opcional.
   - En **Nombre de cola JMS**, especifique el nombre de la cola JMS en la que se publicarán los sucesos. Esta cola ya debe estar definida en el archivo de enlaces JMS que se está utilizando en WebSphere MQ.

     Nota: en algunas versiones de Windows (anteriores a XP), es posible que sea necesario cambiar el valor predeterminado del campo **Nombre de cola JMS** si desea emplear la característica de entrega de sucesos predeterminada. Será necesario cambiar el valor de **Nombre de cola JMS** de `WBIC/DeliveryQ` cola `WBIC\\DeliveryQ. WBIC/QCF`.
   - En **Nombre de fábrica JNDI**, especifique el nombre que se utiliza para acceder al archivo de enlaces. El valor predeterminado permite acceder al enlace predeterminado en el sistema de archivos.
   - En **Paquetes de URL del proveedor**, especifique un URL que permita acceder al archivo de enlaces JMS. Este URL debe ser consistente con el nombre de fábrica JNDI. Este campo es opcional y si no se rellena utiliza la ubicación predeterminada del sistema de archivos para los enlaces JMS.
   - En **Juego de caracteres del mensaje**, especifique el juego de caracteres que debe utilizarse cuando se cree el mensaje de bytes en la cola JMS. El valor predeterminado es UTF-8. Este campo sólo es relevante para mensajes de byte.
   - En **URL del proveedor JMS**, especifique el URL del proveedor JMS. Este campo es opcional y si no se rellena utiliza el proveedor JMS predeterminado que se identificó durante la instalación.
5. Pulse **Guardar**.

Especificación de sucesos alertables

Acerca de esta tarea

Cuando se produce un suceso en WebSphere Partner Gateway, se genera un código de suceso. Mediante la página de códigos de suceso, puede establecer el estado alertable del código de suceso. Cuando se establece un suceso como alertable, el suceso aparece en la lista Nombre de suceso de la página Alerta. A continuación, puede establecer una alerta para el suceso.

Para indicar qué sucesos deben ser de alerta:

Procedimiento

1. Pulse **Administración del concentrador > Configuración del concentrador > Códigos de suceso**. Aparece la página Códigos de suceso.
2. Para cada suceso que desee hacer alertable:
   a. Pulse el icono **Ver detalles** junto al código de suceso. Aparece la página Detalles de código de suceso .
   b. Seleccione **Alertable**.
   c. Pulse **Guardar**.

Actualización de un transporte definido por el usuario

Tal como se describe en los apartados Capítulo 7, “Definición de receptores”, en la página 59 y en Capítulo 11, “Creación de destinos”, en la página 223, es posible subir un archivo XML que describa un transporte definido por el usuario. Utilice **Gestionar tipos de transporte** para subir el archivo. Después de subir el archivo XML, el transporte pasa a estar disponible para su utilización al definir un receptor o destino.

El archivo XML que describe el transporte definido por el usuario incluye los atributos del transporte. Estos atributos aparecen (en el apartado **Atributos de transporte personalizado**) en la página del receptor o de destino cuando se especifica un transporte definido por el usuario. Por ejemplo, un transporte definido por el usuario para un destino puede incluir el atributo DestinationRetryCount.

La persona que escribió el archivo XML en el que se describe el transporte puede actualizar los atributos (añadiendo, borrando o modificándolos). Si se modifica el archivo XML, utilice de nuevo **Gestionar tipos de transporte** para subir el archivo. Cualquier cambio en los atributos se refleja en la página de destino o del receptor.

Ejemplos

WebSphere Partner Gateway tiene paquetes con algunos ejemplos, que proporcionan descripciones y funcionalidades personalizadas. Estos paquetes se encuentran en el directorio donde se extrae la instalación de WebSphere Partner Gateway, en las carpetas **DevelopmentKits** e **Integration**.

La carpeta DevelopmentKits contiene los ejemplos siguientes:

- API administrativa: como las API administrativas están en desuso, el programa de utilidad Migración de socios se utiliza para crear y actualizar tareas.
- Migración: contiene ejemplos para Exportar e Importar la configuración.

  - Exportar configuración: muestra el procedimiento para exportar las configuraciones de WebSphere Partner Gateway mediante un componente java desde el archivo de script de la línea de mandatos.
  - Importar configuración: muestra el procedimiento para importar las configuraciones de WebSphere Partner Gateway mediante un componente java desde el archivo de script de la línea de mandatos.
- UserExits: formato de ejemplos para escribir códigos de salida de usuario personalizados para traducción y validación.
  - El ejemplo *EDITransTypeBusinessProcess* proporciona funcionalidad personalizada para documentos EDI que están pasando a través del sistema. Este ejemplo de salida de usuario está diseñado para analizar el Tipo de transacción de EDI desde un documento X12 de EDI. Se pueden extraer otros valores modificando el criterio de análisis.
  - El ejemplo *salida de usuario de traducción personalizada* proporciona funcionalidad de traducción para un documento XML de entrada.
  - El ejemplo *salida de usuario de validación personalizada* proporciona funcionalidad de validación para un documento XML de entrada.
- Casos de ejemplo: formados de ejemplos que proporcionan las directrices para configurar un WebSphere Partner Gateway System para los protocolos mencionados más abajo, sin empaquetado, así como, con empaquetado AS. Para cada protocolo, el archivo de importación de configuración también se proporciona.
  - XML personalizado
  - EDI-X12
  - Documentos binarios

La carpeta Integración contiene los ejemplos de integración siguientes:

- Integración de WebSphere Transformation Extender: ejemplo que muestra la integración con WebSphere Transformation Extender para transformar un documento XML en un archivo sin formato.
- Ejemplo de WebSphere Business Integration Message Broker: ejemplo que muestra cómo WebSphere Partner Gateway se comunica con WebSphere Business Integration Message Broker.
- Integración de WebSphere Process Server: ejemplo que muestra cómo WebSphere Partner Gateway se integra con WebSphere Process Server sobre JMS.
- Integración de WebSphere Interchange Server: ejemplo que muestra cómo WebSphere Partner Gateway se integra con Interchange Server mediante HTTP y JMS.

Capítulo 17. Editor CPP/CPA

El editor CPP/CPA es un plugin de eclipse que ayuda a crear un documento CPP/CPA de una plantilla y permite al usuario para editar en formato tabla. Además, maneja validaciones de datos y esquema.

Prerequisitos:

- Se requiere WID/RAD versión 6.1 o superior
- Coloque el plugin del editor de CPP/A en la carpeta del plugin de IDE

Un documento de Acuerdo de Protocolo de Colaboración (CPA) también se puede crear desde dos documentos de Perfil de Protocolo de Colaboración (CPP). CPP define las funciones de una parte implicada en negocios empresariales con otras partes. CPA describe el acuerdo de intercambio de mensajes entre dos Partes. Para crear un CPP, introduzca los valores para los elementos XML individuales (los elementos XML individuales se componen de diversos atributos) a través de la interfaz de usuario del editor. Una vez se cree el documento CPA mediante el editor y el estado sea "ACORDADO", se puede importar en WebSphere Partner Gateway. Los archivos importados crean automáticamente lo siguiente:

- Socios
- Pasarelas B2B
- Interacciones y conexiones

Aparte de esto, define automáticamente las definiciones de documento y permite las funciones de B2B necesarias.

Puede realizar lo siguiente mediante la interfaz de usuario del editor CPP/CPA:

- "Creación de un documento CPP"
- "Creación de un documento CPA" en la página 316
- "Edición de valores en el editor" en la página 316

Para que el editor CPP/CPA sea el editor predeterminado, realice lo siguiente:

1. En el entorno del plugin de eclipse, pulse el menú **Ventana** y seleccione **Preferencias**
2. En la ventana de preferencia, pulse **General > Editor > Asociaciones de archivo**.
3. Seleccione "*.xml" en la lista **Tipos de archivo** y "Editor multipágina CPPEditor" en la DE **Editores asociados**.
4. Pulse **Predeterminado**.

Creación de un documento CPP

Para crear un documento CPP, realice lo siguiente:

1. En IDE, seleccione **Archivo** >**Nuevo**.
2. En la ventana **Nuevo**, seleccione **CPAEditor** > **Archivo de perfil de protocolo de colaboración**
3. Pulse **Siguiente** e introduzca los valores del poseedor de CPP/CPA.
4. Pulse **Finalizar**. Se crea el archivo nuevo bajo el contenedor especificado.

5. Si ha configurado CPAEditor como predeterminado, modifique los valores en la plantilla. De lo contrario, el archivo se abrirá en un editor XML. Para abrir el archivo en CPAEditor, pulse con el botón derecho y seleccione **Abrir con** > **Editor multipágina CPAEditor**.
6. Introduzca los valores para los atributos de todos los elementos. Para algunos atributos, puede seleccionar el valor apropiado de las diferentes opciones.
7. Pulse **Guardar**. Se muestra un mensaje que confirma la creación correcta de un documento CPP.

Creación de un documento CPA

Debe seleccionar una de las siguientes opciones:

- Caso 1: la creación de un CPA mediante una plantilla permite introducir valores para elementos XML individuales (los elementos XML individuales se componen de diversos atributos) a través de la interfaz de usuario del editor.
- Caso 2: creación de un CPA desde dos CPP.

Para crear un CPA mediante una plantilla, siga estos pasos:

1. En IDE, seleccione **Archivo** >**Nuevo**.
2. En la ventana **Nuevo**, seleccione **CPAEditor** > **Archivo de perfil de acuerdo de colaboración**
3. Pulse **Siguiente** e introduzca los valores del poseedor de CPP/CPA.
4. Pulse **Finalizar**. Se crea el archivo nuevo bajo el contenedor especificado.
5. Si ha configurado CPAEditor como predeterminado, modifique los valores en la plantilla. De lo contrario, el archivo se abrirá en un editor XML. Para abrir el archivo en CPAEditor, pulse con el botón derecho y seleccione **Abrir con** > **Editor multipágina CPPEditor**.
6. Introduzca los valores de los atributos de todos los elementos. Para algunos atributos, puede seleccionar el valor apropiado de las diferentes opciones.
7. Pulse **Guardar**. Se muestra un mensaje que confirma la creación correcta de un documento CPA.

Para crear un CPA de dos CPP, siga estos pasos:

1. En IDE, pulse **Archivo**> **Nuevo** > **Otros**.
2. En la ventana **Nuevo**, seleccione **CPAEditor** > **Fusionar perfiles de protocolos de colaboración**.
3. Pulse **Siguiente**
4. Introduzca los valores del poseedor CPP/CPA y la vía de acceso y nombres de los archivos CPP que desee fusionar.
5. Pulse **Finalizar**. El archivo fusionado se crea en el contenedor específico.
6. Si ha configurado CPAEditor como predeterminado, modifique los valores en la plantilla. De lo contrario, el archivo se abrirá en un editor XML. Para abrir el archivo en CPAEditor, pulse con el botón derecho y seleccione **Abrir con** > **Editor multipágina CPPEditor**.

Edición de valores en el editor

Para editar los valores en la tabla del editor, coloque el cursor en la celda y edite los valores. Cada elemento PartyInfo tiene un único partyName asociado. Los diversos subelementos que hay bajo PartyInfo son PartyId, PartyRef, Rol de colaboración, Certificado, SecurityDetails, DeliveryChannel, Transporte, DocExchange y OverrideMshActionBinding. Estos valores están disponible en

diferentes tabuladores en el editor CPP/CPA. PartyName sirve como identificador único de PartyInfo con el elemento PartyInfo correspondiente.

Por ejemplo, el elemento Certificado que es el subelemento del elemento PartyInfo puede producirse una o más veces. El elemento PartyInfo puede producirse diversas veces en un CPP.

Capítulo 18. Correo electrónico web

Las nuevas características del release del correo electrónico web son una adición al soporte existente de WebSphere Partner Gateway. Esto permite a los socios, clientes y vendedores interactuar con el concentrador utilizando solamente los navegadores soportados, es decir, soporte basado en web para la interacción B2B. La versión web de la consola de WebSphere Partner Gateway se abre en un navegador y no se necesita infraestructura externa, como un servidor FTP, un recurso de correo electrónico, etc. En esta versión de WebSphere Partner Gateway se pueden realizar las siguientes tareas adicionales:

- Subida de documentos para transacciones
- Supervisión del estado de documentos de empresa
- Descarga de los documentos de empresa recibidos

Esta característica es principalmente para socios externos, que no tienen la infraestructura para participar en las transacciones. En este capítulo se detallan los pasos de los requisitos previos necesarios para trabajar con la característica de correo electrónico web.

Nota: Este release sólo soporta documentos del paquete "Ninguno".

Requisitos previos

Para que un socio externo utilice las características del correo electrónico web, el administrador de concentrador debe proporcionar los siguientes permisos:

- "Habilitación del correo electrónico web a nivel de concentrador"
- "Habilitación del correo electrónico web a nivel de socio"
- "Habilitación del destinatario de bandeja web" en la página 320

Habilitación del correo electrónico web a nivel de concentrador

Acerca de esta tarea

Para habilitar permisos para Bandeja de entrada y Bandeja de salida:

1. Vaya a la página **Administración del concentrador** > **Configuración de la consola** > **Permisos**.
2. En la página de la lista **Permiso**, habilite Bandeja de entrada y Bandeja de salida.

Nota: Esta actividad se realiza de una vez para la administración del concentrador.

Habilitación del correo electrónico web a nivel de socio

Acerca de esta tarea

Estos pasos se realizan para un nuevo socio externo:

1. Inicie sesión en la consola como administrador de concentrador.

   Nota: Cuando cree un nuevo socio externo, se creará un grupo de usuarios web automáticamente. Del mismo modo, cuando se instale este parche, se crea un grupo de usuarios web predeterminado para los socios existentes.

2. En la página **Grupos**, pulse el icono de ver permisos del nuevo grupo.
3. Seleccione **Leer / Escribir** para Bandeja de entrada y Bandeja de salida.
4. Cree un nuevo usuario.
5. En la página **Miembros**, asigne el usuario al grupo.

Nota: Esta actividad se realiza de una vez para la administración del concentrador.

Habilitación del destinatario de bandeja web

Acerca de esta tarea

Tras la instalación de la característica de correo electrónico web, el administrador de concentrador debe habilitar el destinatario antes de enviar documentos al socio interno. El estado predeterminado del destinatario de bandeja web es inhabilitado.

Nota: El destinatario de bandeja web es un sistema creado y no se puede suprimir. Los pasos para habilitar el destinatario de bandeja web son los siguientes:

1. Vaya a **Administración del concentrador** > **Destinatarios**.
2. Habilite el destinatario de bandeja web.

Nota: Para modificar el intervalo de sondeo del destinatario de bandeja web edite el atributo de intervalo de sondeo correspondiente.

Limitaciones del correo electrónico web

Las siguientes son las limitaciones del correo electrónico web:

- Se puede enviar un máximo de 10 MB a socios internos.

  Nota: Puede ser más o menos dependiendo de la red, el navegador y la memoria.
- No se puede suprimir el receptor del correo electrónico web.
- No se pueden enviar documentos EDI/XML en formato binario.

Capítulo 19. Ejemplos básicos

En este apéndice se proporcionan ejemplos de la configuración del concentrador. Incluye los siguientes temas:

- " Configuración básica - Intercambio de documentos EDI de paso a través"
- " Configuración básica - Establecimiento de la seguridad para documentos entrantes y salientes" en la página 327
- "Ampliación de la configuración básica" en la página 332

Se proporciona un apéndice separado con ejemplos de cómo realizar intercambios EDI que incluyen acciones de desensobrado, transformación, ensobrado y transmisión de acuse de recibo funcional. Consulte el apartado Capítulo 20, "Ejemplos EDI", en la página 341.

Estos ejemplos tienen como objetivo facilitar una visión general de los pasos necesarios para configurar un sistema. Si está utilizando estos ejemplos para configurar el sistema, modifique la información específica (por ejemplo, nombres e ID de empresa) de modo que se adapten a las necesidades de la empresa.

Configuración básica - Intercambio de documentos EDI de paso a través

En este ejemplo, la configuración del concentrador es bastante sencilla: se definen dos receptores (uno para documentos que llegan al concentrador desde un socio y otro para aquellos documentos que llegan al concentrador desde un sistema de fondo del socio interno). Los intercambios que están configurados en este ejemplo utilizan las definiciones de documento proporcionadas por WebSphere Partner Gateway; por lo tanto, sólo tiene que crear interacciones basadas en dichos flujos. No se utiliza ningún XML personalizado en este ejemplo.

Este ejemplo muestra un intercambio entre una aplicación de fondo del socio interno y un socio externo (Socio dos).

Configuración del concentrador

El primer paso para establecer el concentrador es crear los dos receptores.

- Un receptor HTTP (llamado "HttpReceiver") para recibir documentos mediante HTTP (del Socio dos) que deben enviarse al sistema de fondo del socio interno.
- Un receptor de directorio de archivos (llamado "FileSystemReceiver") para recuperar documentos del sistema de archivos (del sistema de fondo de socio interno) que deben enviarse al Socio dos.

Definición de los receptores

Acerca de esta tarea

Para crear un receptor para la recepción de documentos a través de HTTP:

1. Pulse **Administración del concentrador > Configuración del concentrador > Receptores**.
2. Pulse **Crear destinatario**.
3. En Nombre del receptor, escriba: **HttpReceiver**.
4. En la lista Transporte, seleccione **HTTP/S**.

5. En Modalidad de funcionamiento, utilice el valor predeterminado de **Producción**.
6. En URI, escriba: **/bcgreceiver/submit**
7. Pulse **Guardar**.

A continuación, cree un receptor para que sondee un directorio en el sistema de archivos. La creación de un receptor crea un nuevo directorio de forma automática en el sistema de archivos.

Para crear el receptor de sistema de archivos:

1. Pulse **Administración del concentrador > Configuración del concentrador > Receptores**.
2. Pulse **Crear destinatario**.
3. En Nombre del receptor, escriba: **FileSystemReceiver**.
4. En la lista Transporte, seleccione **Directorio de archivos**.
5. En Modalidad de funcionamiento predeterminada, utilice el valor predeterminado de **Producción**.
6. En Vía de acceso raíz de documento, escriba: **\temp\FileSystemReceiver**

   Nota: esto creará un directorio FileSystemReceiver dentro del directorio temp. Asegúrese de que en el sistema de archivos haya un directorio temp.
7. Pulse **Guardar**.

Definición de tipos de documentos e interacciones

Acerca de esta tarea

En este ejemplo, se va a configurar el intercambio de documentos que cumplen con el estándar EDI-X12. En este ejemplo, los documentos simplemente pasan por el concentrador. El intercambio EDI no se desensobra y no se produce ninguna transformación. Consulte el Capítulo 23, “Atributos”, en la página 435 para obtener ejemplos de cómo desensobrar un intercambio, transformar las transacciones y enviar acuses de recibo.

En este apartado, se describen los siguientes intercambios:

- Envío de un documento EDI-X12, sin empaquetado, desde el socio interno al Socio Dos
- Envío de un documento EDI-X12, empaquetado en AS2, desde el Socio Dos al socio interno

Debido al empaquetamiento y protocolos implicados, no es necesario crear una nueva definición de documento. Los paquetes, protocolos y tipos de documentos son aquellos predefinidos en el sistema.

No obstante, sí necesitará definir las interacciones basadas en estos tipos de documentos predefinidos.

Cree la primera interacción, en la que el origen es un documento con formato ISA que cumple el estándar EDI-X12 sin empaquetado y el destino es un documento con formato ISA que cumple el estándar EDI-X12 con empaquetado AS.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. En la columna **Origen**, expanda:

a. **Paquete: Ninguno**
b. **Protocolo: EDI-X12**

4. Pulse **Tipo de documento: ISA**
5. En la columna **Destino**, expanda:
   a. **Paquete: AS**
   b. **Protocolo: EDI-X12**
6. Pulse **Tipo de documento: ISA**
7. En la lista **Acción**, seleccione **Paso a través**.
8. Pulse **Guardar**.

Cree una segunda interacción, en la que el formato origen es un documento con formato ISA que cumple el estándar EDI-X12 con empaquetado AS y el formato destino es un documento con formato ISA que cumple el estándar EDI-X12 sin empaquetado:

1. Pulse **Crear interacción**.
2. En la columna **Origen**, expanda:
   a. **Paquete:AS**
   b. **Protocolo: EDI-X12**
3. Pulse **Tipo de documento: ISA**
4. En la columna **Destino**, expanda:
   a. **Paquete:Ninguno**
   b. **Protocolo: EDI-X12**
5. Pulse **Tipo de documento:ISA**
6. En la lista **Acción**, seleccione **Paso a través**.
7. Pulse **Guardar**.

Creación de socios y conexiones de socios

En este ejemplo, se creará un socio externo, además del socio interno. Los destinos de los socios incluyen transportes estándares y no se definen puntos de configuración para los destinos.

Creación de socios

Cree dos nuevos socios. Para definir el socio interno:

1. Pulse **Administración de cuentas** en el menú principal. La página Búsqueda de socios es la vista predeterminada.
2. Pulse **Crear**.
3. En **Nombre de inicio de sesión de empresa**, escriba: **CommMan**.
4. En **Nombre de visualización de socio**, escriba: **Comm Man**.
5. En **Tipo de socio**, seleccione **Socio interno**.
6. Pulse **Nuevo** bajo **ID de empresa**.
7. En **Tipo**, deje **DUNS** y especifique **123456789** como Identificador.

   Nota: aquí y en toda esta publicación, los números DUNS sólo se proporcionan como ejemplos.
8. Pulse **Nuevo** bajo **ID de empresa**.
9. Seleccione **Formato libre** y especifique un valor de **12-3456789** como identificador

10. Pulse **Guardar**.

Para definir el Socio Dos:

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Crear**.
3. En **Nombre de inicio de sesión de empresa**, escriba: **partnerTwo**
4. En **Nombre de visualización de socio**, escriba: **Socio dos**
5. En **Tipo de socio**, seleccione **Socio externo.**
6. Pulse **Nuevo** bajo **ID de empresa**.
7. En **Tipo**, deje **DUNS** y especifique **987654321** como Identificador.
8. Pulse **Nuevo** bajo **ID de empresa**.
9. Seleccione **Formato libre** y especifique el valor **98-7654321** como identificador.
10. Pulse **Guardar**.

Acaba de definir el socio interno y el Socio Dos en el concentrador.

Los siguientes pasos sirven para configurar los destinos para el socio interno y el Socio dos.

Creación de destinos

Acerca de esta tarea

Antes de crear un destino de directorio de archivos para el socio interno, deberá crear la estructura de directorios utilizada por este destino. Cree un nuevo directorio FileSystemDestination en la unidad raíz. Este directorio será utilizado por el socio interno para almacenar archivos recibidos de socios externos.

En el caso del socio interno, el destino representa el punto de entrada al sistema de fondo.

Para crear un destino para el socio interno:

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Buscar**.
3. Seleccione **Socio interno** pulsando el icono **Ver detalles**.
4. Pulse **Destinos** en la barra de navegación horizontal.
5. Pulse **Crear**.
6. En **Nombre de destino**, escriba: **FileSystemDestination**.
7. En **Transporte**, seleccione **Directorio de archivos**.
8. En **Dirección**, escriba: **file://C:\FileSystemDestination**.
9. Pulse **Guardar**.

A continuación, establezca este destino recién creado como el destino predeterminado para el socio interno.

1. Pulse **Lista** para ver todos los destinos configurados para el socio interno.
2. Pulse **Ver destinos predeterminados**.
3. En la lista **Producción**, seleccione **FileSystemDestination**.
4. Pulse **Guardar**.

Cree un destino para Socio dos

1. Pulse **Administración de cuentas > Perfiles>**.

2. Pulse **Buscar** y luego seleccione **Socio Dos** pulsando el icono **Ver detalles**.
3. Pulse **Destinos** en la barra de navegación horizontal.
4. Pulse **Crear**.
5. En **Nombre de destino**, escriba: **HttpDestination**.
6. En **Transporte**, seleccione **HTTP/1.1**.
7. En **Dirección**, escriba: **http://<***dirección_IP***>:80/input/AS2**, donde <*dirección_IP*> representa el sistema del Socio Dos.
8. En **Nombre de usuario**, escriba: **Comm Man**.
9. En **Contraseña**, escriba: **commMan**.
10. Pulse **Guardar**.

Tenga en cuenta que este ejemplo asume que Socio dos requiere un nombre de usuario y una contraseña para cualquier socio que inicie sesión en su sistema.

De nuevo, necesitará definir un destino predeterminado para este socio.

1. Pulse **Lista** seguido de **Ver destinos predeterminados**.
2. En la lista **Producción**, seleccione **HttpDestination**.
3. Pulse **Guardar**.

Configuración de posibilidades B2B

Acerca de esta tarea

A continuación defina las funciones B2B para el socio interno.

1. En el menú principal, pulse **Administración de cuentas > Perfiles > Socio**.
2. Pulse **Buscar**.
3. Seleccione **Socio interno** pulsando el icono **Ver detalles**.
4. Pulse **Funciones B2B** en la barra de navegación horizontal.
5. Establezca el origen y el destino del paquete: Ninguno, Protocolo: EDI-X12 y Tipo de documento: ISA llevando a cabo los siguientes pasos:
   a. Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: Ninguno**
   b. Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno**
   c. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**.
   d. Pulse el icono **El rol no está activo** para **Protocolo: EDI-X12 (ALL)** tanto para origen como para destino.
   e. Pulse el icono **Expandir** situado junto a **Protocolo: EDI-X12 (ALL)**.
   f. Pulse el icono **El rol no está activo** para **Tipo de documento: ISA** para el origen y el destino.

A continuación, establezca las funciones B2B para el Socio Dos.

Procedimiento

1. En el menú principal, pulse **Administración de cuentas > Perfiles > Socio**.
2. Pulse **Buscar**.
3. Seleccione Socio Dos pulsando el icono **Ver detalles**.
4. Pulse **Funciones B2B** en la barra de navegación horizontal.

5. Seleccione Establecer origen y Establecer destino para Paquete: AS, Protocolo: EDI-X12 y Flujo de documentos: ISA; para ello, lleve a cabo los pasos siguientes:
   a. Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: AS**
   b. Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: AS**
   c. Pulse el icono **Expandir** situado junto a **Paquete: AS**.
   d. Pulse el icono **El rol no está activo** para **Protocolo: EDI-X12 (ALL)** tanto para origen como para destino.
   e. Pulse el icono **Expandir** situado junto a **Protocolo: EDI-X12 (ALL)**.
   f. Pulse el icono **El rol no está activo** para **Tipo de documento: ISA** para el origen y el destino.

Definición de conexiones de socio

Acerca de esta tarea

Defina la conexión de socio para documentos EDI sin empaquetado que procedan del socio interno para ser enviados al Socio dos.

1. Pulse **Administración de cuentas > Conexiones**.
2. En la lista **Origen**, seleccione **Socio interno**.
3. En la lista **Destino**, seleccione **Socio Dos**.
4. Pulse **Buscar**.
5. Pulse **Activar** para la conexión con la información siguiente:
   a. **Origen**
      1) Paquete: **Ninguno (N/D)**
      2) Protocolo: **EDI-X12 (ALL)**
      3) Tipo de documento: **ISA(ALL)**
   b. **Destino**
      1) Paquete: **AS (N/D)**
      2) Protocolo: **EDI-X12 (ALL)**
      3) Tipo de documento: **ISA(ALL)**

A continuación, defina la conexión para los documentos EDI empaquetados en AS2 que el Socio dos envía al socio interno sin empaquetado. Es muy similar a la conexión definida en el apartado anterior, excepto que también configurará atributos AS2.

1. Pulse **Administración de cuentas > Conexiones**.
2. En la lista **Origen**, seleccione **Socio Dos**.
3. En la lista **Destino**, seleccione **Socio interno**.
4. Pulse **Buscar**.
5. Pulse **Activar** para la conexión con la información siguiente:
   a. **Origen**
      1) Paquete: **AS (N/D)**
      2) Protocolo: **EDI-X12 (ALL)**
      3) Tipo de documento: **ISA(ALL)**
   b. **Destino**
      1) Paquete: **Ninguno (N/D)**
      2) Protocolo: **EDI-X12 (ALL)**

3) Tipo de documento: **ISA(ALL)**

A continuación, seleccione Atributos situado junto al recuadro **Paquete: AS (N/D)** del Socio Dos.

1. Edite los atributos del paquete: AS (N\D) desplazándose por la página y pulsando el icono **Expandir** situado junto a **Paquete: AS (N/D)**.
2. Especifique un valor en Dirección de correo electrónico de MDN de AS (AS1). Puede ser cualquier dirección de correo electrónico.
3. Especifique un valor en el URL de HTTP de MDN de AS (AS2). Especifíquelo de la manera siguiente: **http://<***dirección_IP***>:57080/bcgreceiver/submit,** donde <*dirección_IP*> es el concentrador.
4. Pulse **Guardar**.

Configuración básica - Establecimiento de la seguridad para documentos entrantes y salientes

En este apartado aprenderá a añadir los siguientes tipos de seguridad a la configuración básica:

- Autenticación de servidor SSL (Capa de sockets protegidos)
- Cifrado
- Firmas digitales

Establecimiento de la autenticación SSL para documentos entrantes

Acerca de esta tarea

En este apartado, utilice iKeyman para configurar la autenticación del servidor de modo que el Socio Dos pueda enviar documentos AS2 mediante HTTPS.

Para configurar la autenticación del servidor, realice los pasos siguientes:

1. Inicie la aplicación iKeyman; para ello, abra el archivo iKeyman.bat en el directorio /<*DirProducto*>/was/bin.
2. Abra el almacén de claves predeterminadas del Receptor, bcgSecurity.jks. En la barra de menús, seleccione la opción **Abrir archivo de base de datos de claves**. En una instalación predeterminada, bcgSecurity.jks está ubicado en el directorio: <*DirProducto*>/common/security/keystore
3. Cuando el sistema se lo solicite, especifique la contraseña predeterminada de bcgSecurity.jks. La contraseña es WebAS.
4. Si es la primera vez que abre el archivo bcgSecurity.jks, elimine el certificado “ficticio”.

El paso siguiente es crear un certificado autofirmado. Al crear un certificado personal autofirmado, se crea una clave privada y una pública dentro del archivo de almacén de claves del servidor.

Para crear un certificado autofirmado:

1. Pulse **New Self Signed** (Nuevo certificado autofirmado).
2. Dé al certificado una etiqueta clave para identificar de forma exclusiva el certificado dentro del almacén de claves. Utilice la etiqueta **selfSignedCert**.

3. Especifique el nombre común del servidor. Ésta es la identidad principal y universal del certificado. Debe identificar de forma exclusiva el valor principal que representa.
4. Especifique el nombre de la organización.
5. Acepte todos los otros valores predeterminados y pulse **Aceptar**.

Presuponga que el Socio Dos desea enviar un mensaje EDI en AS2 mediante HTTP seguro. Para ello, el Socio Dos necesitará hacer referencia al certificado público (que se ha creado como parte de la creación del certificado autofirmado).

Para permitir que el Socio Dos utilice el certificado público, exporte el certificado público del archivo de almacenamiento de claves del servidor, como se explica a continuación:

1. Seleccione el certificado autofirmado recién creado en el programa de utilidad IBM Key Management.
2. Pulse **Extract Certificate** (Extraer certificado).
3. Cambie el tipo de datos por **Binary DER**.
4. Proporcione el nombre de archivo **commManPublic** y pulse **Aceptar**.

Por último, utilice la herramienta iKeyman para exportar el par de certificado autofirmado y clave privada con el formato de un archivo PKCS12. Este archivo PCKS12 se utilizará para cifrado, que se describe en un apartado posterior.

Para exportar el par certificado autofirmado y clave privada:

1. Pulse **Exportar/Importar**.
2. Cambie el tipo de archivo de claves a **PKCS12**.
3. Proporcione el nombre de archivo **commManPrivate** y pulse **Aceptar**.
4. Especifique una contraseña para proteger el archivo PKCS12 destino. Confirme la contraseña y pulse **Aceptar**.

Nota: detenga y reinicie el receptor para que estos cambios surtan efecto.

La contraseña especificada se utilizará más tarde al importar este certificado privado en el concentrador.

El Socio Dos debe realizar pasos de configuración, como importar el certificado y cambiar la dirección por aquella adonde envía los documentos AS2. Por ejemplo, el Socio Dos debe cambiar la dirección por:

`https://<dirección_IP>:57443/bcgreceiver/submit`

donde *<dirección_IP>* se refiere al concentrador.

Acto seguido, el certificado autofirmado que se ha colocado en el almacén de claves predeterminadas del receptor se presenta al Socio Dos siempre que éste envía un documento mediante HTTP seguro.

Para configurar la situación inversa, el Socio Dos debe proporcionar al concentrador una clave SSL con el formato de un archivo .der (es este caso, partnerTwoSSL.der). Si fuera necesario, el Socio Dos debe cambiar también la configuración para permitir la recepción de documentos mediante transporte HTTPS.

Cargue el archivo del Socio Dos, partnerTwoSSL.der, en el perfil del operador de concentrador como certificado raíz. Un certificado raíz es un certificado emitido desde una autoridad certificadora (CA) que se utiliza al establecer una cadena de certificados. En este ejemplo, el Socio Dos ha generado el certificado, que se carga como un certificado raíz para permitir al concentrador reconocer al remitente y confiar en él.

Cargue partnerTwoSSL.der en el concentrador:

1. En el menú principal, pulse **Administración de cuentas > Perfiles > Socio**.
2. Pulse **Buscar**.
3. Seleccione **Operador de concentrador** seleccionando el icono **Ver detalles**.
4. Pulse **Certificados** y, a continuación, **Cargar certificado**.
5. Establezca el **Tipo de certificado** como **Certificado raíz e intermedio**.
6. Cambie la descripción por **Certificado SSL de Socio Dos**.
7. Establezca el campo **Estado** en **Habilitado**.
8. Pulse **Examinar** y vaya al directorio en el que ha guardado partnerTwoSSL.der.
9. Seleccione el certificado y pulse **Abrir**.
10. Pulse **Subir** y, a continuación, **Guardar**.

Cambie el destino del Socio dos para que utilice HTTP seguro.

1. Pulse **Administración de cuentas > Perfiles > Socio** en la barra de navegación horizontal.
2. Pulse **Buscar** y seleccione Socio Dos pulsando el icono **Ver detalles**.
3. Pulse **Destinos** en la barra de navegación horizontal. A continuación, seleccione HttpDestination pulsando el icono **Ver detalles**.
4. Edítelo pulsando el icono **Editar**.
5. Cambie el valor del transporte a **HTTPS/1.1**
6. Cambie el valor de la dirección como se indica a continuación: **https://<***dirección_IP***>:443/input/AS2**, donde *<dirección_IP>* se refiere a la máquina del Socio Dos.
7. No es necesario modificar el resto de valores. Pulse **Guardar**.

Establecimiento del cifrado

Acerca de esta tarea

En este apartado se proporcionan instrucciones para configurar el cifrado.

El Socio Dos debe realizar los pasos de configuración necesarios (por ejemplo, importar el certificado público y el certificado autofirmado) y configurar el cifrado en documentos enviados al concentrador.

WebSphere Partner Gateway utilizará su clave privada para descifrar documentos. Para ello, primero debe cargar la clave privada extraída desde el certificado autofirmado a la Consola de comunidad. Realice esta tarea una vez que ha iniciado sesión en la Consola de comunidad como operador de concentrador e instale el certificado en su propio perfil.

Para cargar el archivo PKCS12:

1. Pulse **Administración de cuentas > Perfiles > Socio** en la barra de navegación horizontal.

2. Pulse **Buscar**.
3. Seleccione **Operador de concentrador** pulsando el icono **Ver detalles**.
4. Pulse **Certificados** y, a continuación, **Cargar PKCS12**.
5. Seleccione el recuadro de selección que hay a la izquierda de **Cifrado**.
6. Cambie la descripción por **CommManPrivate**.
7. Seleccione **Habilitado**.
8. Pulse **Examinar** y vaya al directorio en el que se encuentra el archivo PKCS12, commManPrivate.p12.
9. Seleccione el archivo y pulse **Abrir**.
10. Especifique la contraseña proporcionada para el archivo PKCS12.
11. Deje la Modalidad de funcionamiento como **Producción**.
12. Pulse **Subir** y, a continuación, **Guardar**.

Esto completa la configuración necesaria para permitir que un socio envíe transacciones cifradas mediante HTTP seguro al concentrador.

En el apartado siguiente, el procedimiento anterior se invierte: el concentrador envía una transacción EDI cifrada mediante HTTP seguro.

El Socio Dos debe generar un documento de par de claves de descifrado (en este ejemplo, partnerTwoDecrypt.der) y poner el certificado público a disposición del concentrador.

Como se ha mencionado anteriormente, la clave pública será utilizada por el concentrador al cifrar las transacciones que se envíen al socio. Para ello, primero debe cargar el certificado público en el concentrador.

Procedimiento

1. En el menú principal, pulse **Administración de cuentas > Perfiles > Socio**.
2. Pulse **Buscar**.
3. Seleccione Socio Dos pulsando el icono **Ver detalles**.
4. Pulse **Certificados** en la barra de navegación horizontal.
5. Pulse **Cargar certificado**.
6. Seleccione el recuadro de selección situado junto **Cifrado**.
7. Cambie la descripción por **Descifrado de Socio Dos**.
8. Establezca el estado en **Habilitado**.
9. Pulse **Examinar**.
10. Vaya al directorio en el que se ha almacenado el certificado de descifrado, partnerTwoDecrypt.der.
11. Seleccione el certificado y pulse **Abrir**.
12. Deje la Modalidad de funcionamiento como **Producción**
13. Pulse **Subir** y, a continuación, **Guardar**.

Resultados

El último paso en la configuración del concentrador para que envíe mensajes cifrados a través de HTTP seguro utilizando AS2 es modificar la conexión del socio que existe entre el socio interno y el Socio dos.

Para modificar la conexión del socio desde la Consola de comunidad:

1. Pulse **Administración de cuentas > Conexiones** en la barra de navegación horizontal.
2. En la lista **Origen**, seleccione **Comm Man**.
3. En la lista **Destino**, seleccione **Socio Dos**.
4. Pulse **Buscar**.
5. Pulse el botón **Atributos** correspondiente a Destino.
6. En el resumen de conexión, observe que el atributo **AS cifrado** tiene un valor actual de **No**. Edite este valor pulsando el icono **Expandir** junto a **Paquete: AS (N/D)**.

   Nota: para ver esta opción, es necesario desplazarse por la página hacia abajo.
7. En la lista, actualice el atributo **AS cifrado** con el valor **Sí** y pulse **Guardar**.

Establecimiento de firmas de documentos

Acerca de esta tarea

Al firmar digitalmente una transacción o un mensaje, WebSphere Partner Gateway utiliza la clave privada para crear la firma y firmar. El socio que recibe el mensaje utiliza la clave pública para validar la firma. WebSphere Partner Gateway utiliza firmas digitales a este efecto.

Este apartado proporciona los pasos necesarios para configurar el concentrador y el socio para que puedan utilizar firmas digitales.

El Socio Dos debe realizar los pasos de configuración necesarios (por ejemplo, crear un documento autofirmado llamado, en este caso, partnerTwoSigning.der) y configurar la firma de documentos. El Socio Dos debe poner partnerTwoSigning.der a disposición del concentrador.

Para cargar el certificado digital en el concentrador:

1. Pulse **Administración de cuentas > Perfiles > Socio** en la barra de navegación horizontal.
2. Pulse **Buscar**.
3. Seleccione Socio Dos pulsando el icono **Ver detalles**.
4. Elija **Certificados** en la barra de navegación horizontal.
5. Pulse **Cargar certificado**.
6. Seleccione el recuadro de selección que hay junto a **Firma digital**.
7. Cambie la descripción por **Comm Man Signing**.
8. Establezca el campo **Estado** en **Habilitado**.
9. Pulse **Examinar**.
10. Vaya al directorio que contiene el certificado digital, partnerTwoSigning.der, selecciónelo y pulse **Abrir**.
11. Pulse **Subir** y, a continuación, **Guardar**.

Esto completa la configuración inicial de firmas digitales.

El socio utiliza el certificado público para autenticar transacciones firmadas enviadas al concentrador.

El concentrador utilizará la clave privada para firmar digitalmente las transacciones salientes que se envíen al socio. Habilite primero la clave privada para firma digital.

Para habilitar la clave privada para firma digital:

1. Pulse **Administración de cuentas > Certificados > Socio** en la barra de navegación horizontal.
2. Pulse el icono **Ver detalles** situado junto a **Operador de concentrador**.
3. Pulse el icono **Ver detalles** situado junto a **Comm ManPrivate**.

   Nota: éste es el certificado privado cargado en el concentrador previamente.
4. Pulse el icono **Editar**.
5. Seleccione el recuadro de selección que hay junto a **Firma digital**.

   Nota: si hay más de un certificado de firma digital, debe seleccionar cual es el primario y cual es el secundario seleccionando **Primario** o **Secundario** en la lista **Utilización de certificado**.
6. Pulse **Guardar**.

A continuación, modifique los atributos de la conexión de socio existente entre el socio interno y el Socio dos para albergar AS2 firmado.

Para modificar los atributos de la conexión de socio:

1. Pulse **Administración de cuentas > Conexiones** en la barra de navegación horizontal.
2. Seleccione **Socio interno** en la lista **Origen**.
3. Seleccione **Socio Dos** en la lista **Destino**.
4. Pulse **Buscar**.
5. Pulse el botón **Atributos** correspondiente Socio Dos.
6. Edite el atributo **AS firmada** pulsando el icono **Expandir** junto a **Paquete: AS (N/D)**.
7. Seleccione **Sí** en la lista **AS firmada**.
8. Pulse **Guardar**.

Esto completa la configuración necesaria para enviar una transacción AS2 firmada desde WebSphere Partner Gateway al socio.

Ampliación de la configuración básica

En este apartado se muestra cómo modificar la configuración básica descrita en este apéndice. Utilizando los mismos socios y configuración descritos anteriormente (un socio interno, utilizando un ID de DUNS de 123456789 y un destino de directorio de archivos y un socio llamado SocioDos con un ID de DUNS de 987654321 y un destino HTTP), este apartado describe cómo añadir soporte para:

- Transporte FTP
- Documentos XML personalizados
- Archivos binarios (sin empaquetado)

Creación de un receptor FTP

Acerca de esta tarea

El receptor FTP recibe los archivos y los pasa al Gestor de documentos para que los procese. Como se describe en el apartado "Configuración del servidor FTP para la recepción de documentos" en la página 35, antes de poder crear un receptor FTP, deberá tener un servidor FTP instalado y deberá haber creado un directorio FTP y configurado el servidor FTP.

En este ejemplo, se presupone que el servidor FTP se ha configurado para el Socio Dos y que el directorio raíz es c:/ftproot.

1. Pulse **Administración del concentrador > Configuración del concentrador > Receptores**.
2. Pulse **Crear destinatario**.
3. Especifique la información siguiente:
   a. Nombre de receptor: **FTP_Receptor**
   b. Transporte: **Directorio FTP**
   c. Directorio raíz de FTP: **C:/ftproot**
4. Pulse **Guardar**.

Establecimiento del concentrador para la recepción de archivos binarios

En este apartado se describen los pasos necesarios para configurar el concentrador de modo que reciba documentos binarios que el Socio Dos envíe al socio interno.

Creación de una interacción para documentos binarios

Acerca de esta tarea

De manera predeterminada, WebSphere Partner Gateway proporciona cuatro interacciones que incluyen documentos binarios. No obstante, no proporciona una interacción para documentos binarios empaquetados como Ninguno dirigidos a un socio con el documento también empaquetado como Ninguno. En este apartado creará la interacción necesaria para permitir que documentos binarios pasen a través del sistema.

Procedimiento

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Pulse **Crear** en la vista **Gestionar interacción**.
4. En **Origen** seleccione: **Paquete: Ninguno Protocolo: Binario (1.0) Tipo de documento: Binario (1.0)**.
5. En **Destino** seleccione: **Paquete: Ninguno Protocolo: Binario (1.0) Tipo de documento: Binario (1.0)**.
6. De forma opcional, seleccione la correlación **Transformación**.
7. En la lista **Acción**, seleccione **Paso a través**.
8. Pulse **Guardar**.

Actualización de posibilidades B2B para el socio interno

Acerca de esta tarea

En este apartado se muestra cómo configurar el socio interno para poder aceptar documentos binarios.

Procedimiento

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Buscar**.
3. Pulse el icono **Ver detalles** situado junto a **Comm Man**.
4. Pulse **Posibilidades B2B**.
5. Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.
6. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**.
7. Pulse el icono **El rol no está activo** para **Protocolo: Binario (1.0)** debajo de **Establecer destino**.
8. Pulse el icono **Expandir** situado junto a **Protocolo: Binario (1.0)**.
9. Finalmente, pulse el icono **El rol no está activo** para **Tipo de documento: Binario (1.0)** en **Establecer destino**.

Actualización de funciones B2B para el Socio Dos

Acerca de esta tarea

En este apartado se muestra cómo configurar el Socio Dos para poder enviar documentos binarios.

Procedimiento

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Buscar**.
3. Pulse el icono **Ver detalles** situado junto al Socio Dos.
4. Pulse **Posibilidades B2B**.
5. Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: Ninguno** para habilitarlo.
6. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**.
7. Pulse el icono **El rol no está activo** para **Protocolo: Binario (1.0)** debajo de **Establecer origen**.
8. Pulse el icono **Expandir** situado junto a **Protocolo: Binario (1.0)**.
9. Finalmente, pulse el icono **El rol no está activo** para **Tipo de documento: Binario (1.0)** en **Establecer origen**.

Creación de una nueva conexión de socio

Acerca de esta tarea

Este apartado muestra cómo configurar una nueva conexión de socios entre el socio interno y el Socio dos para documentos binarios.

Procedimiento

1. Pulse **Administración de cuentas > Conexiones**.
2. Seleccione **Socio Dos** en la lista **Origen**.
3. Seleccione **Socio interno** en la lista **Destino**.

4. Pulse **Buscar**.
5. Busque la conexión **Ninguno (N/D), Binario (1.0), Binario (1.0)** para **Ninguno (N/D), Binario (1.0), Binario (1.0)** y pulse **Activar** para activarla.

Establecimiento del concentrador para documentos XML personalizados

Tal como se describe en el apartado "Proceso de documentos de XML personalizado" en la página 159, debe configurar el concentrador para poder direccionar archivos XML personalizados. En este apartado se describen los pasos necesarios para configurar el Gestor de documentos de modo que pueda direccionar el documento XML siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Tester>
<Tester type="Test type A">
    <From>987654321</From>
    <To>123456789</To>
</Tester>
```

En este ejemplo, el Gestor de documentos utiliza el distintivo de directorio raíz para identificar el tipo de documento XML. Extrae los valores de los campos De y A para identificar el identificador de empresa Socio de origen y el identificador de empresa Socio de destino.

Creación de un formato de definición de protocolo CustomXML

Acerca de esta tarea

El primer paso es crear un protocolo nuevo para el XML personalizado que va a intercambiar.

Procedimiento

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse **Crear definición de documento**.
3. Seleccione **Protocolo** en la lista **Tipo de definición de documentos**.
4. Especifique la información siguiente:
   a. Código: **XML personalizado**
   b. Versión: **1.0**
   c. Descripción: **Definición de protocolo de ejemplo**
5. Establezca **Nivel de documento** en **No**.
6. Establezca **Estado** en **Habilitado**.
7. Establezca **Visibilidad: Administración del concentrador** en **Sí**.
8. Establezca **Visibilidad: Socio interno** en **Sí**.
9. Establezca **Visibilidad: Socio** en **Sí**.
10. Seleccione:
    a. Paquete: **AS**
    b. Paquete: **Ninguno**
    c. Paquete: **Integración de programas de fondo**.
11. Pulse **Guardar**.

Creación de una definición de documento Tester_XML

Acerca de esta tarea

El segundo paso es crear una definición de documento para el nuevo protocolo.

Procedimiento

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse **Crear definición de documento**.
3. Seleccione **Tipo de documento** en la lista **Tipo de definición de documento**.
4. Especifique la información siguiente:
   a. Nombre: **Tester_XML**
   b. Versión: **1.0**
   c. Descripción: **Ejemplo de tipo de documento XML personalizado**
5. Establezca **Nivel de documento** en **Sí**.
6. Establezca **Estado** en **Habilitado**.
7. Establezca **Visibilidad: Administración del concentrador** en **Sí**.
8. Establezca **Visibilidad: Socio interno** en **Sí**.
9. Establezca **Visibilidad: Socio** en **Sí**.
10. Pulse el icono **Expandir** situado junto a **Paquete: AS** y seleccione **Protocolo: CustomXML**.
11. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno** y seleccione **Protocolo: CustomXML**.
12. Pulse el icono **Expandir** situado junto a **Paquete: integración de fondo** y seleccione **Protocolo: CustomXML**.
13. Pulse **Guardar**.

Creación del formato Tester_XML

Acerca de esta tarea

Por último, debe crear el formato XML asociado con el protocolo nuevo.

Procedimiento

1. Pulse **Administración del concentrador > Configuración del concentrador > Formatos XML**.
2. Pulse **Crear familia de documentos**.
3. Especifique o seleccione la siguiente información:
   a. Nombre de familia: **Familia de ejemplo**
   b. Protocolo: **XML 1.0 personalizado**
   c. Tipo de familia: **Distintivo raíz**
   d. Opción de archivo grande: **Ninguno**
   e. Identificador de familia: **Tester**
4. Pulse **Guardar**.
5. En la página resultante Familia de documentos, pulse **Crear formato XML**.
6. En la lista Tipo de documento, seleccione **Tester_XML**.
7. Para el valor Identificador de formato, especifique **Test type A**.
8. Para la Expresión XPath para el identificador de formato, especifique **/Tester/@type**.

9. Deje en blanco el campo Espacio de nombres de prefijo (no se utiliza ningún espacio de nombres en el documento) y el Tipo de retorno como **Texto**.
10. Especifique **1** en el campo del valor Versión de formato y el campo Expresión XPath. Cambie el Tipo de retorno a **Constante**. Esto quiere decir que todos los documentos que tienen el Identificador de formato "Tester" tendrán la versión correcta para una coincidencia con este formato. Esto se debe a que la versión de todos los documentos será 1 y la versión de este formato es también 1. Por lo tanto, la versión siempre coincide.
11. Especifique **/Tester/From** como Expresión de XPath para el Identificador de empresa de origen.
12. Especifique **/Tester/To** como Expresión de XPath para el identificador de empresa de destino.
13. Deje los restantes campos en el formato tal y como están. Son opcionales y no se utilizan en este ejemplo.
14. Pulse **Guardar**.

Creación de una interacción para documentos Tester_XML

Acerca de esta tarea

Ahora tiene un nuevo protocolo y un tipo de documento con el que configurar una interacción.

Procedimiento

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacción**.
2. En la pantalla **Gestionar interacción**, pulse **Crear interacción**.
3. En **Origen**, seleccione:
   a. Paquete: **Ninguno**
   b. Protocolo: **XML (1.0) personalizado**
   c. Tipo de documento: **Tester_XML (1.0)**.
4. En **Destino**, seleccione:
   a. Paquete: **Ninguno**
   b. Protocolo: **XML (1.0) personalizado**
   c. Tipo de documento: **Tester_XML (1.0)**.
5. En la lista **Acción**, seleccione **Paso a través**.
6. Pulse **Guardar**.

Actualización de posibilidades B2B para el socio interno

Acerca de esta tarea

Para habilitar el intercambio del documento XML personalizado, deberá actualizar las funciones B2B de los socios.

Primero, habilite el Socio interno para que reciba (o sea el destino de) documentos Tester_XML.

Procedimiento

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Buscar**.

3. Seleccione el Socio interno de la lista de socios. (Tenga en cuenta que este ejemplo asume que el Socio interno tiene el identificador de empresa de 123456789.)
4. Pulse **Posibilidades B2B**.
5. Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.
6. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**.
7. Pulse el icono **El rol no está activo** para **Protocolo: XML (1.0) personalizado** para **Establecer destino**.
8. Pulse el icono **Expandir** junto al **Protocolo: XML (1.0) personalizado** .
9. Finalmente, pulse el icono **El rol no está activo** para **Tipo de documento: Tester_XML (1.0)** para **Establecer destino**.

Actualización de funciones B2B para el Socio Dos

Acerca de esta tarea

Actualice las funciones B2B del Socio dos para habilitar el intercambio de mensajes utilizando el nuevo formato XML personalizado.

Habilite Socio dos para que sea el origen de los documentos Tester_XML. (Tenga en cuenta que el ejemplo asume que Socio dos tiene un identificador de empresa de 987654321.)

Procedimiento

1. Pulse **Administración de cuentas > Perfiles>**.
2. Pulse **Buscar**.
3. Seleccione **Socio dos** en la lista de socios. (Tenga en cuenta que este ejemplo asume que Socio dos tiene el identificador de empresa de 987654321.)
4. Pulse **Posibilidades B2B**.
5. Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: Ninguno** para habilitarlo.
6. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**.
7. Pulse el icono **El rol no está activo** para **Protocolo: XML (1.0) personalizado** para **Establecer origen**.
8. Pulse el icono **Expandir** junto al **Protocolo: XML (1.0) personalizado** .
9. Finalmente, pulse el icono **El rol no está activo** para **Tipo de documento: Tester_XML (1.0)** para **Establecer origen**.

Creación de una nueva conexión de socio

Acerca de esta tarea

Finalmente, cree una nueva conexión de socio.

Procedimiento

1. Pulse **Administración de cuentas > Conexiones.**
2. Seleccione **Socio Dos** en la lista **Origen**.
3. Seleccione **Socio interno** en la lista **Destino**.
4. Pulse **Buscar**.
5. Busque la conexión **Ninguno (N/A), XML (1.0) personalizado, Tester_XML (1.0)**a **Ninguno (N/A), XML (1.0) personalizado, Tester_XML (1.0)** y pulse **Activar** para activarla.

Direccionamiento de un documento utilizando XML personalizado

Copie el XML de ejemplo en la parte inicial de este ejemplo y péguelo en un editor de texto. Guarde el archivo en el sistema con un nombre de su elección. A continuación, envíe el archivo al concentrador soltándolo en el directorio utilizado por el receptor del archivo. Busque en el Visor de documentos y debería ver que el documento está direccionado desde Socio dos al Socio interno utilizando la conexión que ha definido para él.

Capítulo 20. Ejemplos EDI

En este apéndice se proporcionan ejemplos del envío o recepción de intercambios EDI y de su transformación en documentos XML y de datos orientados a registros (ROD) o a partir de ellos.

Los ejemplos que aparecen en este apéndice no están relacionados con los del Capítulo 19, “Ejemplos básicos”, en la página 321. En este apéndice se crearán nuevos destinos y perfiles para los ejemplos.

Nota: un ejemplo de un intercambio EDI que se pasa a través del concentrador (sin desensobrado ni transformación) se incluye en el apartado Capítulo 19, “Ejemplos básicos”, en la página 321.

Todos estos cuatro ejemplos son autónomos. Por ejemplo, si sigue el ejemplo de EDI a XML, verá todos los pasos (desde la creación de destinos hasta la activación de conexiones) para dicho ejemplo.

Este apéndice incluye los siguientes temas:

- “ Ejemplo de EDI a ROD”
- “ Ejemplo de EDI a XML” en la página 355
- “ Ejemplo de XML a EDI” en la página 360
- “ Ejemplo de ROD a EDI” en la página 368

Estos ejemplos tienen como objetivo facilitar una visión general de los pasos necesarios para configurar un sistema. Si está utilizando estos ejemplos para configurar el sistema, modifique la información específica (por ejemplo, nombres e ID de empresa) de modo que se adapten a las necesidades de la empresa.

Ejemplo de EDI a ROD

En este apartado se proporciona un ejemplo del envío de una transacción EDI (dentro de un sobre) al concentrador, donde se transforma en un documento de datos orientados a registros (ROD) y se envía al socio interno.

Desensobrado y transformación de un intercambio EDI

Acerca de esta tarea

En este ejemplo, se da por supuesto que el especialista en correlaciones de Data Interchange Services ha creado una correlación de transformación que toma una transacción estándar EDI 850 (definida con el diccionario X12V5R1 y correspondiente a la versión 5010 de X12) y la transforma en un documento orientado a registros (ROD) que procesará la aplicación de fondo del socio interno. En este ejemplo, la correlación se denomina S_DT_EDI_TO_ROD.eif.

El especialista en correlaciones de Data Interchange Services puede exportar la correlación de transformación directamente a la base de datos de WebSphere Partner Gateway. Si lo desea, el especialista en correlaciones de Data Interchange Services puede enviarle el archivo, en cuyo caso debe emplear el programa de utilidad bcgDISImport para importarlo en WebSphere Partner Gateway. En este apéndice se da por supuesto el segundo caso.

Importación de la correlación de transformación
Acerca de esta tarea

En este apartado se describen los pasos para importar una correlación de transformación que tomará la entrada EDI y la transformará en un formato de datos orientados a registros (ROD). En el proceso de importar la correlación de transformación, también se importa la definición de documento asociada a la correlación.

Para poder importar la correlación de transformación, el especialista de correlaciones de Data Interchange Services debe enviársela. En este grupo de pasos se da por supuesto que el archivo, S_DT_EDI_TO_ROD.eif, está en el sistema.

1. Abra una ventana de mandatos.
2. Especifique el siguiente mandato o script:
   - En un sistema UNIX:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```

   - En un sistema Windows:

     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
     <password> S_DT_EDI_TO_ROD.eif
     ```

     donde *<database_user_ID>* y *<password>* son los valores utilizados al instalar la base de datos como parte de la instalación de WebSphere Partner Gateway.

Verificación de la correlación de transformación y de las definiciones de documento
Acerca de esta tarea

Para verificar las correlaciones de transformación y las definiciones de documento que se han importado están disponibles en la Consola de comunidad, realice estos pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de transformación**.

   Aparece la correlación S_DT_EDI_TO_ROD.
2. Pulse el icono **Ver detalles** situado junto a la correlación.

   Verá las definiciones de documento con las que esta correlación está asociada:

Tabla 35. Definición de documento asociada con la correlación

Origen	Destino
Paquete: N/D Protocolo: X12V5R1 (ALL)Tipo de documento: 850 (ALL)	Paquete: ninguno Protocolo: DEMO850CL_DICTIONARY(ALL) Tipo de documento: DEMO850CLSUW (ALL)

La correlación S_DT_EDI_TO_ROD se ha definido para que tome una transacción X12 850 (que cumple con el estándar X12V5R1) y la transforme en un protocolo personalizado (DEMO850CL_DICTIONARY) y tipo de documento (DEMO850CLSUW).

Configuración del receptor
Acerca de esta tarea

En este apartado, se creará un receptor de directorio de sistema de archivos para el concentrador:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** y pulse **Crear receptor**.
2. En Nombre del receptor, escriba: **EDIFileTarget**.
3. En la lista Transporte, seleccione **Directorio de archivos**.
4. En Vía de acceso raíz de documentos, escriba: **/Data/Manager/editarget**.
5. Pulse **Guardar**.

El socio envía el intercambio EDI a este receptor.

Creación de interacciones

Acerca de esta tarea

Cree dos interacciones, uno para el sobre EDI y uno para la transacción incluida en el sobre EDI.

Cree una interacción que represente el sobre EDI.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse **Crear interacción**.
3. En **Origen**, expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA**.
4. Enr **Destino**, expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y seleccione **Tipo de documento> ISA.**
5. En la lista Acción, seleccione **Desensobrar EDI**.

   Nota: en esta interacción no se produce ninguna transacción. El intercambio EDI se desensobra, lo que resulta en la transacción individual (850). Por lo tanto, no es necesaria una correlación de transformación para esta interacción.
6. Pulse **Guardar**.

Cree una interacción que tenga un origen que represente la transacción 850 y un destino que represente el documento transformado.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse **Crear interacción**.
3. En **Origen**, expanda **Paquete: N/D** y **Protocolo: X12V5R1** y seleccione **Tipo de documento: 850**.
4. En **Destino**, expanda **Paquete: Ninguno** y **Protocolo: DEMO850CL_DICTIONARY** y seleccione **Tipo de documento: DEMO850CLSUW**.
5. En la lista Correlación de transformación, seleccione **S_DT_EDI_TO_ROD**.
6. En la lista Acción, seleccione **Validación de EDI y conversión de EDI**.
7. Pulse **Guardar**.

Esta interacción representa la transformación de una transacción EDI X12 850 estándar en un formato distinto y, por lo tanto, debe seleccionar una correlación de transformación.

Creación de socios
Acerca de esta tarea

Para este ejemplo, tendrá dos socios: el socio interno (gestor) y un socio externo (TP1).

Cree el perfil del Socio interno:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **ComManager**
3. En Nombre de visualización de socio: escriba **Gestor**
4. En Tipo de socio, seleccione **Socio interno**.
5. Pulse **Nuevo** para ID de empresa y escriba `000000000` como ID de formato libre.

   Nota: asegúrese de seleccionar Formato libre, no DUNS.
6. Pulse **Nuevo** otra vez para ID de empresa y escriba `01-000000000` como ID de formato libre.
7. Pulse **Guardar**.

Cree el segundo socio:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **TP1**
3. En Nombre de visualización de socio, escriba **TP1**
4. En Tipo de socio, seleccione **Socio externo**.
5. Pulse **Nuevo** en ID de empresa y escriba `000000001` como ID de formato libre.

   Nota: asegúrese de seleccionar Formato libre, no DUNS.
6. Pulse **Nuevo** otra vez para ID de empresa y escriba `01-000000001` como ID de formato libre.
7. Pulse **Guardar**.

Creación de destinos
Acerca de esta tarea

Cree destinos de directorio de archivos para ambos socios en el ejemplo. En primer lugar, cree un destino para el gestor:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Pulse el icono **Ver detalles** situado junto al perfil del gestor.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir en el sistema de archivos.
   a. En Nombre, escriba **DestinoArchivoGestor**.
   b. En la lista Transporte, seleccione **Directorio de archivos**.
   c. En Dirección, escriba: **file://Data/Manager/filedestination**
   d. Pulse **Guardar**.
5. Pulse **Lista** para listar todos los destinos del socio interno.
6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino creado en el paso 4.
8. Pulse **Guardar**.

A continuación, cree un destino para el socio.

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Seleccione el otro socio que ha creado para este ejemplo pulsando sobre el icono **Ver detalles** junto a **TP1**.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir.
   a. En Nombre, escriba **DestinoArchivoTP1**.
   b. En la lista Transporte, seleccione **Directorio de archivos**.
   c. En Dirección, escriba: **file://Data/TP1/filedestination**
   d. Pulse **Guardar**.
5. Pulse **Lista** para listar todos los destinos del socio.
6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino creado en el paso 4.
8. Pulse **Guardar**.

Establecimiento de posibilidades B2B

Acerca de esta tarea

Habilite las funciones B2B de los dos socios en este intercambio. En este ejemplo, el intercambio EDI se origina con un socio externo (TP1) y se entregará al socio interno.

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Pulse el icono **Ver detalles** para el socio de origen en este ejemplo (**TP1**).
3. Pulse **Posibilidades B2B**.
4. Habilite dos conjuntos de capacidades para el socio de origen.
   a. Primero, habilite la definición de documento que representa el sobre EDI:
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: Ninguno** para habilitarlo.
      2) Expanda **Paquete: Ninguno**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: EDI-X12 (ALL)**.
      4) Expanda **Protocolo: EDI-X12 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: ISA (ALL)**.
   b. A continuación, habilite la definición de documento que representa la transacción 850:
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: X12V5R1 (ALL)**.
      4) Expanda **Protocolo: X12V5R1 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: 850**.
5. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
6. Pulse el icono **Ver detalles** para el socio de destino en este ejemplo (**Gestor**).

7. Pulse **Posibilidades B2B**.
8. Habilite dos conjuntos de posibilidades para el socio de destino.
   a. Primero, habilite la definición de documento que representa el sobre:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: EDI-X12 (ALL)**.
      4) Expanda **Protocolo: EDI-X12 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Tipo de documento: ISA (ALL)**.
   b. A continuación, habilite la definición de documento que representa el documento transformado:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.
      2) Expanda **Paquete: Ninguno**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: DEMO850CL_DICTIONARY (ALL)**.
      4) Expanda **Protocolo: DEMO850CL_DICTIONARY (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Tipo de documento: DEMO850CLSUW(ALL)**.

Activación de las conexiones

Acerca de esta tarea

Para activar las conexiones:

1. Pulse **Administración de cuentas > Conexiones**.
2. Seleccione **TP1** en la lista Origen.
3. Seleccione **Gestor** en la lista Destino.
4. Pulse **Buscar**.
5. Pulse **Activar** para la conexión que representa el sobre:

Tabla 36. Conexión de sobre

Origen	Destino
Paquete: ninguno (N/DA) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA (ALL)	Paquete: N/D (N/D) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA(ALL)

6. Pulse **Activar** para la conexión que representa la transacción 850 para el documento transformado:

Tabla 37. Transacción EDI para la conexión de documento ROD

Origen	Destino
Paquete: N/D (N/D) Protocolo: X12V5R1Tipo de documento: 850 (ALL)	Paquete: ninguno (N/D) Protocolo: DEMO850CL_DICTIONARY (ALL) Tipo de documento: DEMO850CLSUW (ALL)

Adición de atributos
Acerca de esta tarea

Establezca el atributo que admite documentos con ID duplicados:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**.
3. Pulse el icono **Editar valores de atributo** situado junto a **Protocolo: EDI-X12**.
4. Desplácese al apartado de la página Atributos de contexto de tipo de documento. En la fila **Permitir documentos con ID de documento duplicados**, seleccione **Sí** en la lista.
5. Pulse **Guardar**.

En este punto, si TP1 envía un intercambio EDI que contiene una transacción 850 al socio interno, el intercambio EDI se desensobrará, dando como resultado una transacción 850. Esta transacción se transformará después en el tipo de documento DEMO850CLSUW, y el documento transformado se enviará al destino del socio interno.

Adición de un TA1 al intercambio

En X12, el TA1 es un segmento opcional que puede utilizarse para acusar recibo de un intercambio. El remitente puede solicitar un TA1 del receptor estableciendo el elemento 14 de la cabecera de control de intercambio ISA en **1**. El atributo Permitir una solicitud TA1 en WebSphere Partner Gateway puede utilizarse para controlar si se envía un TA1 cuando el remitente lo solicita.

La correlación &WDI_TA1_ACK se instala durante la instalación de WebSphere Partner Gateway, por lo que no tendrá que importarlo.

Creación de asociaciones
Acerca de esta tarea

Para asociar una correlación con una definición de documento, lleve a cabo los siguientes pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de acuse de recibo funcional de EDI**.

   Aparece la correlación &WDI_TA1_ACK.
2. Pulse el icono **Ver detalles** situado junto a la correlación.

   Visualizará la información sobre la correlación así como una carpeta para cada tipo de paquete disponible en el sistema.
3. Cree la asociación con la definición de documento llevando a cabo los siguientes pasos:
   a. Seleccione el recuadro de selección situado junto a **Paquete: Ninguno** y expanda la carpeta.
   b. Seleccione el recuadro de selección situado junto a **Protocolo: EDI-X12 (ALL)** y expanda la carpeta.
   c. Seleccione el recuadro de selección situado junto a **Tipo de documento: ISA (ALL)**.
   d. Pulse **Guardar**.

Ha creado una asociación entre la correlación &WDI_TA1_ACK1 y la definición de documento del sobre.

Creación de interacciones
Acerca de esta tarea

Cree una interacción que represente la transacción TA1.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. En **Origen**, expanda **Paquete: N/D** y **Protocolo: &X44TA1** y seleccione **Tipo de documento: TA1**.
4. En **Destino**, expanda **Paquete: N/D** y **Protocolo: &X44TA1** y seleccione **Tipo de documento: TA1**.
5. En la lista Acción, seleccione **Paso a través**.
6. Pulse **Guardar**.

Cree una interacción que tenga un origen que represente el sobre EDI que mantendrá el TA1.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. En **Origen**, expanda **Paquete: N/D** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA**.
4. En **Destino**, expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA.**
5. En la lista Acción, seleccione **Paso a través**.
6. Pulse **Guardar**.

Habilitación de posibilidades B2B
Acerca de esta tarea

A continuación, añada las interacciones recién creadas a las funciones B2B de los socios.

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Pulse el icono **Ver detalles** para el socio de origen en este ejemplo (**Gestor**).

   Nota: recuerde que el TA1 fluye del socio que recibe el documento ROD al socio que lo ha enviado. En este ejemplo, el Gestor es el origen del TA1 y el socio TP1 es el destino.
3. Pulse **Posibilidades B2B**.
4. Habilite dos conjuntos de capacidades para el socio de origen.
   a. Primero, habilite la posibilidad para el TA1.
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: &X44TA1**.
      4) Expanda **Protocolo: &X44TA1**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: TA1 (ALL)**.
   b. A continuación, habilite la posibilidad para el sobre:

1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
2) Expanda **Paquete: N/D**.
3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: EDI-X12**.
4) Expanda **Protocolo: EDI-X12 (ALL)**.
5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: ISA (ALL)**.

5. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
6. Pulse el icono **Ver detalles** para el socio de destino en este ejemplo (**TP1**).
7. Pulse **Posibilidades B2B**.
8. Habilite dos conjuntos de posibilidades para el socio de destino.
   a. Primero, habilite la definición de documento que representa el TA1:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol está activo** bajo **Establecer destino** para **Protocolo: &X44TA1 (ALL)**.
      4) Expanda **Protocolo: &X44TA1 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Tipo de documento: TA1 (ALL)**.
   b. A continuación, habilite la definición de documento que representa el sobre EDI:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.
      2) Expanda **Paquete: Ninguno**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: EDI-X12 (ALL)**.
      4) Expanda **Protocolo: EDI-X12 (ALL)**.
      5) Pulse el icono **El rol no está activo** en **Establecer destino** for **Tipo de documento: ISA (ALL)**.

Creación del perfil de sobre

Acerca de esta tarea

A continuación, cree el perfil para el sobre que contendrá el TA1:

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Perfil de sobre**.
2. Pulse **Crear**.
3. Escriba el nombre del perfil: **EnvProf1**.
4. En la lista Estándar EDI, seleccione **X12**.
5. El botón **General** está seleccionado de manera predeterminada. Escriba los siguientes valores para los atributos generales del sobre:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**

6. Pulse **Intercambio** y escriba los siguientes valores para los atributos de intercambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Pulse **Guardar**.

Activación de conexiones de socio
Acerca de esta tarea

Para activar las conexiones:

1. Pulse **Administración de cuentas > Conexiones**.
2. Seleccione **Gestor** en la lista Origen.
3. Seleccione **TP1** en la lista Destino.
4. Pulse **Buscar**.
5. Active la conexión que representa el TA1.

Tabla 38. Conexión TA1

Origen	Destino
Paquete: N/D (N/D) Protocolo: &X44TA1 (ALL) Tipo de documento: TA1 (ALL)	Paquete: N/D (N/D) Protocolo: &X44TA1 (ALL) Tipo de documento: TA1 (ALL)

6. Active la conexión que representa el sobre:

Tabla 39. Conexión de sobre

Origen	Destino
Paquete: N/D (N/D) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA(ALL)	Paquete: ninguno (N/DA) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA (ALL)

Configuración de los atributos
Acerca de esta tarea

Para especificar atributos para el perfil de sobre:

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Seleccione **TP1** en la lista.
3. Pulse **Posibilidades B2B**.
4. Pulse el icono **Expandir** situado junto a **Paquete: Ninguno**.
5. Pulse el icono **Editar** situado junto a **Protocolo: EDI-X12 (ALL)**.
6. En la fila **Permitir una solicitud TA1**, seleccione **Sí**.
7. Pulse **Guardar**.
8. Pulse de nuevo **Funciones B2B**.
9. Pulse el icono **Expandir** situado junto a **Paquete: N/D**.
10. Pulse el icono **Editar** situado junto a **Protocolo: &X44TA1 (ALL)**.

11. Especifique los siguientes atributos:
    a. En la fila Perfil de sobre, seleccione **EnvProf1** en la lista.
    b. En la fila Calificador de intercambio, escriba **01**.
    c. En la fila Identificador de intercambio, escriba **000000001**.
    d. En el Indicador de uso del intercambio, escriba **T**.
12. Pulse **Guardar**.

En esta serie de tareas, se ha añadido un acuse de recibo TA1 al intercambio. Cuando se recibe un intercambio, WebSphere Partner Gateway devuelve un TA1 al remitente (TP1). El TA1 se envía en un sobre conforme al perfil de sobre EnvProf1.

Adición de una correlación de FA

En este apartado se describe cómo añadir un acuse de recibo funcional estándar (997) al flujo descrito en " Ejemplo de EDI a ROD" en la página 341. El acuse de recibo funcional proporciona una confirmación para el remitente de que se ha recibido la transacción.

Nota: este ejemplo es parecido a " Adición de un TA1 al intercambio" en la página 347. Sin embargo, no está relacionado directamente con dicho ejemplo. Más bien se crea basándose en las tareas realizadas en " Ejemplo de EDI a ROD" en la página 341.

WebSphere Partner Gateway incluye un conjunto de nombres de correlaciones de acuse de recibo funcional preinstaladas que empiezan por $DT_FA. A continuación le siguen el nombre del mensaje de acuse de recibo funcional y la versión y el release del mensaje. Por ejemplo, la versión 2 release 4 de mensaje de acuse de recibo funcional 997 se denomina $DT_997V2R4. Consulte el apartado "Configuración de reconocimientos" en la página 218 para obtener la lista de correlaciones que se proporcionan con WebSphere Partner Gateway.

Información relacionada

Creación de asociaciones

Acerca de esta tarea

Para asociar una correlación con una definición de documento, lleve a cabo los siguientes pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de acuse de recibo funcional de EDI**.

   Aparece la correlación &DT_FA997V2R4.
2. Pulse el icono **Ver detalles** situado junto a la correlación.

   Visualizará la información sobre la correlación así como una carpeta para cada tipo de paquete disponible en el sistema.
3. Cree la asociación con la definición de documento llevando a cabo los siguientes pasos:
   a. Seleccione el recuadro de selección situado junto a **Paquete: N/D** y expanda la carpeta
   b. Seleccione el recuadro de selección situado junto a **Protocolo: X12V5R1** y expanda la carpeta.
   c. Seleccione el recuadro de selección situado junto a **Tipo de documento: 850**.
   d. Pulse **Guardar**.

Ha asociado esta correlación 997 de acuse de recibo funcional con el protocolo X12.

Creación de interacciones
Acerca de esta tarea

Cree una interacción que representa el acuse de recibo 997.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Bajo **Origen**, expanda **Paquete: N/D** y **Protocolo: &DT99724** y seleccione **Tipo de documento: 997**.
4. Bajo **Destino**, expanda **Paquete: N/D** y **Protocolo: &DT99724** y seleccione **Tipo de documento: 997**.
5. En la lista Acción, seleccione **Paso a través**.
6. Pulse **Guardar**.

Cree una interacción que represente el sobre.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda **Paquete: N/D** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA**.
4. Expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA**.
5. En la lista Acción, seleccione **Paso a través**.
6. Pulse **Guardar**.

Habilitación de posibilidades B2B
Acerca de esta tarea

A continuación, añada las interacciones recién creadas a las funciones B2B de los socios.

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Pulse el icono **Ver detalles** para el socio de origen en este ejemplo (**Gestor**).

   Nota: recuerde que el acuse de recibo funcional fluye desde el socio que recibe el documento ROD al socio que lo ha enviado. En este ejemplo el Gestor es el origen del acuse de recibo funcional y el socio TP1 es el destino.
3. Pulse **Posibilidades B2B**.
4. Habilite dos conjuntos de capacidades para el socio de origen.
   a. Primero, habilite la posibilidad para el FA.
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: &DT99724**.
      4) Expanda **Protocolo: &DT99724**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: 997 (ALL)**.
   b. A continuación, habilite la posibilidad para el sobre:

1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
2) Expanda **Paquete: N/D**.
3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: EDI-X12**.
4) Expanda **Protocolo: EDI-X12 (ALL)**.
5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: ISA (ALL)**.

5. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
6. Pulse el icono **Ver detalles** para el socio de destino en este ejemplo (**TP1**).
7. Pulse **Posibilidades B2B**.
8. Habilite dos conjuntos de posibilidades para el socio de destino.
   a. Primero, habilite la definición de documento que representa el 997:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol está activo** bajo **Establecer destino** para **Protocolo: &DT99724 (ALL)**.
      4) Expanda **Protocolo: &DT99724 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Tipo de documento: 997 (ALL)**.
   b. A continuación, habilite la definición de documento que representa el sobre EDI:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.
      2) Expanda **Paquete: Ninguno**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: EDI-X12 (ALL)**.
      4) Expanda **Protocolo: EDI-X12 (ALL)**.
      5) Pulse el icono **El rol no está activo** en **Establecer destino** for **Tipo de documento: ISA(ALL)**.

Creación del perfil de sobre

Acerca de esta tarea

A continuación, cree el perfil para el sobre que contendrá el acuse de recibo funcional 997. Un acuse de recibo funcional, como una transacción, se debe ensobrar para su envío.

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Perfil de sobre**.
2. Pulse **Crear**.
3. Escriba el nombre del perfil: **EnvProf1**.
4. En la lista Estándar EDI, seleccione **X12**.
5. El botón **General** está seleccionado de manera predeterminada. Escriba los siguientes valores para los atributos generales del sobre:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**

- MAXDOCS: **1000**

6. Pulse el botón **Intercambio** y escriba los siguientes valores para los atributos de intercambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Pulse **Guardar**.

Activación de conexiones de socio
Acerca de esta tarea

Para activar las conexiones:

1. Pulse **Administración de cuentas > Conexiones**.
2. Seleccione **Gestor** en la lista Origen.
3. Seleccione **TP1** en la lista Destino.
4. Pulse **Buscar**.
5. Pulse **Activar** en la conexión que representa el acuse de recibo funcional 997:

Tabla 40. Conexión de acuse de recibo funcional

Origen	Destino
Paquete: N/D (N/D) Protocolo: &DT99724 (ALL) Tipo de documento: 997 (ALL)	Paquete: N/D (N/D) Protocolo: &DT99724 (ALL) Tipo de documento: 997 (ALL)

6. Pulse **Activar** para la conexión que representa el sobre EDI que se devuelve al originador del intercambio.

Tabla 41. Conexión de sobre

Origen	Destino
Paquete: N/D (N/D) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA(ALL)	Paquete: ninguno (N/DA) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA (ALL)

Configuración de atributos
Acerca de esta tarea

Primero debe especificar qué correlación de FA va a utilizar:

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Seleccione **TP1** en la lista.
3. Pulse **Posibilidades B2B**.
4. Pulse el icono **Expandir** situado junto a **Paquete: N/D**.
5. Pulse el icono **Editar** situado junto a **Protocolo: X12V5R1 (ALL)**.
6. En la fila Correlación de acuse de recibo funcional, seleccione **&DT_FA997V2R4**.
7. Pulse de nuevo **Funciones B2B**.

8. Pulse el icono **Expandir** situado junto a **Paquete: N/D**.
9. Pulse el icono **Editar** situado junto a **Protocolo: &DT99724 (ALL)**.
10. Especifique los siguientes atributos:
    a. En la fila Perfil de sobre, seleccione **EnvProf1** en la lista.
    b. En la fila Calificador de intercambio, escriba **01**.
    c. En la fila Identificador de intercambio, escriba **000000001**.
    d. En el Indicador de uso del intercambio, escriba **T**.
11. Pulse **Guardar**.

En esta serie de tareas ha añadido un reconocimiento funcional de EDI-X12 997 al intercambio, de modo que cuando el socio interno recibe el documento, se envía el 997 de vuelta al remitente (TP1). El acuse de recibo 997 se envía en un sobre conforme al perfil de sobre EnvProf1.

Ejemplo de EDI a XML

En este apartado se proporciona un ejemplo del envío de una transacción EDI (dentro de un sobre) al concentrador, donde se transforma en un documento XML y se envía al socio interno.

En este ejemplo, se da por supuesto que el especialista en correlaciones de Data Interchange Services ha creado una correlación de transformación que toma una transacción EDI 879 estándar (definida con el diccionario X12V5R1, correspondiente a la versión 5010 de X12) y la transforma en un documento XML que la aplicación de fondo del socio interno procesará. En este ejemplo, la correlación se denomina S_DT_EDI_TO_XML.eif.

El especialista en correlaciones de Data Interchange Services puede exportar la correlación de transformación directamente a la base de datos de WebSphere Partner Gateway. Si lo desea, el especialista en correlaciones de Data Interchange Services puede enviarle el archivo, en cuyo caso debe emplear el programa de utilidad bcgDISImport para importarlo en WebSphere Partner Gateway. En este apéndice se da por supuesto el segundo caso.

Importación de la correlación de transformación

Acerca de esta tarea

En este apartado se describen los pasos para importar una correlación de transformación que tomará la entrada EDI y la transformará en un formato XML. En el proceso de importar la correlación de transformación, también se importa la definición de documento asociada a la correlación.

Para poder importar la correlación de transformación, el especialista de correlaciones de Data Interchange Services debe enviársela. En este grupo de pasos se da por supuesto que el archivo, S_DT_EDI_TO_XML.eif, está en el sistema.

1. Abra una ventana de mandatos.
2. Especifique el siguiente mandato o script:
   - En un sistema UNIX:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```

   - En un sistema Windows:

     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
      <password> S_DT_EDI_TO_XML.eif
     ```

donde *<database_user_ID>* y *<password>* son los valores utilizados al instalar la base de datos como parte de la instalación de WebSphere Partner Gateway.

Verificación de la correlación de transformación y de las definiciones de documento

Acerca de esta tarea

Para verificar las correlaciones de transformación y las definiciones de documento que se han importado están disponibles en la Consola de comunidad, realice estos pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de transformación**.

   Aparece la correlación S_DT_EDI_TO_XML.
2. Pulse el icono **Ver detalles** situado junto a la correlación.

   Verá las definiciones de documento con las que esta correlación está asociada:

Tabla 42. Definición de documento asociada con la correlación

Origen	Destino
Paquete: N/D Protocolo: X12V5R1Tipo de documento: 879 (ALL)	Paquete: ninguno Protocolo: FVT-XML-TEST (ALL) Tipo de documento: WWRE_ITEMCREATIONINTERNAL (ALL)

La correlación S_DT_EDI_TO_XML se ha definido para que tome una transacción X12 879 (que cumple el estándar X12V5R1) y transformarla en un protocolo personalizado.

Configuración del receptor

Acerca de esta tarea

En este apartado, se creará un receptor de directorio de sistema de archivos para el concentrador:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** y pulse **Crear receptor**.
2. En Nombre del receptor, escriba: **EDIFileTarget**.
3. En la lista Transporte, seleccione **Directorio de archivos**.
4. En Vía de acceso raíz de documentos, escriba: **/Data/Manager/editarget**.
5. Pulse **Guardar**.

El socio envía el intercambio EDI a este receptor.

Creación de interacciones

Acerca de esta tarea

Cree dos interacciones, uno para el sobre EDI y uno para la transacción incluida en el sobre EDI.

Cree una interacción que represente el sobre EDI.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.

3. Expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA**.
4. Expanda **Paquete: N/D** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA.**
5. En la lista Acción, seleccione **Desensobrar EDI**.

   Nota: en esta interacción no se produce ninguna transacción. El intercambio EDI se desensobra, lo que resulta en la transacción individual (879). Por lo tanto, no es necesaria una correlación de transformación para esta interacción.
6. Pulse **Guardar**.

Cree una interacción que tenga un origen que represente la transacción 879 y un destino que represente el documento transformado.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda **Paquete: N/D** y **Protocolo: X12V5R1** y seleccione **Tipo de documento: 879**.
4. Expanda **Paquete: Ninguno** y **Protocolo: FVT-XML-TEST** y seleccione **Tipo de documento: WWRE_ITEMCREATIONINTERNAL**.
5. En la lista Correlación de transformación, seleccione **S_DT_EDI_TO_XML**.
6. En la lista Acción, seleccione **Validación de EDI y conversión de EDI**.
7. Pulse **Guardar**.

Esta interacción representa la transformación de una transacción EDI X12 879 estándar en un formato distinto y, por lo tanto, debe seleccionar una correlación de transformación.

Creación de socios

Acerca de esta tarea

Para este ejemplo, tendrá dos socios: el socio interno (gestor) y un socio externo (TP1).

Cree el perfil del Socio interno:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **ComManager**
3. En Nombre de visualización de socio: escriba **Gestor**
4. En Tipo de socio, seleccione **Socio interno**.
5. Pulse **Nuevo** para ID de empresa y escriba `000000000` como ID de formato libre.

   Nota: asegúrese de seleccionar Formato libre, no DUNS.
6. Pulse **Nuevo** otra vez para ID de empresa y escriba `01-000000000` como ID de formato libre.
7. Pulse **Guardar**.

Cree el segundo socio:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **TP1**

3. En Nombre de visualización de socio, escriba **TP1**
4. En Tipo de socio, seleccione **Socio externo**.
5. Pulse **Nuevo** en ID de empresa y escriba `000000001` como ID de formato libre.

   Nota: asegúrese de seleccionar Formato libre, no DUNS.
6. Pulse **Nuevo** otra vez para ID de empresa y escriba `01-000000001` como ID de formato libre.
7. Pulse **Guardar**.

Creación de destinos

Acerca de esta tarea

Cree destinos de directorio de archivos para ambos socios en el ejemplo. En primer lugar, cree un destino para el gestor:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Pulse el icono **Ver detalles** situado junto al perfil del gestor.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir en el sistema de archivos.
   a. En Nombre, escriba **DestinoArchivoGestor**.
   b. En la lista Transporte, seleccione **Directorio de archivos**.
   c. En Dirección, escriba: **file://Data/Manager/filedestination**
   d. Pulse **Guardar**.
5. Pulse **Lista** para listar todos los destinos del socio interno.
6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino creado en el paso 4.
8. Pulse **Guardar**.

A continuación, cree un destino para el socio.

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Seleccione el otro socio que ha creado para este ejemplo pulsando sobre el icono **Ver detalles** junto a **TP1**.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir.
   a. En Nombre, escriba **DestinoArchivoTP1**.
   b. En la lista Transporte, seleccione **Directorio de archivos**.
   c. En Dirección, escriba: **file://Data/TP1/filedestination**
   d. Pulse **Guardar**.
5. Pulse **Lista** para listar todos los destinos del socio.
6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino creado en el paso 4.
8. Pulse **Guardar**.

Establecimiento de posibilidades B2B

Acerca de esta tarea

Habilite las funciones B2B de los dos socios en este intercambio. En este ejemplo, el intercambio EDI se origina con un socio externo (TP1) y se entregará al socio interno.

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Pulse el icono **Ver detalles** para el socio de origen en este ejemplo (**TP1**).
3. Pulse **Posibilidades B2B**.
4. Habilite dos conjuntos de capacidades para el socio de origen.
   a. Primero, habilite la definición de documento que representa el sobre EDI:
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: Ninguno** para habilitarlo.
      2) Expanda **Paquete: Ninguno**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: EDI-X12 (ALL)**.
      4) Expanda **Protocolo: EDI-X12 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: ISA (ALL)**.
   b. A continuación, habilite la definición de documento que representa la transacción:
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: X12V5R1 (ALL)**.
      4) Expanda **Protocolo: X12V5R1 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: 879**.
5. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
6. Pulse el icono **Ver detalles** para el socio de destino en este ejemplo (**Gestor**).
7. Pulse **Posibilidades B2B**.
8. Habilite dos conjuntos de posibilidades para el socio de destino.
   a. Primero, habilite la definición de documento:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: EDI-X12 (ALL)**.
      4) Expanda **Protocolo: EDI-X12 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Tipo de documento: ISA (ALL)**.
   b. A continuación, habilite la definición de documento que representa el documento transformado:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.

2) Expanda **Paquete: Ninguno**.
3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: FVT-XML-TEST (ALL)**.
4) Expanda **Protocolo: FVT-XML-TEST (ALL)**.
5) Pulse el icono **El rol no está activo** en **Establecer destino** para **Tipo de documentoWWRE_ITEMCREATIONINTERNAL(ALL)**.

Activación de las conexiones

Acerca de esta tarea

Para activar las conexiones:

1. Pulse **Administración de cuentas > Conexiones**.
2. Seleccione **TP1** en la lista Origen.
3. Seleccione **Gestor** en la lista Destino.
4. Pulse **Buscar**.
5. Pulse **Activar** para la conexión que representa el sobre:

Tabla 43. Conexión de sobre

Origen	Destino
Paquete: ninguno (N/DA) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA (ALL)	Paquete: N/D (N/D) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA(ALL)

6. Pulse **Activar** para la conexión que representa la transacción 879 para el documento transformado:

Tabla 44. Transacción EDI para la conexión de documento XML

Origen	Destino
Paquete: N/D (N/D) Protocolo: X12V5R1 (ALL)Tipo de documento: 879 (ALL)	Paquete: ninguno (N/D) Protocolo: FVT-XML-TEST (ALL) Tipo de documento: WWRE_ITEMCREATIONINTERNAL (ALL)

En este punto, si TP1 enviase un intercambio EDI que contuviese una transacción 879 al socio interno, el intercambio EDI se desensobraría, obteniendo como resultado una transacción 879. La transacción 879 se transformaría entonces y el documento transformado se enviaría al destino del socio interno.

Ejemplo de XML a EDI

En este apartado se proporciona un ejemplo del socio interno enviando un documento XML al concentrador, donde se transforma en una transacción EDI, se ensobra dentro de un intercambio EDI y se envía a un socio.

En este ejemplo, se asume que el especialista de correlación de Data Interchange Services ha creado una correlación de transformación que toma un documento XML y lo transforma en una transacción 850 estándar (definida con el diccionario MX12V3R1) que será procesado por el socio. En este ejemplo, la correlación se denomina S_DT_XML_TO_EDI.eif.

El especialista en correlaciones de Data Interchange Services puede exportar la correlación de transformación directamente a la base de datos de WebSphere Partner Gateway. Si lo desea, el especialista en correlaciones de Data Interchange

Services puede enviarle el archivo, en cuyo caso debe emplear el programa de utilidad bcgDISImport para importarlo en WebSphere Partner Gateway. En este apéndice se da por supuesto el segundo caso.

Importación de la correlación de transformación

Acerca de esta tarea

En este apartado se describen los pasos para importar una correlación de transformación que tomará la entrada XML y la transformará en una transacción EDI. En el proceso de importar la correlación de transformación, también se importa la definición de documento asociada a la correlación.

Para poder importar la correlación de transformación, el especialista de correlaciones de Data Interchange Services debe enviársela. En este grupo de pasos se da por supuesto que el archivo, S_DT_XML_TO_EDI.eif, está en el sistema.

1. Abra una ventana de mandatos.
2. Especifique el siguiente mandato o script:
   - En un sistema UNIX:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_XML_TO_EDI.eif
     ```

   - En un sistema Windows:

     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
      <password> S_DT_XML_TO_EDI.eif
     ```

     donde *<database_user_ID>* y *<password>* son los valores utilizados al instalar la base de datos como parte de la instalación de WebSphere Partner Gateway.

Verificación de la correlación de transformación y de las definiciones de documento

Acerca de esta tarea

Para verificar las correlaciones de transformación y las definiciones de documento que se han importado están disponibles en la Consola de comunidad, realice estos pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de transformación**.

   Aparece la correlación S_DT_XML_TO_EDI.
2. Pulse el icono **Ver detalles** situado junto a la correlación.

   Verá las definiciones de documento con las que esta correlación está asociada:

Tabla 45. Definiciones de documento asociadas con la correlación

Origen	Destino
Paquete: ninguno Protocolo: FVT-XML-TEST (ALL) Tipo de documento: ICGCPO (ALL)	Paquete: N/D Protocolo: MX12V3R1 (ALL) Tipo de documento: 850 (ALL)

La correlación S_DT_XML_TO_EDI se ha definido para tomar un documento XML y lo transforma en una transacción EDI.

Configuración del receptor

Acerca de esta tarea

En este apartado, se creará un receptor de directorio de sistema de archivos para el concentrador:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** y pulse **Crear receptor**.
2. En Nombre del receptor, escriba: **XMLFileTarget**.
3. En la lista Transporte, seleccione **Directorio de archivos**.
4. En Vía de acceso raíz de documentos, escriba: **/Data/Manager/xmltarget**.
5. En la lista Puntos de configuración, seleccione **preproceso**.
6. Seleccione **com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler** en la Lista disponible y pulse **Añadir** para moverlo a la Lista configurada.
7. Pulse **Guardar**.

El socio interno envía el documento XML a este receptor.

Creación de interacciones

Acerca de esta tarea

Cree dos interacciones, una para la transformación de XML a EDI y otra para el sobre EDI.

Cree una interacción que tenga un origen que represente el documento XML y un destino que representa la transacción 850 transformada.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda **Paquete: Ninguno** y **Protocolo: FVT-XML-TEST** y seleccione **Tipo de documento: ICGCPO**.
4. Expanda **Paquete: N/D** y **Protocolo: MX12V3R1** y seleccione **Tipo de documento: 850**.
5. En la lista Correlación de transformación, seleccione **S_DT_XML_TO_EDI**.
6. En la lista Acción, seleccione **Conversión de XML y Validación de EDI**.
7. Pulse **Guardar**.

Esta interacción representa la transformación de un documento XML en una transacción EDI y, por lo tanto, debe seleccionar una correlación de transformación.

Cree una interacción que represente el sobre EDI.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda **Paquete: N/D** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA**.
4. Expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA.**
5. En la lista Acción, seleccione **Paso a través**.

   Nota: en esta interacción no se produce ninguna transacción.

6. Pulse **Guardar**.

Creación de socios

Acerca de esta tarea

Para este ejemplo, tendrá dos socios: el socio interno (gestor) y un socio externo (TP1).

Cree el perfil del Socio interno:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **ComManager**
3. En Nombre de visualización de socio, escriba: **Gestor**.
4. En Tipo de socio, seleccione **Socio interno**.
5. Pulse **Nuevo** para ID de empresa y escriba `000000000` como ID de formato libre.

   Nota: asegúrese de seleccionar Formato libre, no DUNS.
6. Pulse **Nuevo** para crear un ID de empresa y escriba `01-000000000` como ID de formato libre. Al pulsar Nuevo, el cuadro de texto del ID de correo electrónico también se habilita y se muestra para que cree un ID de correo electrónico.
7. Pulse **Nuevo** para crear un nuevo ID de correo electrónico y escriba su ID de correo electrónico en Identificador de correo electrónico. Del mismo modo, puede pulsar Nuevo para crear varios ID de correo electrónico.
8. Pulse **Guardar**.

Cree el segundo socio:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **TP1**
3. En Nombre de visualización de socio, escriba **TP1**
4. En Tipo de socio, seleccione **Socio externo**.
5. Pulse **Nuevo** para crear un ID de empresa y escriba `01-000000000` como ID de formato libre. Al pulsar Nuevo, el cuadro de texto del ID de correo electrónico también se habilita y se muestra para que cree un ID de correo electrónico.

   Nota: asegúrese de seleccionar Formato libre, no DUNS.
6. Pulse **Nuevo** para crear un nuevo ID de correo electrónico y escriba su ID de correo electrónico en Identificador de correo electrónico. Del mismo modo, puede pulsar Nuevo para crear varios ID de correo electrónico.
7. Pulse **Guardar**.

Creación de destinos

Acerca de esta tarea

Cree destinos de directorio de archivos para ambos socios en el ejemplo. En primer lugar, cree un destino para el gestor:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Pulse el icono **Ver detalles** situado junto al perfil del gestor.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir en el sistema de archivos.

a. En Nombre, escriba **DestinoArchivoGestor**.
b. En la lista Transporte, seleccione **Directorio de archivos**.
c. En Dirección, escriba: **file://Data/Manager/filedestination**
d. Pulse **Guardar**.

5. Pulse **Lista** para listar todos los destinos del socio interno.
6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino creado en el paso 4 en la página 363.
8. Pulse **Guardar**.

A continuación, cree un destino para el socio.

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Seleccione el otro socio que ha creado para este ejemplo pulsando sobre el icono **Ver detalles** junto a **TP1**.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir.
   a. En Nombre, escriba **DestinoArchivoTP1**.
   b. En la lista Transporte, seleccione **Directorio de archivos**.
   c. En Dirección, escriba: **file://Data/TP1/filedestination**
   d. Pulse **Guardar**.
5. Pulse **Lista** para listar todos los destinos del socio.
6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino creado en el paso 4.
8. Pulse **Guardar**.

Establecimiento de posibilidades B2B

Acerca de esta tarea

Habilite las funciones B2B de los dos socios en este intercambio. En este ejemplo, el documento XML se origina desde el socio interno y se entregará al socio externo.

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Pulse el icono **Ver detalles** para el socio de origen en este ejemplo (**ComMan**).
3. Pulse **Posibilidades B2B**.
4. Habilite tres conjuntos de posibilidades para el socio de origen.
   a. Habilite la definición de documento que representa el documento XML:
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: Ninguno** para habilitarlo.
      2) Expanda **Paquete: Ninguno**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: FVT-XML-TEST (ALL)**.
      4) Expanda **Protocolo: FVT-XML-TEST (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: ICGCPO (ALL)**.
   b. A continuación, habilite la definición de documento que representa el documento transformado:

1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
2) Expanda **Paquete: N/D**.
3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: MX12V3R1 (ALL)**.
4) Expanda **Protocolo: MX12V3R1 (ALL)**.
5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: 850**.

c. A continuación, habilite la definición de documento que representa el sobre EDI:
1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
2) Expanda **Paquete: N/D**.
3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: EDI-X12 (ALL)**.
4) Expanda **Protocolo: EDI-X12 (ALL)**.
5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: ISA (ALL)**.

5. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
6. Pulse el icono **Ver detalles** para el socio de destino en este ejemplo (**TP1**).
7. Pulse **Posibilidades B2B**.
8. Habilite dos conjuntos de posibilidades para el socio de destino.
a. Primero, habilite la definición de documento que representa la transacción EDI 850:
1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: N/D** para habilitarlo.
2) Expanda **Paquete: N/D**.
3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: MX12V3R1 (ALL)**.
4) Expanda **Protocolo: MX12V3R1 (ALL)**.
5) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Tipo de documento: 850 (ALL)**.

b. A continuación, habilite la definición de documento:
1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.
2) Expanda **Paquete: Ninguno**.
3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: EDI-X12 (ALL)**.
4) Expanda **Protocolo: EDI-X12 (ALL)**.
5) Pulse el icono **El rol no está activo** en **Establecer destino** for **Tipo de documento: ISA(ALL)**.

Creación del perfil de sobre

Acerca de esta tarea

A continuación, cree el perfil para el sobre que contendrá la transacción 850 transformada.

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Perfil de sobre**.
2. Pulse **Crear**.
3. Escriba el nombre del perfil: **EnvProf1**.
4. En la lista Estándar EDI, seleccione **X12**.
5. El botón **General** está seleccionado de manera predeterminada. Escriba los siguientes valores para los atributos generales del sobre:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Pulse **Intercambio** y escriba los siguientes valores para los atributos de intercambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. Pulse **Guardar**.

Creación del formato XML

Acerca de esta tarea

En este apartado se creará el formato XML personalizado.

1. Pulse **Administración del concentrador > Configuración del concentrador > Formatos XML**.
2. Pulse **Crear formato XML**.
3. En Formato de direccionamiento, seleccione **FVT-XML-TEST ALL**.
4. En Tipo de archivo, seleccione **XML**.
5. En Tipo de identificador, seleccione **Distintivo de directorio raíz** y escriba **MMDoc**.
6. En ID de empresa de origen, seleccione **Constante** y escriba **000000000**.
7. En ID de origen de destino, seleccione **Constante** y escriba **000000001**.
8. En Tipo de documento de origen, seleccione **Constante** y escriba **ICGCPO**.
9. En Versión del tipo de documento de origen, seleccione **Constante** y escriba **ALL**.
10. Pulse **Guardar**.

Activación de las conexiones

Acerca de esta tarea

Active las conexiones de socio:

1. Pulse **Administración de cuentas > Conexiones**.
2. Seleccione **Gestor** en la lista Origen.
3. Seleccione **TP1** en la lista Destino.

4. Pulse **Buscar**.
5. Pulse **Activar** para la siguiente conexión:

Tabla 46. Conexión de documento XML con transacción EDI

Origen	Destino
Paquete: ninguno (N/DA) Protocolo: FVT-XML-TEST (ALL) Tipo de documento: ICGCPO (ALL)	Paquete: N/D (N/D) Protocolo: MX12V3R1 (ALL) Tipo de documento: 850(ALL)

6. Pulse **Activar** para la conexión que representa el sobre EDI:

Tabla 47. Conexión del sobre EDI

Origen	Destino
Paquete: N/D (N/D) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA(ALL)	Paquete: ninguno (N/DA) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA (ALL)

Configuración de atributos

Acerca de esta tarea

Configure los atributos de funciones B2B del socio de destino (TP1) y del socio de origen (Gestor):

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Pulse el icono **Ver detalles** situado junto a **TPI** para seleccionarlo.
3. Pulse **Posibilidades B2B**.
4. Pulse el icono **Expandir** situado junto a **Paquete: N/D**.
5. Pulse el icono **Editar** situado junto a **Protocolo: MX12V3R1**.
6. Especifique los siguientes atributos:
   a. En la fila Perfil de sobre, seleccione **EnvProf1** en la lista.
   b. En la fila Calificador de intercambio, escriba **01**.
   c. En la fila Identificador de intercambio, escriba **000000001**.
   d. En el Indicador de uso del intercambio, escriba **T**.
7. Pulse **Guardar**.
8. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
9. Pulse Ver detalles junto a **Gestor** para seleccionarlo.
10. Pulse **Posibilidades B2B**.
11. Pulse el icono **Expandir** situado junto a **Paquete: N/D**.
12. Pulse el icono **Editar** situado junto a **Protocolo: MX12V3R1 (ALL)**.
13. Especifique los siguientes atributos:
    a. En la fila Calificador de intercambio, escriba **01**.
    b. En la fila Identificador de intercambio, escriba **000000000**.
    c. En el Indicador de uso del intercambio, escriba **T**.
14. Pulse **Guardar**.

En este momento, si el socio de origen (el socio interno) enviase un documento XML al socio, se convertiría (en el concentrador) en una transacción EDI, se ensobraría y, a continuación, se enviaría al destino del socio.

Ejemplo de ROD a EDI

En este apartado se proporciona un ejemplo del socio interno enviando un documento ROD al concentrador, donde se transforma en una transacción EDI, se ensobra dentro de un intercambio EDI y se envía a un socio.

En este ejemplo, se asume que el especialista en correlaciones de Data Interchange Services ha creado una correlación de transformación que toma un documento orientado a objetos (ROD) y lo transforma en una transacción EDI 850 estándar (definida con el diccionario X12V5R1, correspondiente a la versión 5010 de X12) que procesará el socio. En este ejemplo, la correlación se denomina S_DT_ROD_TO_EDI.eif.

El especialista en correlaciones de Data Interchange Services puede exportar la correlación de transformación directamente a la base de datos de WebSphere Partner Gateway. Si lo desea, el especialista en correlaciones de Data Interchange Services puede enviarle el archivo, en cuyo caso debe emplear el programa de utilidad bcgDISImport para importarlo en WebSphere Partner Gateway. En este apéndice se da por supuesto el segundo caso.

Importación de la correlación de transformación

Acerca de esta tarea

En este apartado se describen los pasos para importar una correlación de transformación que tomará la entrada ROD y la transformará en una transacción X12. En el proceso de importar la correlación de transformación, también se importa la definición de documento asociada a la correlación.

Para poder importar la correlación de transformación, el especialista de correlaciones de Data Interchange Services debe enviársela. En este grupo de pasos se da por supuesto que el archivo, S_DT_ROD_TO_EDI.eif, está en el sistema.

1. Abra una ventana de mandatos.
2. Especifique el siguiente mandato o script:
   - En un sistema UNIX:

     ```
     <ProductDir>/bin/bcgDISImport.sh <database_user_ID>
      <password> S_DT_ROD_TO_EDI.eif
     ```

   - En un sistema Windows:

     ```
     <ProductDir>\bin\bcgDISImport.bat <database_user_ID>
      <password> S_DT_ROD_TO_EDI.eif
     ```

     donde *<database_user_ID>* y *<password>* son los valores utilizados al instalar la base de datos como parte de la instalación de WebSphere Partner Gateway.

Verificación de la correlación de transformación y de las definiciones de documento

Acerca de esta tarea

Para verificar las correlaciones de transformación y las definiciones de documento que se han importado están disponibles en la Consola de comunidad, realice estos pasos:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Correlaciones> Correlaciones de transformación**.

   Aparece la correlación S_DT_ROD_TO_EDI.
2. Pulse el icono **Ver detalles** situado junto a la correlación.

Verá las definiciones de documento con las que esta correlación está asociada:

Tabla 48. Definiciones de documento asociadas con la correlación

Origen	Destino
Paquete: ninguno Protocolo: ROD-TO-EDI_DICT (ALL) Tipo de documento: DTROD-TO-EDI_ROD (ALL)	Paquete: N/D Protocolo: X12V5R1(ALL) Tipo de documento: 850 (ALL)

La correlación S_DT_ROD_TO_EDI se ha definido de forma que tome un documento ROD asociado al diccionario ROD-TO-EDI_DICT y lo transforme en una transacción X12 850 que cumpla con el estándar X12V5R1.

Configuración del receptor

Acerca de esta tarea

En este apartado, se creará un receptor de directorio de sistema de archivos para el concentrador:

1. Pulse **Administrador de concentrador > Configuración del concentrador > Receptores** y pulse **Crear receptor**.
2. En Nombre del receptor, escriba: **RODFileTarget**.
3. En la lista Transporte, seleccione **Directorio de archivos**.
4. En Vía de acceso raíz de documentos, escriba: **/Data/Manager/rodtarget**.
5. En la lista Puntos de configuración, seleccione **preproceso**.
6. Seleccione **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** en la Lista disponible y pulse **Añadir** para moverlo a la Lista configurada.
7. Seleccione **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** en la Lista configurada y pulse **Configurar**.
8. Añada los valores que se muestran en la tabla:

Tabla 49. Atributos del manejador de divisor ROD

Campo	Valor
Nombre De empaquetado	Ninguno
Versión De empaquetado	N/D
Nombre De protocolo	ROD-TO-EDI_DICT
Versión De protocolo	ALL
Código De proceso	DTROD-TO-EDI_ROD
Versión De proceso	ALL
METADICTIONARY	ROD-TO-EDI_DICT
METADOCUMENT	DTROD-TO-EDI_ROD
METASYNTAX	rod
ENCODING	ascii
BCG_BATCHDOCS	ON

9. Pulse **Establecer valores**.
10. Pulse **Guardar**.

El socio interno envía el documento ROD a este destino.

Creación de interacciones

Acerca de esta tarea

Cree dos interacciones, una para el sobre EDI que se enviará desde el concentrador y la otra para la transformación del documento ROD a EDI.

Cree una interacción que tenga un origen que represente el documento ROD y un destino que represente el documento X12.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda **Paquete: Ninguno** y **Protocolo: ROD-TO-EDI_DICT** y seleccione **DTROD-TO-EDI_ROD**.
4. Expanda **Paquete: N/D** y **Protocolo: X12V5R1** y seleccione **Tipo de documento: 850**.
5. En la lista Correlación de transformación, seleccione **S_DT_ROD_TO_EDI**.
6. En la lista Acción, seleccione **Conversión de ROD y Validación de EDI**.
7. Pulse **Guardar**.

Esta interacción representa la transformación de un documento ROD en una transacción X12 estándar y, por lo tanto, debe seleccionar una correlación de transformación.

Cree una interacción que represente el sobre EDI.

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento > Gestionar interacciones**.
2. En la pantalla **Gestionar interacciones**, pulse **Crear interacción**.
3. Expanda **Paquete: N/D** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA**.
4. Expanda **Paquete: Ninguno** y **Protocolo: EDI-X12** y seleccione **Tipo de documento: ISA.**
5. En la lista Acción, seleccione **Paso a través**.

   Nota: en esta interacción no se produce ninguna transacción. Esta interacción es para ensobrar el intercambio EDI.
6. Pulse **Guardar**.

Creación de socios

Acerca de esta tarea

Para este ejemplo, tendrá dos socios: el socio interno (gestor) y un socio externo (TP1).

Cree el perfil del Socio interno:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **ComManager**
3. En Nombre de visualización de socio: escriba **Gestor**
4. En Tipo de socio, seleccione **Socio interno**.
5. Pulse **Nuevo** para ID de empresa y escriba `000000000` como ID de formato libre.

Nota: asegúrese de seleccionar Formato libre, no DUNS.

6. Pulse **Nuevo** otra vez para ID de empresa y escriba `01-000000000` como ID de formato libre.
7. Pulse **Guardar**.

Cree el segundo socio:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Crear**.
2. En Nombre de inicio de sesión de empresa, escriba **TP1**
3. En Nombre de visualización de socio, escriba **TP1**
4. En Tipo de socio, seleccione **Socio externo**.
5. Pulse **Nuevo** en ID de empresa y escriba `000000001` como ID de formato libre.

   Nota: asegúrese de seleccionar Formato libre, no DUNS.
6. Pulse **Nuevo** otra vez para ID de empresa y escriba `01-000000001` como ID de formato libre.
7. Pulse **Guardar**.

Creación de destinos

Acerca de esta tarea

Cree destinos de directorio de archivos para ambos socios en el ejemplo. En primer lugar, cree un destino para el gestor:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Pulse el icono **Ver detalles** situado junto al perfil del gestor.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir en el sistema de archivos.
   a. En Nombre, escriba **DestinoArchivoGestor**.
   b. En la lista Transporte, seleccione **Directorio de archivos**.
   c. En Dirección, escriba: **file://Data/Manager/filedestination**
   d. Pulse **Guardar**.
5. Pulse **Lista** para listar todos los destinos del socio interno.
6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino que ha creado en el paso 4
8. Pulse **Guardar**.

A continuación, cree un destino para el socio.

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Seleccione el otro socio que ha creado para este ejemplo pulsando sobre el icono **Ver detalles** junto a **TP1**.
3. Pulse **Destinos** y, a continuación, **Crear**.
4. Especifique los siguientes valores para el destino. Recuerde que el directorio de archivos (toda la vía de acceso) ya debe existir.
   a. En Nombre, escriba **DestinoArchivoTP1**.
   b. En la lista Transporte, seleccione **Directorio de archivos**.
   c. En Dirección, escriba: **file://Data/TP1/filedestination**
   d. Pulse **Guardar**.
5. Pulse **Lista** para listar todos los destinos del socio.

6. Pulse **Ver destinos predeterminados**.
7. En la lista **Producción**, seleccione el destino creado en el paso 4 en la página 371.
8. Pulse **Guardar**.

Establecimiento de posibilidades B2B

Acerca de esta tarea

Habilite las funciones B2B de los dos socios en este intercambio. En este ejemplo, el documento ROD se origina en el socio interno y se entregará al socio externo (TP1).

1. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
2. Pulse el icono **Ver detalles** para el socio de origen en este ejemplo (**Gestor**).
3. Pulse **Posibilidades B2B**.
4. Habilite dos conjuntos de capacidades para el socio de origen.
   a. Primero, habilite la definición de documento que representa el documento ROD:
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: Ninguno** para habilitarlo.
      2) Expanda **Paquete: Ninguno**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: ROD-TO-EDI_DICT (ALL)**.
      4) Expanda **Protocolo: ROD-TO-EDI_DICT (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: DTROD-TO-EDI_ROD (ALL)**.
   b. A continuación, habilite la definición de documento que representa el sobre EDI:
      1) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Protocolo: EDI-X12 (ALL)**.
      4) Expanda **Protocolo: EDI-X12 (ALL)**.
      5) Pulse el icono **El rol no está activo** bajo **Establecer origen** para **Tipo de documento: ISA (ALL)**.
5. Pulse **Administración de cuentas > Perfiles > Socio** y a continuación pulse **Buscar**.
6. Pulse el icono **Ver detalles** para el socio de destino en este ejemplo (**TP1**).
7. Pulse **Posibilidades B2B**.
8. Habilite dos conjuntos de posibilidades para el socio de destino.
   a. Primero, habilite la definición de documento que representa la transacción EDI 850:
      1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: N/D** para habilitarlo.
      2) Expanda **Paquete: N/D**.
      3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: X12V5R1 (ALL)**.
      4) Expanda **Protocolo: X12V5R1 (ALL)**.

5) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Tipo de documento: 850 (ALL)**.

b. A continuación, habilite la definición de documento que representa el sobre:
   1) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Paquete: Ninguno** para habilitarlo.
   2) Expanda **Paquete: Ninguno**.
   3) Pulse el icono **El rol no está activo** bajo **Establecer destino** para **Protocolo: EDI-X12 (ALL)**.
   4) Expanda **Protocolo: EDI-X12 (ALL)**.
   5) Pulse el icono **El rol no está activo** en **Establecer destino** for **Tipo de documento: ISA (ALL)**.

Creación del perfil de sobre

Acerca de esta tarea

A continuación, cree el perfil para el sobre que contendrá la transacción 850 transformada.

1. Pulse **Administrador de concentrador > Configuración del concentrador > EDI > Perfil de sobre**.
2. Pulse **Crear**.
3. Escriba el nombre del perfil: **EnvProf1**.
4. En la lista Estándar EDI, seleccione **X12**.
5. El botón **General** está seleccionado de manera predeterminada. Escriba los siguientes valores para los atributos generales del sobre:
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Pulse el botón **Intercambio** y escriba los siguientes valores para los atributos de intercambio:
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Pulse **Guardar**.

Activación de las conexiones

Acerca de esta tarea

Para activar las conexiones:

1. Pulse **Administración de cuentas > Conexiones**.
2. Seleccione **Gestor** en la lista Origen.
3. Seleccione **TP1** en la lista Destino.
4. Pulse **Buscar**.

5. Pulse **Activar** para la conexión que representa el documento ROD para la transacción EDI:

Tabla 50. Conexión de ROD a EDI

Origen	Destino
Paquete: N/D (N/D) Protocolo: ROD-TO-EDI_DICT (ALL) Tipo de documento: DTROD-TO-EDI_ROD (ALL)	Paquete: ninguno (N/D) Protocolo: X12V5R1 (ALL) Tipo de documento: 850

6. Pulse **Activar** para la conexión que representa el sobre:

Tabla 51. Conexión de sobre

Origen	Destino
Paquete: ninguno (N/DA) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA (ALL)	Paquete: N/D (N/D) Protocolo: EDI-X12 (ALL) Tipo de documento: ISA(ALL)

Configuración de atributos

Acerca de esta tarea

Para especificar atributos para el perfil de sobre:

1. Pulse **Administración de cuentas > Perfiles > Socio** y pulse **Buscar**.
2. Seleccione **TP1** en la lista.
3. Pulse **Posibilidades B2B**.
4. Pulse el icono **Expandir** situado junto a **Paquete: N/D**.
5. Pulse el icono **Editar** situado junto a **Protocolo: X12V5R1**.
6. Especifique los siguientes atributos:
   a. En la fila Perfil de sobre, seleccione **EnvProf1** en la lista.
   b. En la fila Calificador de intercambio, escriba **01**.
   c. En la fila Identificador de intercambio, escriba **000000001**.
   d. En el Indicador de uso del intercambio, escriba **T**.
7. Pulse **Guardar**.

En este punto, si el socio interno enviase un documento ROD al concentrador, el documento se transformaría en una transacción 850, que se ensobraría y enviaría al destino del socio.

Capítulo 21. Información adicional de RosettaNet

En este apéndice se proporciona información adicional sobre el soporte RosettaNet. Incluye los siguientes temas:

- "Desactivación de PIPs"
- " Suministro de notificación de anomalías"
- "Creación de paquetes de definición de documentos PIP" en la página 377
- "Paquetes de definición de documentos PIP" en la página 389

Desactivación de PIPs

Acerca de esta tarea

Después de cargar un paquete PIP en WebSphere Partner Gateway, no podrá eliminarse. Sin embargo, puede desactivar el PIP para que no pueda utilizarse.

Para desactivar un PIP para todas las comunicaciones con los socios, lleve a cabo los siguientes pasos:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición de documento**.
2. Expanda las definiciones de documento para revelar el tipo de documento del PIP que desea inhabilitar.
3. En la columna Estado del paquete, pulse **Habilitado**. La columna Estado muestra ahora **Inhabilitado** y WebSphere Partner Gateway no podrá utilizar la definición del documento para el PIP.

Para desactivar una comunicación de PIP con un socio determinado, desactive la conexión con el socio definido para el PIP.

Suministro de notificación de anomalías

PIP 0A1

Si se produce una anomalía durante el proceso de un mensaje PIP, WebSphere Partner Gateway utiliza el PIP 0A1 como mecanismo para enviar la anomalía al socio o al sistema de fondo que ha enviado el mensaje. Por ejemplo, supongamos que un sistema de fondo inicia un PIP 3A4. WebSphere Partner Gateway procesa el mensaje RNSC y envía un mensaje RosettaNet al socio. WebSphere Partner Gateway espera la respuesta al mensaje RosettaNet hasta que el tiempo de espera alcanza el límite establecido. Después de producirse, WebSphere Partner Gateway crea un PIP 0A1 y lo envía al socio. El PIP 0A1 identifica la condición de excepción para que el socio pueda entonces compensar la anomalía del PIP 3A4.

Para proporcionar notificación de anomalías, suba un paquete 0A1 y cree una conexión PIP con el socio utilizando este paquete.

Actualización de la información de contacto

Para cambiar la información de contacto de RosettaNet con el PIP 0A1, debe editar el archivo BCG.Properties, que está en el directorio *<DirProducto>*/router/lib/config.

Estos campos rellenan la información de contacto en el PIP 0A1. Fax es opcional (el valor puede quedar en blanco), pero el resto son necesarios.

- **bcg.0A1.fromContactName**
- **bcg.0A1.fromEMailAddr**
- **bcg.0A1.fromPhoneNbr**
- **bcg.0A1.fromFaxNbr**

Los números de teléfono están limitados a 30 bytes en longitud. El resto de campos no tienen ningún límite de longitud. Si se modifican los valores, se debe reiniciar el Gestor de documentos.

Edición de valores de atributo RosettaNet

Acerca de esta tarea

Para soporte RosettaNet, una definición de documento de tipo de acción tiene un conjunto determinado de atributos. Estos atributos proporcionan información que se utiliza para validar el mensaje PIP, para definir los roles y servicios utilizados en el PIP y para definir la respuesta ante la acción. Los paquetes PIP facilitados por WebSphere Partner Gateway definen automáticamente valores para estos atributos y normalmente no es necesario modificarlos.

Para editar los atributos de RosettaNet de una definición de documento de acción, lleve a cabo los siguientes pasos:

1. Pulse **Administración del concentrador > Configuración del concentrador > Definición del documento**
2. Pulse los iconos **Expandir** para expandir individualmente un nodo al nivel de definición de documento correspondiente o seleccione **Todos** para expandir todo el árbol.
3. La columna Acciones de cada acción contiene un icono **Editar valores de atributo de RosettaNet**. Pulse este icono para editar los atributos de RosettaNet de la acción. La Consola de comunidad muestra un listado de atributos definidos bajo Atributos de RosettaNet.
4. Complete los parámetros siguientes bajo Atributos de RosettaNet. (Estos atributos se definen automáticamente cuando se sube un PIP al sistema).

Tabla 52. Atributos de RosettaNet

Atributo de RosettaNet	Descripción
Nombre de DTD	Identifica el nombre de la acción del PIP en el DTD proporcionado por RosettaNet
De Servicio	Contiene el nombre de servicio del componente de red del socio o del sistema de fondo que está enviando el mensaje
A Servicio	Contiene el nombre de servicio de componente de red del socio o sistema de fondo que está recibiendo el mensaje
De rol	Contiene el nombre de rol del socio o sistema de fondo que está enviando el mensaje
A rol	Contiene el nombre de rol del socio o sistema de fondo que está recibiendo el mensaje
Distintivo raíz	Contiene el nombre del elemento raíz en el documento XML asociado con el PIP
Respuesta desde Nombre de acción	Identifica la siguiente Acción que debe realizarse en el PIP

Nota: si la consola muestra el mensaje `No se ha encontrado ningún atributo`, significa que los atributos no se han definido.

5. Si la consola muestra este mensaje para una definición de nivel inferior, la definición podría seguir siendo válida pues heredaría los atributos de la definición de nivel superior. La adición de atributos y de sus valores modifica los atributos heredados y cambia la función de la definición del documento.
6. Pulse **Guardar**.

Creación de paquetes de definición de documentos PIP

Acerca de esta tarea

Puesto que RosettaNet en ocasiones añade PIP, quizás necesite crear sus propios paquetes PIP para dar soporte a estos nuevos PIP o para dar soporte a ampliaciones de los PIP. Excepto donde se indique lo contrario, los procedimientos en este apartado describes cómo crear el paquete de definición de documento PIP para PIP 5C4 V01.03.00. WebSphere Partner Gateway proporciona un paquete de definición de documento PIP para PIP 5C4 V01.02.00. Los procedimientos, por lo tanto, documentan cómo realizar una actualización. Sin embargo, la creación de un paquete de definición de documento PIP es similar y los procedimientos identifican cualquier paso adicional.

Antes de empezar, descargue las especificaciones de PIP de www.rosettanet.org para la nueva versión y, si está realizando una actualización, la versión anterior. Por ejemplo, si está realizando la actualización que se describe en los procedimientos, descargue 5C4_DistributeRegistrationStatus_V01_03_00.zip y 5C4_DistributeRegistrationStatus_V01_02_00.zip. La especificación incluye los siguientes tipos de archivo:

- Directrices para mensajes XML de RosettaNet - Los archivos HTML como 5C4_MG_V01_03_00_RegistrationStatusNotification.htm que definen la cardinalidad, el vocabulario, la estructura y los valores de elementos de datos y los tipos de valores permitidos del PIP.
- Esquema de mensaje XML de RosettaNet - Los archivos DTD como 5C4_MS_V01_03_RegistrationStatusNotification.dtd que definen el orden o secuencia, la nomenclatura de elementos, la composición y los atributos del PIP.
- Especificación de PIP - el archivo DOC (por ejemplo 5C4_Spec_V01_03_00.doc) que proporciona los controles de rendimiento empresarial del PIP.
- Notas de release de PIP - el archivo DOC (por ejemplo 5C4_V01_03_00_ReleaseNotes.doc) que describe la diferencia entre esta versión y la versión anterior.

La creación o actualización de un paquete de definición de documento PIP implica los siguientes procedimientos:

- Creación de los archivos XSD
- Creación del archivo XML
- Creación de los paquetes

Creación de los archivos XSD

Acerca de esta tarea

Un paquete de definición de documento PIP contiene archivos de esquema XML que definen formatos de mensajes y valores aceptables para elementos. El siguiente procedimiento describe cómo crear estos archivos basándose en el contenido del archivo de especificación de PIP.

En el archivo de especificación de PIP, se creará como mínimo un archivo XSD para cada archivo DTD. En el ejemplo de la actualización a PIP 5C4 V01.03.00, puesto que ha cambiado el formato de mensaje, el procedimiento describe cómo crear el archivo BCG_5C4RegistrationStatusNotification_V01.03.xsd como ejemplo. Para obtener más información acerca de los archivos XSD, consulte el apartado "Acerca de la validación" en la página 387.

Para crear los archivos XSD para el paquete de definición de documento PIP, lleve a cabo los siguientes pasos:

1. Importe o suba el archivo DTD a un editor de XML como WebSphere Studio Application Developer. Por ejemplo, cargue el archivo 5C4_MS_V01_03_RegistrationStatusNotification.dtd.
2. Utilizando el editor XML, convierta el DTD en un esquema XML. Los pasos siguientes describen cómo llevar a cabo esto con la ayuda del Application Developer:
   a. En el panel de navegación de la perspectiva XML, abra el proyecto que contiene el archivo DTD importado.
   b. Pulse el botón derecho sobre el archivo DTD y seleccione **Generar > Esquema XML**.
   c. En el panel Generar, escriba o seleccione en qué posición desea guardar el nuevo archivo XSD. En el campo Nombre de archivo, escriba el nombre del nuevo archivo XSD. En el ejemplo, el nombre BCG_5C4RegistrationStatusNotification_V01.03.xsd.
   d. Pulse **Finalizar**.
3. Compense los elementos que tienen múltiples valores de cardinalidad en las directrices de XML de RosettaNet añadiendo especificaciones al nuevo archivo XSD. Las directrices muestran los elementos del mensaje en forma de árbol, mostrando la cardinalidad de cada elemento a la izquierda del elemento.

   Normalmente, los elementos de las directrices coinciden con las definiciones de los elementos en el archivo DTD. Sin embargo, las directrices podrían incluir algunos elementos que tienen los mismos nombres pero cardinalidades diferentes. Puesto que DTD no puede proporcionar la cardinalidad en este caso, será necesario modificar el XSD. Por ejemplo, el archivo de directrices 5C4_MG_V01_03_00_RegistrationStatusNotification.htm tiene una definición de ContactInformation en la línea 15 que tiene cinco elementos hijo con las siguientes cardinalidades:

   1 contactName

   0..1 EmailAddress

   0..1 facsimileNumber

   0..1 PhysicalLocation

   0..1 telephoneNumber

   La definición de ContactInformation de la línea 150 tiene cuatro elementos hijo con las siguientes cardinalidades:

   1 contactName

1 EmailAddress

0..1 facsimileNumber

1 telephoneNumber

En el archivo XSD, sin embargo, cada hijo de ContactInformation tiene una cardinalidad que obedece a ambas definiciones:

```
<xsd:element name="ContactInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="contactName"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="facsimileNumber"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="PhysicalLocation"/>
      <xsd:element maxOccurs="1" minOccurs="0" ref="telephoneNumber"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Si está actualizando el paquete de definición de documento PIP basándose en otra versión del paquete y desea reutilizar una definición de la otra versión, lleve a cabo los siguientes pasos para cada una de estas definiciones:

a. Suprima la definición del elemento. Por ejemplo, suprima el elemento ContactInformation.

b. Abra el paquete de definición de documento PIP de la versión que está sustituyendo. Por ejemplo, abra el archivo BCG_Package_RNIFV02.00_5C4V01.02.zip.

c. Busque la definición que desea volver a utilizar. Por ejemplo, la definición de ContactInformation_tipo7 en el archivo BCG_ContactInformation_Types.xsd coincide con la definición que se necesita para la línea 15 de las directrices.

```
<xsd:complexType name="ContactInformation_type7">
  <xsd:sequence>
    <xsd:element name="contactName" type="common_FreeFormText_R"/>
    <xsd:element name="EmailAddress" type="common_EmailAddres_R"
        minOccurs="0"/>
    <xsd:element name="facsimileNumber"
        type="common_CommunicationsNumber_R" minOccurs="0"/>
    <xsd:element name="PhysicalLocation"
        type="PhysicalLocation_type1" minOccurs="0" />
    <xsd:element name="telephoneNumber"
        type="common_CommunicationsNumber_R minOccurs="0" />
  </xsd:sequence>
</xsd:complexType>
```

d. En el nuevo archivo XSD que está creando para el paquete de definición de documento PIP actualizado, cree una referencia al archivo XSD que contiene la definición que desea reutilizar. Por ejemplo, cree una referencia a BCG_ContactInformation_Types.xsd en el archivo BCG_5C4RegistrationStatusNotification_V01.03.xsd del siguiente modo:

```
<xsd:include schemaLocation="BCG_ContactInformation_Types.xsd"/>
```

e. En el nuevo archivo XSD, suprima el atributo ref de los elementos que se refieren al elemento que ha suprimido. Añada un atributo de tipo que se refiera a la definición que está reutilizando. Por ejemplo, en el elemento productProviderFieldApplicationEngineer, suprima *ref="Contact Information"* y añada la siguiente información:

```
name="ContactInformation"
 type="ContactInformation_type7"
```

Si está creando un paquete de definición de documento PIP o actualizando un paquete de definición de documento PIP pero la definición que necesita no

existe en la otra versión, lleve a cabo los siguientes pasos para cada instancia del elemento que encuentre en las directrices:

a. Suprima la definición del elemento. Por ejemplo, suprima el elemento ContactInformation.

b. Cree una definición sustitutiva. Por ejemplo, cree la definición ContactInformation_localType1 para la definición de la línea 15 de las directrices.

```
<xsd:complexType name="ContactInformation_localType1">
  <xsd:sequence>
    <xsd:element ref="contactName"/>
    <xsd:element maxOccurs="1" minOccurs="0" ref="EmailAddress"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="facsimileNumber"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="PhysicalLocation"/>
    <xsd:element maxOccurs="1" minOccurs="0"
        ref="telephoneNumber"/>
  </xsd:sequence>
</xsd:complexType>
```

c. Para los elementos que se refieran al elemento que ha suprimido, suprima su atributo ref y añada un atributo de tipo que se refiera al tipo complejo apropiado definido en el paso anterior. Por ejemplo, en el elemento productProviderFieldApplicationEngineer, suprima *ref="Contact Information"* y añada la siguiente información:

```
name="ContactInformation"
type="ContactInformation_localType1"
```

La Figura 35 muestra el elemento productProviderFieldApplicationEngineer antes de modificarse.

```
<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="ContactInformation"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figura 35. Elemento productProviderFieldApplicationEngineer previo a la modificación

La Figura 36 muestra el elemento productProviderFieldApplicationEngineer después de modificarse.

```
<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ContactInformation"
          type="ContactInformation_localType1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figura 36. Elemento productProviderFieldApplicationEngineer después de su modificación

4. Especifique los valores de enumeración para los elementos que sólo pueden tener valores específicos. Las directrices definen los valores de enumeración en las tablas del apartado Información de directrices.

   Por ejemplo, en un mensaje PIP 5C4 V01.03.00, GlobalRegistrationComplexityLevelCode sólo puede tener los siguientes valores: Above average (por encima de la media), Average (normal), Maximum (máximo), Minimum (mínimo), None (ninguno) y Some (alguno).

Si está actualizando el paquete de definición de documento PIP basándose en otra versión del paquete y desea reutilizar un conjunto de valores de enumeración de la otra versión, lleve a cabo los siguientes pasos para cada conjunto:

a. Suprima la definición para el elemento. Por ejemplo, suprima el elemento GlobalRegistrationComplexityLevelCode:

b. Abra el paquete de definición de documento PIP de la versión que está sustituyendo. Por ejemplo, abra el archivo BCG_Package_RNIFV02.00_5C4V01.02.zip.

c. Busque la definición que contiene los valores de enumeración que desea reutilizar. Por ejemplo, la definición _GlobalRegistrationComplexityLevelCode del archivo BCG_GlobalRegistrationComplexityLevelCode.xsd contiene las definiciones del valor de enumeración que se definen en la tabla Instancia de entidad.

```
<xsd:simpleType name="_GlobalRegistrationComplexityLevelCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Above average"/>
    <xsd:enumeration value="Average"/>
    <xsd:enumeration value="Maximum"/>
    <xsd:enumeration value="Minimum"/>
    <xsd:enumeration value="None"/>
    <xsd:enumeration value="Some"/>
  </xsd:restriction>
</xsd:simpleType>
```

d. En el nuevo archivo XSD que está creando para el paquete de definición de documento PIP actualizado, cree una referencia al archivo XSD que contiene la definición que desea reutilizar. Por ejemplo, cree una referencia a BCG_GlobalRegistrationComplexityLevelCode.xsd en el archivo BCG_5C4RegistrationStatusNotification_V01.03.xsd del siguiente modo:

```
<xsd:include schemaLocation=
    "BCG_GlobalRegistrationComplexityLevelCode_Types.xsd" />
```

e. En el nuevo archivo XSD, suprima el atributo ref de los elementos que se refieren al elemento que ha suprimido. Añada un atributo de tipo que se refiera a la definición que está reutilizando. Por ejemplo, en el elemento DesignAssemblyInformation, suprima *ref*=”GlobalRegistrationComplexityLevelCode” y añada la siguiente información:

```
name="GlobalRegistrationComplexityLevelCode"
type="_GlobalRegistrationComplexityLevelCode"
```

Si está creando un paquete de definición de documento PIP o actualizando un paquete de definición de documento PIP pero las definiciones del valor de enumeración que necesita no existen en la otra versión, lleve a cabo los siguientes pasos para cualquier elemento con valores enumerados en las directrices:

a. Suprima la definición del elemento. Por ejemplo, suprima el elemento GlobalRegistrationComplexityLevelCode.

b. Cree una definición sustitutiva. Por ejemplo, cree la definición GlobalRegistrationComplexityLevelCode_localType e incluya las definiciones del valor de enumeración tal como se describen en la tabla.

```
<xsd:simpleType
    name="GlobalRegistrationComplexityLevelCode_localType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Above average"/>
    <xsd:enumeration value="Average"/>
    <xsd:enumeration value="Maximum"/>
    <xsd:enumeration value="Minimum"/>
```

```
          <xsd:enumeration value="None"/>
          <xsd:enumeration value="Some"/>
        </xsd:restriction>
      </xsd:simpleType>
```

c. Para los elementos que se refieran al elemento que ha suprimido, suprima su atributo ref y añada un atributo de tipo que se refiera al tipo complejo apropiado definido en el paso anterior. Por ejemplo, suprima *ref="GlobalRegistrationComplexityLevelCode"* y añada la siguiente información:

```
name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"
```

La Figura 37 muestra el elemento DesignAssemblyInformation antes de modificarse.

```
<xsd:element name="DesignAssemblyInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="assemblyComments"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="demandCreatorTrackingIdentifier"/>
      <xsd:element maxOccurs="unbounded" minOccurs="0"
          ref="DesignPartInformation"/>
      <xsd:element ref="DesignRegistrationIdentification"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="GeographicRegion"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="GlobalRegistrationComplexityLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
          ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figura 37. Elemento DesignAssemblyInformation previo a la modificación

La Figura 38 en la página 383 muestra el elemento DesignAssemblyInformation después de modificarse.

```
<xsd:element name="DesignAssemblyInformation">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="assemblyComments"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="demandCreatorTrackingIdentifier"/>
      <xsd:element maxOccurs="unbounded" minOccurs="0"
         ref="DesignPartInformation"/>
      <xsd:element ref="DesignRegistrationIdentification"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="GeographicRegion"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         name="GlobalRegistrationComplexityLevelCode"
           type="GlobalRegistrationComplexityLevelCode_localType"/>

      <xsd:element maxOccurs="1" minOccurs="0"
         ref="GlobalRegistrationInvolvementLevelCode"/>
      <xsd:element maxOccurs="1" minOccurs="0"
         ref="RegistrationStatus"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figura 38. Elemento DesignAssemblyInformation después de la modificación

5. Establezca el tipo de datos, la longitud mínima, la longitud máxima y la representación de las entidades de datos. Las directrices de mensajes XML de RosettaNet proporcionan esta información en la tabla Entidades de datos empresariales fundamentales.

   Si está actualizando el paquete de definición de documento PIP basándose en otra versión del paquete y desea reutilizar una definición de entidad de datos de otra versión, lleve a cabo los siguientes pasos para cada conjunto:

   a. Suprima la definición para el elemento de entidad de datos. Por ejemplo, suprima el elemento DateStamp.

   b. Abra el paquete de definición de documento PIP de la versión que está sustituyendo. Por ejemplo, abra el archivo BCG_Package_RNIFV02.00_5C4V01.02.zip.

   c. Busque la definición que desea volver a utilizar. Por ejemplo, la definición _common_DateStamp_R del archivo BCG_common.xsd contiene la siguiente definición, que se ajusta a la información indicada en las directrices.

      ```
      <xsd:simpleType name="_common_DateStamp_R">
        <xsd:restriction base="xsd:string">
          <xsd:pattern value="[0-9]{8}Z" />
        </xsd:restriction>
      </xsd:simpleType>
      ```

   d. En el nuevo archivo XSD que está creando para el paquete de definición de documento PIP actualizado, cree una referencia al archivo XSD que contiene la definición que desea reutilizar. Por ejemplo, cree una referencia al archivo BCG_common.xsd en el archivo BCG_5C4RegistrationStatusNotification_V01.03.xsd del siguiente modo:

      ```
      <xsd:include schemaLocation="BCG_common.xsd" />
      ```

   e. En el nuevo archivo XSD, suprima el atributo ref de los elementos que se refieren al elemento que ha suprimido. Añada un atributo de tipo que se refiera a la definición que está reutilizando. Por ejemplo, en el elemento DesignAssemblyInformation, suprima *ref*=”DateStamp” y añada la siguiente información:

      ```
      name="DateStamp" type="_common_DateStamp_R"
      ```

Si está creando un paquete de definición de documento PIP o está actualizando un paquete de definición de documento PIP pero la definición de entidad de datos que necesita no existe en la otra versión, lleve a cabo los siguientes pasos para cada elemento de entidad de datos:

a. Suprima la definición del elemento. Por ejemplo, suprima el elemento DateStamp.

b. Cree una definición sustitutiva. Por ejemplo, utilice el tipo de datos, la longitud mínima, la longitud máxima y la representación para crear la definición DateStamp_localType.

```
<xsd:simpleType name="DateStamp_localType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{8}Z" />
  </xsd:restriction>
</xsd:simpleType>
```

c. Para los elementos que se refieran al elemento que ha suprimido, suprima su atributo ref y añada un atributo de tipo que se refiera al tipo complejo apropiado definido en el paso anterior. Por ejemplo, suprima *ref="DateStamp"* y añada la siguiente información:

```
name="DateStamp" type="DateStamp_localType"
```

La Figura 39 muestra el elemento beginDate antes de modificarse.

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element ref="DateStamp"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figura 39. Elemento beginDate previo a la modificación

La Figura 40 muestra el elemento beginDate después de modificarse.

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element name="DateStamp" type="DateStamp_localType"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figura 40. Elemento beginDate después de la modificación

Creación del archivo XML

Acerca de esta tarea

Después de haber creado los archivos XSD para el paquete de definición de documento PIP, ya puede crear el archivo XML para el paquete RNIF y el archivo XML para el paquete de integración de fondo. Por ejemplo, estos paquetes se denominan BCG_Package_RNIFV02.00_5C4V01.03.zip y BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.03.zip. El siguiente procedimiento describe cómo crear el archivo XML para el paquete RNIF:

1. Extraiga el archivo XML de un archivo de definición de documento PIP RNIF. Si está efectuando una actualización, extraiga el archivo de la versión anterior del paquete (por ejemplo, BCG_Package_RNIFV02.00_5C4V01.02.zip). Si está creando un nuevo paquete, extraiga el archivo de un paquete de definición de documento PIP que sea similar al que está creando. Por ejemplo, si está

creando un paquete para dar soporte a un PIP de dos acciones, copie el archivo XML de otro paquete PIP de dos acciones.

2. Copie el archivo y cámbiele el nombre del modo pertinente (por ejemplo, BCG_RNIFV02.00_5C4V01.03.xml).
3. En el archivo nuevo, actualice los elementos que contienen información sobre el PIP. Por ejemplo, la tabla siguiente muestra la información que debe actualizarse en el ejemplo del PIP 5C4. Observe que la información podría aparecer más de una vez en el archivo. Asegúrese de actualizar todas las instancias.

Tabla 53. Información de actualización de PIP 5C4

Información que debe modificarse	**Valor anterior**	**Valor nuevo**
ID de PIP	5C4	5C4
Versión de PIP	V01.02	V01.03
El nombre del archivo DTD del mensaje de solicitud sin la extensión del archivo	5C4_MS_V01_02_ RegistrationStatusNotification	5C4_MS_V01_03_ RegistrationStatusNotification
El nombre del archivo DTD del mensaje de confirmación sin la extensión del archivo (sólo para PIP de dos acciones)	N/D	N/D
El nombre del archivo XSD del mensaje de solicitud sin la extensión del archivo	BCG_5C4RegistrationStatus Notification_V01.02	BCG_5C4RegistrationStatus Notification_V01.03
El nombre del archivo XSD del mensaje de confirmación sin la extensión del archivo (sólo para PIP de dos acciones)	N/D	N/D
Nombre del elemento raíz en el archivo XSD para el mensaje de solicitud	Notificación Pip5C4RegistrationStatus	Notificación Pip5C4RegistrationStatus
Nombre del elemento raíz en el archivo XSD para el mensaje de confirmación (sólo para PIP de dos acciones)	N/D	N/D

4. Abra el documento de la especificación de PIP y utilícelo para actualizar la información que aparece en la tabla siguiente. Si está realizando una actualización, compare las especificaciones de las versiones, pues quizás no sea necesario que actualice estos valores.

Tabla 54. Información de actualización de PIP 5C4 de la especificación de PIP

Información que debe actualizarse	Descripción	Valor en el paquete 5C4
Nombre de la actividad	Especificado en la tabla 3-2	Distribución de estado de registro
Nombre de rol del iniciador	Especificado en la tabla 3-1	Proveedor de productos
Nombre de rol del respondedor	Especificado en la tabla 3-1	Creador de la demanda
Nombre de acción de solicitud	Especificado en la tabla 4-2	Notificación de estado de registro
Nombre de acción de confirmación	Especificado en la tabla 4-2 (sólo para PIP de dos acciones)	N/D

5. Actualice los valores de los atributos del paquete. Si está realizando una actualización, compare las especificaciones de las versiones, pues quizás no sea necesario que actualice estos valores.

   Nota: si está creando el paquete de integración de programas de fondo, omita este paso y vaya al paso 6 en la página 387.

Tabla 55. Actualizaciones de los atributos de PIP 5C4

Información que debe actualizarse	Descripción	Valor en el paquete 5C4	Vía de acceso del elemento en el archivo XML
NonRepudiation necesario	Especificado en la tabla 3-3	N	ns1:Paquete ns1:Protocolo ns1:Proceso ns1:Atributo (Su ATTRIBUTEKEY es NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
No rechazo de recibo	Especificado en la tabla 3-3	N	ns1:Paquete ns1:Protocolo ns1:Proceso ns1:Atributo (Su ATTRIBUTEKEY es NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
Firma digital necesaria	Especificado en la tabla 5-1	Y	ns1:Paquete ns1:Protocolo ns1:Proceso ns1:Atributo (Su ATTRIBUTEKEY es DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
TimeToAcknowledge	Especificado en la tabla 3-3	2 (120 min)	ns1:Paquete ns1:Protocolo ns1:Proceso ns1:Atributo (Su ATTRIBUTEKEY es TimeToAcknowledge) ns1:AttributeValue ATTRVALUE
TimeToPerform	Especificado en la tabla 3-3	2 (120 min)	ns1:Paquete ns1:Protocolo ns1:Proceso ns1:Atributo (Su ATTRIBUTEKEY es TimeToPerform) ns1:AttributeValue ATTRVALUE
RetryCount	Especificado en la tabla 3-3	3	ns1:Paquete ns1:Protocolo ns1:Proceso ns1:Atributo (Su ATTRIBUTEKEY es RetryCount) ns1:AttributeValue ATTRVALUE

6. Actualice los elementos ns1:Package/ns1:Protocol/GuidelineMap para eliminar los archivos XSD que no se utilicen y para añadir los archivos XSD que se han creado o para los que se han establecido referencias.

Para crear el paquete de integración de programas de fondo, repita los pasos 1 en la página 384 a 6, con las diferencias siguientes:

- En el paso 1 en la página 384, extraiga el archivo XML del paquete de integración de programas de fondo (por ejemplo, BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip).
- No lleve a cabo el paso 5 en la página 386.

Después de crear los archivos XML y XSD, podrá crear los paquetes de flujo de documentos PIP.

Creación del paquete

Acerca de esta tarea

Para crear el paquete RNIF, siga estos pasos:

1. Cree un directorio GuidelineMaps y copie los archivos XSD del paquete en este directorio.
2. Cree un directorio Packages y copie el archivo XML RNIF en este directorio.
3. Vaya al directorio padre y cree un paquete de definición de documento PIP (archivo ZIP) que contenga los directorios GuidelineMaps y Packages. Debe respetar la estructura de directorios del archivo ZIP.

Para crear el paquete de integración de programas de fondo, siga los pasos 1 a 3, pero utilice el archivo XML de la integración de programas de fondo del archivo RNIF.

Tras crear el paquete PIP, puede subirlo mediante el procedimiento descrito en "Paquetes de tipo de documento RNIF y PIP" en la página 114.

Acerca de la validación

WebSphere Partner Gateway valida el contenido de servicio de un mensaje RosettaNet utilizando correlaciones de validación. Estas correlaciones de validación definen la estructura de un mensaje válido y definen su cardinalidad, formato y los valores válidos (enumeración) de los elementos del mensaje. Dentro de cada paquete de definición de documento PIP, WebSphere Partner Gateway proporciona las correlaciones de validación como archivos XSD en el directorio GuidelineMaps.

Debido a que RosettaNet especifica el formato de un mensaje PIP, generalmente no necesitará personalizar las correlaciones de validación. Sin embargo, si lo necesita, consulte el apartado "Creación de paquetes de definición de documentos PIP" en la página 377 para obtener información acerca de los pasos necesarios para actualizar los archivos XSD utilizados para validar los mensajes y para saber cómo crear un paquete de definición de documento PIP.

Cardinalidad

La cardinalidad determina el número de veces que un elemento particular puede o debe aparecer en un mensaje. En las correlaciones de validación, los atributos minOccurs y maxOccurs determinan la cardinalidad del atributo, tal como se muestra en el ejemplo de BCG_5C4RegistrationStatusNotification_V01.02.xsd:

```
<xsd:element name="GeographicRegion" type="GeographicRegionType"
    minOccurs="0"/>
```

Si WebSphere Partner Gateway no necesita comprobar la cardinalidad de un elemento, los valores de los atributos minOccurs y maxOccurs del elemento en la correlación de validación son "0" y "unbounded", tal como se indica en el ejemplo siguiente:

```
<xsd:element name="DesignRegistrationIdentification"
    type="DesignRegistrationIdentificationType2"
    minOccurs="0" maxOccurs="unbounded"/>
```

Formato

El formato determina la disposición o diseño de los datos para el tipo de un elemento. En las correlaciones de validación, el tipo tiene una o más restricciones como se muestra en los siguientes ejemplos:

Ejemplo 1

```
<xsd:simpleType name="_common_LineNumber_R">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1" />
    <xsd:maxLength value="6" />
  </xsd:restriction>
</xsd:simpleType>
```

Todos los elementos de tipo _common_LineNumber_R de un mensaje deben ser Strings y deben tener una longitud de entre 1 y 6 caracteres.

Ejemplo 2

```
<xsd:simpleType name="_GlobalLocationIdentifier">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{9}.{1,4}" />
  </xsd:restriction>
</xsd:simpleType>
```

Todos los elementos de tipo _GlobalLocationIdentifier de un mensaje deben ser Strings y deben tener nueve caracteres de datos numéricos seguidos por entre uno y cuatro caracteres de datos alfanuméricos. Por lo tanto, la longitud mínima es 10 caracteres y la máxima es 13.

Ejemplo 3

```
<xsd:element name="DayOfMonth">
  <xsd:simpleType>
    <xsd:restriction base="xsd:positiveInteger">
      <xsd:totalDigits value="2" />
      <xsd:minInclusive value="1" />
      <xsd:maxInclusive value="31" />
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
```

Todos los elementos de tipo _DayofMonth de un mensaje deben ser PositiveInteger, deben tener uno o dos caracteres y deben tener un valor entre 1 y 31 (ambos inclusive).

Enumeración

La enumeración determina los valores válidos para un elemento. En las correlaciones de validación, el tipo del elemento tiene una o varias restricciones de enumeración, tal como muestra el ejemplo siguiente:

```
<xsd:simpleType name="_local_GlobalDesignRegistrationNotificationCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Initial" />
    <xsd:enumeration value="Update" />
  </xsd:restriction>
</xsd:simpleType>
```

Todos los elementos de tipo _local_GlobalDesignRegistrationNotificationCode de un mensaje deben tener sólo "Initial" o "Update" como valores.

Paquetes de definición de documentos PIP

En los apartados siguientes se muestran los paquetes de definición de documento PIP proporcionados por WebSphere Partner Gateway para cada PIP. Dentro de cada paquete hay un archivo XML contenido en un directorio Packages y varios archivos XSD contenidos en un directorio GuidelineMaps, que son comunes a todos los paquetes de definición de documento PIP del PIP.

0A1 Notificación de anomalía V1.0

En el apartado siguiente se describe el contenido de PIP 0A1 Notificación de anomalía V1.0.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 0A1 Notificación de anomalía V1.0. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 56. Archivos ZIP y XML de PIP 0A1 Notificación de anomalía V1.0

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_0A11.0.zip	BCG_RNIF1.1_0A11.0.xml
BCG_Package_RNSC1.0_RNIF1.1_0A11.0.zip	BCG_RNSC1.0_RNIF1.1_0A11.0.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 0A1 Notificación de anomalía V1.0:

- 0A1FailureNotification_1.0.xml
- BCG_0A1FailureNotification_1.0.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

0A1 Notificación de anomalía V02.00

En el apartado siguiente se describe el contenido de PIP 0A1 Notificación de anomalía V02.00.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 0A1 Notificación de anomalía V02.00. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 57. Archivos ZIP y XML de PIP 0A1 Notificación de anomalía V02.00

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIFV02.00_0A1V02.00.zip	BCG_RNIFV02.00_0A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_0A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_0A1V02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 0A1 Notificación de anomalía V02.00:

- 0A1FailureNotification_V02.00.xml
- BCG_0A1FailureNotification_V02.00.xsd
- BCG_common.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

2A1 Distribución de información de nuevo producto

En el apartado siguiente se describe el contenido de PIP 2A1 Distribución de información de nuevo producto.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 2A1 Distribución de información de nuevo producto. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 58. Archivos ZIP y XML de 2A1 Distribución de información de nuevo producto

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_2A1V02.00.zip	BCG_RNIF1.1_2A1V02.00.xml
BCG_Package_RNIFV02.00_2A1V02.00.zip	BCG_RNIFV02.00_2A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_2A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_2A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_2A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_2A1V02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 2A1 Distribución de información de nuevo producto:

- BCG_2A1ProductCatalogInformationNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd

- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalProductAssociationCode_V43.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode_V43.xsd
- BCG_GlobalProductTypeCode_V43.xsd
- BCG_GlobalProductUnitofMeasureCode_V43.xsd
- BCG_GlobalProprietaryProductIdentificationTypeCode_V43.xsd
- BCG_GlobalStandardClassificationSchemeCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

2A12 Distribución de maestro de productos

En el apartado siguiente se describe el contenido de PIP 2A12 Distribución de maestro de productos.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 2A12 Distribución de maestro de productos. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 59. Archivos ZIP y XML de 2A12 Distribución de maestro de productos

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_2A12V01.03.zip	BCG_RNIF1.1_2A12V01.03.xml
BCG_Package_RNIFV02.00_2A12V01.03.zip	BCG_RNIFV02.00_2A12V01.03.xml
BCG_Package_RNSC1.0_RNIF1.1_2A12V01.03.zip	BCG_RNSC1.0_RNIF1.1_2A12V01.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_2A12V01.03.zip	BCG_RNSC1.0_RNIFV02.00_2A12V01.03.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 2A12 Distribución de maestro de productos:

- BCG_2A12ProductMasterNotification_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAssemblyLevelCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalLeadTimeClassificationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductLifeCycleStatusCode.xsd
- BCG_GlobalProductProcurementTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A1 Solicitud de oferta

En el apartado siguiente se describe el contenido de PIP 3A1 Solicitud de oferta.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A1 Solicitud de oferta. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 60. Archivos ZIP y XML de PIP 3A1 Solicitud de oferta

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A1V02.00.zip	BCG_RNIF1.1_3A1V02.00.xml
BCG_Package_RNIFV02.00_3A1V02.00.zip	BCG_RNIFV02.00_3A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_3A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A1V02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A1 Solicitud de oferta:

- BCG_3A1QuoteConfirmation_V02.00.xsd
- BCG_3A1QuoteRequest_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalQuoteLineItemStatusCode.xsd
- BCG_GlobalQuoteTypeCode.xsd
- BCG_GlobalStockIndicatorCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A2 Solicitud de precio y disponibilidad

En el apartado siguiente se describe el contenido de PIP 3A2 Solicitud de precio y disponibilidad.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A2 Solicitud de precio y disponibilidad. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 61. Archivos ZIP y XML de 3A2 Solicitud de precio y disponibilidad

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A2R02.01.zip	BCG_RNIF1.1_3A2R02.01.xml
BCG_Package_RNIFV02.00_3A2R02.01.zip	BCG_RNIFV02.00_3A2R02.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3A2R02.01.zip	BCG_RNSC1.0_RNIF1.1_3A2R02.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A2R02.01.zip	BCG_RNSC1.0_RNIFV02.00_3A2R02.01.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A2 Solicitud de precio y disponibilidad:

- BCG_3A2PriceAndAvailabilityRequest_R02.01.xsd
- BCG_3A2PriceAndAvailabilityResponse_R02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerAuthorizationCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPricingTypeCode.xsd
- BCG_GlobalProductAvailabilityCode.xsd
- BCG_GlobalProductStatusCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A4 Solicitud de pedido de compra V02.00

En el apartado siguiente se describe el contenido de PIP 3A4 Solicitud de pedido de compra V02.00.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A4 Solicitud de pedido de compra. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 62. Archivos ZIP y XML de 3A4 Solicitud de pedido de compra

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A4V02.00.zip	BCG_RNIF1.1_3A4V02.00.xml
BCG_Package_RNIFV02.00_3A4V02.00.zip	BCG_RNIFV02.00_3A4V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A4V02.00.zip	BCG_RNSC1.0_RNIF1.1_3A4V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A4V02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A4 Solicitud de pedido de compra:

- BCG_3A4PurchaseOrderConfirmation_V02.00.xsd
- BCG_3A4PurchaseOrderRequest_V02.00.xsd

- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShipmentTermsCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTaxExemptionCode_V422.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A4 Solicitud de pedido de compra V02.02

En el apartado siguiente se describe el contenido de PIP 3A4 Solicitud de pedido de compra V02.00.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A4 Solicitud de pedido de compra. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 63. Archivos ZIP y XML de 3A4 Solicitud de pedido de compra

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A4V02.02.zip	BCG_RNIF1.1_3A4V02.02.xml
BCG_Package_RNIFV02.00_3A4V02.02.zip	BCG_RNIFV02.00_3A4V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A4V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A4V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A4V02.02.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A4 Solicitud de pedido de compra:

- BCG_3A4PurchaseOrderConfirmation_V02.02.xsd
- BCG_3A4PurchaseOrderRequest_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd

- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A5 Consulta del estado del pedido

En el apartado siguiente se describe el contenido de PIP 3A5 Consulta del estado del pedido.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A5 Consulta del estado del pedido. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 64. Archivos ZIP y XML de 3A5 Consulta del estado del pedido

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A5R02.00.zip	BCG_RNIF1.1_3A5R02.00.xml
BCG_Package_RNIFV02.00_3A5R02.00.zip	BCG_RNIFV02.00_3A5R02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3A5R02.00.zip	BCG_RNSC1.0_RNIF1.1_3A5R02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A5R02.00.zip	BCG_RNSC1.0_RNIFV02.00_3A5R02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A5 Consulta del estado del pedido:

- BCG_3A5PurchaseOrderStatusQuery_R02.00.xsd
- BCG_3A5PurchaseOrderStatusResponse_R02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalCustomerTypeCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd

- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriority
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A6 Distribución del estado del pedido

En el apartado siguiente se describe el contenido de PIP 3A6 Distribución del estado del pedido.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A6 Distribución del estado del pedido. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 65. Archivos ZIP y XML de 3A6 Distribución del estado del pedido

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A6V02.02.zip	BCG_RNIF1.1_3A6V02.02.xml
BCG_Package_RNIFV02.00_3A6V02.02.zip	BCG_RNIFV02.00_3A6V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A6V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A6V02.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A6V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A6V02.02.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A6 Distribución del estado del pedido:

- BCG_3A6PurchaseOrderStatusNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalCountryCode.xsd

- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalNotificationReasonCode.xsd
- BCG_GlobalOrderQuantityTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A7 Notificación de actualización de pedido de compra

En el apartado siguiente se describe el contenido de PIP 3A7 Notificación de actualización de pedido de compra.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A7 Notificación de actualización de pedido de compra. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 66. Archivos ZIP y XML de 3A7 Notificación de actualización de pedido de compra

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A7V02.02.zip	BCG_RNIF1.1_3A7V02.02.xml
BCG_Package_RNIFV02.00_3A7V02.02.zip	BCG_RNIFV02.00_3A7V02.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A7V02.02.zip	BCG_RNSC1.0_RNIF1.1_3A7V02.02.xml

Tabla 66. Archivos ZIP y XML de 3A7 Notificación de actualización de pedido de compra (continuación)

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNSC1.0_RNIFV02.00_3A7V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A7V02.02.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A7 Notificación de actualización de pedido de compra:

- BCG_3A7PurchaseOrderUpdateNotification_V02.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A8 Notificación de actualización de pedido de compra V01.02

En el apartado siguiente se describe el contenido de PIP 3A8 Notificación de actualización de pedido de compra V01.02.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A8 Notificación de actualización de pedido de compra. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 67. Archivos ZIP y XML de 3A8 Notificación de actualización de pedido de compra

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A8V01.02.zip	BCG_RNIF1.1_3A8V01.02.xml
BCG_Package_RNIFV02.00_3A8V01.02.zip	BCG_RNIFV02.00_3A8V01.02.xml
BCG_Package_RNSC1.0_RNIF1.1_3A8V01.02.zip	BCG_RNSC1.0_RNIF1.1_3A8V01.02.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.02.zip	BCG_RNSC1.0_RNIFV02.00_3A8V01.02.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A8 Notificación de actualización de pedido de compra:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.02.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalPriceUnitOfMeasureCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd

- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A8 Notificación de actualización de pedido de compra V01.03

En el apartado siguiente se describe el contenido de PIP 3A8 Notificación de actualización de pedido de compra V01.03.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A8 Notificación de actualización de pedido de compra. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 68. Archivos ZIP y XML de 3A8 Notificación de actualización de pedido de compra

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A8V01.03.zip	BCG_RNIF1.1_3A8V01.03.xml
BCG_Package_RNIFV02.00_3A8V01.03.zip	BCG_RNIFV02.00_3A8V01.03.xml
BCG_Package_RNSC1.0_RNIF1.1_3A8V01.03.zip	BCG_RNSC1.0_RNIF1.1_3A8V01.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A8V01.03.zip	BCG_RNSC1.0_RNIFV02.00_3A8V01.03.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A8 Notificación de actualización de pedido de compra:

- BCG_3A8PurchaseOrderChangeConfirmation_V01.03.xsd
- BCG_3A8PurchaseOrderChangeRequest_V01.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAccountClassificationCode.xsd
- BCG_GlobalActionCode.xsd
- BCG_GlobalConfirmationTypeCode.xsd
- BCG_GlobalCountryCode.xsd

- BCG_GlobalCreditCardClassificationCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFinanceTermsCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalGovernmentPriorityRatingCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPaymentConditionCode.xsd
- BCG_GlobalProductSubstitutionReasonCode.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalPurchaseOrderAcknowledgmentReasonCode.xsd
- BCG_GlobalPurchaseOrderFillPriorityCode.xsd
- BCG_GlobalPurchaseOrderStatusCode.xsd
- BCG_GlobalPurchaseOrderTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode_V43.xsd
- BCG_GlobalTaxExemptionCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3A9 Solicitud de cancelación de pedido de compra

En el apartado siguiente se describe el contenido de PIP 3A9 Solicitud de cancelación de pedido de compra.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3A9 Solicitud de cancelación de pedido de compra. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 69. Archivos ZIP y XML de 3A9 Solicitud de cancelación de pedido de compra

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3A9V01.01.zip	BCG_RNIF1.1_3A9V01.01.xml
BCG_Package_RNIFV02.00_3A9V01.01.zip	BCG_RNIFV02.00_3A9V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3A9V01.01.zip	BCG_RNSC1.0_RNIF1.1_3A9V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3A9V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3A9V01.01.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3A9 Solicitud de cancelación de pedido de compra:

- BCG_3A9PurchaseOrderCancellationConfirmation_V01.01.xsd
- BCG_3A9PurchaseOrderCancellationRequest_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPurchaseOrderCancellationCode.xsd
- BCG_GlobalPurchaseOrderCancellationResponseCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B2 Notificación de envío anticipado

En el apartado siguiente se describe el contenido de PIP 3B2 Notificación de envío anticipado.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3B2 Notificación de envío anticipado. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 70. Archivos ZIP y XML de 3B2 Notificación de envío anticipado

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3B2V01.01.zip	BCG_RNIF1.1_3B2V01.01.xml
BCG_Package_RNIFV02.00_3B2V01.01.zip	BCG_RNIFV02.00_3B2V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B2V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B2V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B2V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B2V01.01.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3B2 Notificación de envío anticipado:

- BCG_3B2AdvanceShipmentNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd

- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentChangeDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B3 Distribución del estado del envío

En el apartado siguiente se describe el contenido de PIP 3B3 Distribución del estado del envío.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3B3 Distribución del estado del envío. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 71. Archivos ZIP y XML de 3B3 Distribución del estado del envío

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3B3R01.00.zip	BCG_RNIF1.1_3B3R01.00.xml
BCG_Package_RNIFV02.00_3B3R01.00.zip	BCG_RNIFV02.00_3B3R01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B3R01.00.zip	BCG_RNSC1.0_RNIF1.1_3B3R01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B3R01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B3R01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3B3 Distribución del estado del envío:

- 3B3 Distribute Shipment Status_R01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd

- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalShipmentDispositionCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShipmentStatusCode_V43.xsd
- BCG_GlobalShipmentStatusReportingLevelCode_V43.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_PhysicalAddress_Types_V423.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B11 Notificación de orden de envío

En el apartado siguiente se describe el contenido de PIP 3B11 Notificación de orden de envío.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3B11 Notificación de orden de envío. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 72. Archivos ZIP y XML de 3B11 Notificación de orden de envío

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3B11R01.00A.zip	BCG_RNIF1.1_3B11R01.00A.xml
BCG_Package_RNIFV02.00_3B11R01.00A.zip	BCG_RNIFV02.00_3B11R01.00A.xml
BCG_Package_RNSC1.0_RNIF1.1_3B11R01.00A.zip	BCG_RNSC1.0_RNIF1.1_3B11R01.00A.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B11R01.00A.zip	BCG_RNSC1.0_RNIFV02.00_3B11R01.00A.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3B11 Notificación de orden de envío:

- 3B11 ShippingOrderNotification_R01.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd

- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B12 Solicitud de orden de envío

En el apartado siguiente se describe el contenido de PIP 3B12 Solicitud de orden de envío.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3B12 Solicitud de orden de envío. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 73. Archivos ZIP y XML de 3B12 Solicitud de orden de envío

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3B12V01.01.zip	BCG_RNIF1.1_3B12V01.01.xml
BCG_Package_RNIFV02.00_3B12V01.01.zip	BCG_RNIFV02.00_3B12V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B12V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B12V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B12V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B12V01.01.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3B12 Solicitud de orden de envío:

- BCG_3B12ShippingOrderConfirmation_V01.01.xsd
- BCG_3B12ShippingOrderRequest_V01.01.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd

- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V422.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B13 Notificación de confirmación de orden de envío

En el apartado siguiente se describe el contenido de PIP 3B13 Notificación de confirmación de orden de envío.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3B13 Notificación de confirmación de orden de envío. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 74. Archivos ZIP y XML de 3B13 Notificación de confirmación de orden de envío

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3B13V01.01.zip	BCG_RNIF1.1_3B13V01.01.xml
BCG_Package_RNIFV02.00_3B13V01.01.zip	BCG_RNIFV02.00_3B13V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3B13V01.01.zip	BCG_RNSC1.0_RNIF1.1_3B13V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B13V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3B13V01.01.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3B13 Notificación de confirmación de orden de envío:

- BCG_3B13ShippingOrderConfirmationNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd

- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B14 Solicitud de cancelación de orden de envío

En el apartado siguiente se describe el contenido de PIP 3B14 Solicitud de cancelación de orden de envío.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3B14 Solicitud de cancelación de orden de envío. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 75. Archivos ZIP y XML de 3B14 Solicitud de cancelación de orden de envío

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3B14V01.00.zip	BCG_RNIF1.1_3B14V01.00.xml
BCG_Package_RNIFV02.00_3B14V01.00.zip	BCG_RNIFV02.00_3B14V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B14V01.00.zip	BCG_RNSC1.0_RNIF1.1_3B14V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B14V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B14V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3B14 Solicitud de cancelación de orden de envío:

- 3B14_ShippingOrderCancellationConfirmation_V01.00.xsd
- 3B14_ShippingOrderCancellationRequest_V01.00.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalOrderAdminCode_V22.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd

- BCG_GlobalShippingOrderCancellationStatusReasonCode_V43.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3B18 Notificación de documentación de envío

En el apartado siguiente se describe el contenido de PIP 3B18 Notificación de documentación de envío.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3B18 Notificación de documentación de envío. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 76. Archivos ZIP y XML de 3B18 Notificación de documentación de envío

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3B18V01.00.zip	BCG_RNIF1.1_3B18V01.00.xml
BCG_Package_RNIFV02.00_3B18V01.00.zip	BCG_RNIFV02.00_3B18V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3B18V01.00.zip	BCG_RNSC1.0_RNIF1.1_3B18V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3B18V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3B18V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3B18 Notificación de documentación de envío:

- BCG_3B18ShippingDocumentationNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFreeOnBoardCode_V422.xsd
- BCG_GlobalFreightPaymentTermsCode_V422.xsd
- BCG_GlobalIncotermsCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalOrderAdminCode_V422.xsd
- BCG_GlobalPackageTypeCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerRoleClassificationCode_V422.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode_V422.xsd
- BCG_GlobalPortIdentifierAuthorityCode_V422.xsd

- BCG_GlobalPortTypeCode_V422.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipDateCode.xsd
- BCG_GlobalShipmentModeCode.xsd
- BCG_GlobalShippingDocumentCode_V422.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalSpecialHandlingCode_V422.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C1 Devolución de producto

En el apartado siguiente se describe el contenido de PIP 3C1 Devolución de producto.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3C1 Devolución de producto. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 77. Archivos ZIP y XML de 3C1 Devolución de producto

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3C1V01.00.zip	BCG_RNIF1.1_3C1V01.00.xml
BCG_Package_RNIFV02.00_3C1V01.00.zip	BCG_RNIFV02.00_3C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C1V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3C1 Devolución de producto:

- BCG_3C1ReturnProductConfirmation_V01.00.xsd
- BCG_3C1ReturnProductRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd

- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C3 Notificación de factura

En el apartado siguiente se describe el contenido de PIP 3C3 Notificación de factura.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3C3 Notificación de factura. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 78. Archivos ZIP y XML de 3C3 Notificación de factura

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3C3V01.01.zip	BCG_RNIF1.1_3C3V01.01.xml
BCG_Package_RNIFV02.00_3C3V01.01.zip	BCG_RNIFV02.00_3C3V01.01.xml
BCG_Package_RNSC1.0_RNIF1.1_3C3V01.01.zip	BCG_RNSC1.0_RNIF1.1_3C3V01.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C3V01.01.zip	BCG_RNSC1.0_RNIFV02.00_3C3V01.01.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3C3 Notificación de factura:

- BCG_3C3InvoiceNotification_V01.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd

- BCG_GlobalSpecialHandlingCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C4 Notificación de rechazo de factura

En el apartado siguiente se describe el contenido de PIP 3C4 Notificación de rechazo de factura.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3C4 Notificación de rechazo de factura. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 79. Archivos ZIP y XML de 3C4 Notificación de rechazo de factura

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3C4V01.00.zip	BCG_RNIF1.1_3C4V01.00.xml
BCG_Package_RNIFV02.00_3C4V01.00.zip	BCG_RNIFV02.00_3C4V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C4V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C4V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C4V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C4V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3C4 Notificación de rechazo de factura:

- BCG_3C4InvoiceRejectNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C6 Notificación de información de remesa

En el apartado siguiente se describe el contenido de PIP 3C6 Notificación de información de remesa.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3C6 Notificación de información de remesa. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 80. Archivos ZIP y XML de 3C6 Notificación de información de remesa

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3C6V01.00.zip	BCG_RNIF1.1_3C6V01.00.xml
BCG_Package_RNIFV02.00_3C6V01.00.zip	BCG_RNIFV02.00_3C6V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C6V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C6V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C6V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3C6 Notificación de información de remesa:

- BCG_3C6RemittanceAdviceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalFinancialAdjustmentReasonCode.xsd
- BCG_GlobalInvoiceRejectionCode.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPaymentMethodCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3C7 Notificación de factura de facturación automática

En el apartado siguiente se describe el contenido de PIP 3C7 Notificación de factura de facturación automática.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3C7 Notificación de factura de facturación automática. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 81. Archivos ZIP y XML de 3C7 Notificación de factura de facturación automática

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3C7V01.00.zip	BCG_RNIF1.1_3C7V01.00.xml
BCG_Package_RNIFV02.00_3C7V01.00.zip	BCG_RNIFV02.00_3C7V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3C7V01.00.zip	BCG_RNSC1.0_RNIF1.1_3C7V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3C7V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3C7V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3C7 Notificación de factura de facturación automática:

- BCG_3C7SelfBillingInvoiceNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalDocumentTypeCode.xsd
- BCG_GlobalDocumentTypeCode_V422.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPaymentTermsCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalSaleTypeCode.xsd
- BCG_GlobalShipmentTermsCode.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_InvoiceChargeTypeCode.xsd
- BCG_NationalExportControlClassificationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

3D8 Distribución de trabajo en curso

En el apartado siguiente se describe el contenido de PIP 3D8 Distribución de trabajo en curso.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 3D8 Distribución de trabajo en curso. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 82. Archivos ZIP y XML de 3D8 Distribución de trabajo en curso

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_3D8V01.00.zip	BCG_RNIF1.1_3D8V01.00.xml
BCG_Package_RNIFV02.00_3D8V01.00.zip	BCG_RNIFV02.00_3D8V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_3D8V01.00.zip	BCG_RNSC1.0_RNIF1.1_3D8V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_3D8V01.00.zip	BCG_RNSC1.0_RNIFV02.00_3D8V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 3D8 Distribución de trabajo en curso:

- BCG_3D8WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A1 Notificación de previsión estratégica

En el apartado siguiente se describe el contenido de PIP 4A1 Notificación de previsión estratégica.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4A1 Notificación de previsión estratégica. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 83. Archivos ZIP y XML de 4A1 Notificación de previsión estratégica

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4A1V02.00.zip	BCG_RNIF1.1_4A1V02.00.xml
BCG_Package_RNIFV02.00_4A1V02.00.zip	BCG_RNIFV02.00_4A1V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4A1V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A1V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A1V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A1V02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4A1 Notificación de previsión estratégica:

- BCG_4A1StrategicForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_StrategicForecastQuantityTypeCode.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A3 Notificación de pronóstico con liberación por umbral

En el apartado siguiente se describe el contenido de PIP 4A3 Notificación de pronóstico con liberación por umbral.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4A3 Notificación de pronóstico con liberación por umbral. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 84. Archivos ZIP y XML de 4A3 Notificación de pronóstico con liberación por umbral

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4A3V02.00.zip	BCG_RNIF1.1_4A3V02.00.xml
BCG_Package_RNIFV02.00_4A3V02.00.zip	BCG_RNIFV02.00_4A3V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4A3V02.00.zip	BCG_RNSC1.0_RNIF1.1_4A3V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A3V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A3V02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4A3 Notificación de pronóstico con liberación por umbral:

- BCG_4A3ThresholdReleaseForecastNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_OrderForecastQuantityTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A4 Notificación de planificación de pronóstico con liberación

En el apartado siguiente se describe el contenido de PIP 4A4 Notificación de planificación de pronóstico con liberación.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4A4 Notificación de planificación de pronóstico con liberación. PIP. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 85. Archivos ZIP y XML de 4A4 Notificación de planificación de pronóstico con liberación

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4A4R02.00A.zip	BCG_RNIF1.1_4A4R02.00A.xml
BCG_Package_RNIFV02.00_4A4R02.00A.zip	BCG_RNIFV02.00_4A4R02.00A.xml
BCG_Package_RNSC1.0_RNIF1.1_4A4R02.00A.zip	BCG_RNSC1.0_RNIF1.1_4A4R02.00A.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A4R02.00A.zip	BCG_RNSC1.0_RNIFV02.00_4A4R02.00A.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4A4 Notificación de planificación de pronóstico con liberación.

- BCG_4A4PlanningReleaseForecastNotification_R02.00A.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastQuantityTypeCode_V422.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalIntervalCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalTransportEventCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4A5 Notificación de respuesta de pronóstico

En el apartado siguiente se describe el contenido de PIP 4A5 Notificación de respuesta de pronóstico.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4A5 Notificación de respuesta de pronóstico. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 86. Archivos ZIP y XML de 4C5 Notificación de respuesta de pronóstico

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4A5V02.00.zip	BCG_RNIF1.1_4A5V02.00.xml
BCG_Package_RNIFV02.00_4A5V02.00.zip	BCG_RNIFV02.00_4A5V02.00.xml
BCG_Package_RNSC1.0_RNIF1.1_34A5V02.00.zip	BCG_RNSC1.0_RNIF1.1_34A5V02.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4A5V02.00.zip	BCG_RNSC1.0_RNIFV02.00_4A5V02.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4A5 Notificación de respuesta de pronóstico:

- BCG_4A5ForecastReplyNotification_V02.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd

- BCG_ContactInformation_Types.xsd
- BCG_ForecastReplyQuantityTypeCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalForecastEventCode.xsd
- BCG_GlobalForecastIntervalCode.xsd
- BCG_GlobalForecastInventoryTypeCode.xsd
- BCG_GlobalForecastReferenceTypeCode.xsd
- BCG_GlobalForecastResponseCode.xsd
- BCG_GlobalForecastRevisionReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerReferenceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4B2 Notificación de recibo de envío

En el apartado siguiente se describe el contenido de PIP 4B2 Notificación de recibo de envío.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4B2 Notificación de recibo de envío. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 87. Archivos ZIP y XML de 4B2 Notificación de recibo de envío

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4B2V01.00.zip	BCG_RNIF1.1_4B2V01.00.xml
BCG_Package_RNIFV02.00_4B2V01.00.zip	BCG_RNIFV02.00_4B2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4B2V01.00.zip	BCG_RNSC1.0_RNIF1.1_4B2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4B2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_4B2V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4B2 Notificación de recibo de envío:

- BCG_4B2ShipmentReceiptNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd

- BCG_GlobalLotDiscrepancyReasonCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalReceivingDiscrepancyCode.xsd
- BCG_GlobalReceivingDiscrepancyReasonCode.xsd
- BCG_GlobalSpecialFulfillmentRequestCode.xsd
- BCG_GlobalSpecialHandlingCode.xsd
- BCG_GlobalTrackingReferenceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4B3 Notificación de consumo

En el apartado siguiente se describe el contenido de PIP 4B3 Notificación de consumo.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4B3 Notificación de consumo. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 88. Archivos ZIP y XML de 4B3 Notificación de consumo

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4B3V01.00.zip	BCG_RNIF1.1_4B3V01.00.xml
BCG_Package_RNIFV02.00_4B3V01.00.zip	BCG_RNIFV02.00_4B3V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_4B3V01.00.zip	BCG_RNSC1.0_RNIF1.1_4B3V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_4B3V01.00.zip	BCG_RNSC1.0_RNIFV02.00_4B3V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4B3 Notificación de consumo:

- BCG_4B3ConsumptionNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessDescription_Types_V422.xsd
- BCG_BusinessDescription_Types_V43.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCountryCode.xsd

- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode_V43.xsd
- BCG_GlobalInventoryCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V422.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4C1 Distribución de informe de inventario V02.01

En el apartado siguiente se describe el contenido de PIP 4A3 Distribución de informe de inventario V02.01.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4C1 Distribución de informe de inventario. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 89. Archivos ZIP y XML de 4C1 Distribución de informe de inventario

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4C1V02.01.zip	BCG_RNIF1.1_4C1V02.01.xml
BCG_Package_RNIFV02.00_4C1V02.01.zip	BCG_RNIFV02.00_4C1V02.01.xml
BCG_Package_RNSC1.0_RNIF1.1_4C1V02.01.zip	BCG_RNSC1.0_RNIF1.1_4C1V02.01.xml
BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.01.zip	BCG_RNSC1.0_RNIFV02.00_4C1V02.01.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4C1 Distribución de informe de inventario:

- BCG_4C1InventoryReportNotification_V02.01.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd

- BCG_PhysicalAddress_Types_V422.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

4C1 Distribución de informe de inventario V02.03

En el apartado siguiente se describe el contenido de PIP 4C1 Distribución de informe de inventario V02.03:

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 4C1 Distribución de informe de inventario. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado:

Tabla 90. Archivos ZIP y XML de 4C1 Distribución de informe de inventario

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_4C1V02.03.zip	BCG_RNIF1.1_4C1V02.03.xml
BCG_Package_RNIFV02.00_4C1V02.03.zip	BCG_RNIFV02.00_4C1V02.03.xml
BCG_Package_RNSC1.0_RNIF1.1_4C1V02.03.zip	BCG_RNSC1.0_RNIF1.1_4C1V02.03.xml
BCG_Package_RNSC1.0_RNIFV02.00_4C1V02.03.zip	BCG_RNSC1.0_RNIFV02.00_4C1V02.03.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 4C1 Distribución de informe de inventario:

- BCG_4C1InventoryReportNotification_V02.03.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalInventoryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C1 Distribución de lista de productos

En el apartado siguiente se describe el contenido de PIP 5C1 Distribución de lista de productos.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 5C1 Distribución de lista de productos. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 91. Archivos ZIP y XML de 5C1 Distribución de lista de productos

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_5C1V01.00.zip	BCG_RNIF1.1_5C1V01.00.xml
BCG_Package_RNIFV02.00_5C1V01.00.zip	BCG_RNIFV02.00_5C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C1V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 5C1 Distribución de lista de productos:

- BCG_5C1ProductListNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C2 Petición de registro de diseño

En el apartado siguiente se describe el contenido de PIP 5C2 Solicitud de registro de diseño.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 5C2 Solicitud de registro de diseño. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 92. Archivos ZIP y XML de 5C2 Solicitud de registro de diseño

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_5C2V01.00.zip	BCG_RNIF1.1_5C2V01.00.xml
BCG_Package_RNIFV02.00_5C2V01.00.zip	BCG_RNIFV02.00_5C2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5C2V01.00.zip	BCG_RNSC1.0_RNIF1.1_5C2V01.00.xml

Tabla 92. Archivos ZIP y XML de 5C2 Solicitud de registro de diseño (continuación)

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNSC1.0_RNIFV02.00_5C2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C2V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 5C2 Solicitud de registro de diseño:

- BCG_5C2DesignRegistrationConfirmation_V01.00.xsd
- BCG_5C2DesignRegistrationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_common.xsd
- BCG_common_V422.xsd
- BCG_common_V43.xsd
- BCG_ContactInformation_Types.xsd
- BCG_DesignWinStatusReasonCode_V43.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V43.xsd
- BCG_GlobalMonetaryAmountTypeCode.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd
- BCG_GlobalPriceTypeCode_V43.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_InvoiceChargeTypeCode_V422.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5C4 Distribución de estado de registro

En el apartado siguiente se describe el contenido de PIP 5C4 Distribución de estado de registro.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 5C4 Distribución de estado de registro. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 93. Archivos ZIP y XML de 5C4 Distribución de estado de registro.

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_5C4V01.02.zip	BCG_RNIF1.1_5C4V01.02.xml
BCG_Package_RNIFV02.00_5C4V01.02.zip	BCG_RNIFV02.00_5C4V01.02.xml
BCG_Package_RNSC1.0_RNIF1.1_5C4V01.023.zip	BCG_RNSC1.0_RNIF1.1_5C4V01.023.xml
BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip	BCG_RNSC1.0_RNIFV02.00_5C4V01.02.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 5C4 Distribución de estado de registro:

- BCG_5C4RegistrationStatusNotification_V01.02.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalRegistrationComplexityLevelCode.xsd
- BCG_GlobalRegistrationInvolvementLevelCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

5D1 Solicitud de envío de existencias y autorización de débito

En el apartado siguiente se describe el contenido de PIP 5D1 Solicitud de envío de existencias y autorización de débito.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 5D1 Solicitud de envío de existencias y autorización de débito. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 94. Archivos ZIP y XML de 5D1 Solicitud de envío de existencias y autorización de débito.

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_5D1V01.00.zip	BCG_RNIF1.1_5D1V01.00.xml
BCG_Package_RNIFV02.00_5D1V01.00.zip	BCG_RNIFV02.00_5D1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_5D1V01.00.zip	BCG_RNSC1.0_RNIF1.1_5D1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_5D1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5D1V01.00.xml

Contenido de la correlación de directrices

En el apartado siguiente se describe el contenido de 5D1 Solicitud de envío de existencias y autorización de débito:

- BCG_5D1ShipFromStockAndDebitAuthorizationConfirmation_V01.00.xsd
- BCG_5D1ShipFromStockAndDebitAuthorizationRequest_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriceTypeCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalShipFromStockAndDebitAuthorizationRejectionCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

6C1 Consulta de derecho de servicio

En el apartado siguiente se describe el contenido de PIP 6C1 Consulta de derecho de servicio.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 6C1 Consulta de derecho de servicio. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 95. Archivos ZIP y XML de 6C1 Consulta de derecho de servicio

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_6C1V01.00.zip	BCG_RNIF1.1_6C1V01.00.xml
BCG_Package_RNIFV02.00_6C1V01.00.zip	BCG_RNIFV02.00_6C1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_6C1V01.00.zip	BCG_RNSC1.0_RNIF1.1_6C1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_6C1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_6C1V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 6C1 Consulta de derecho de servicio:

- BCG_6C1ServiceEntitlementQuery_V01.00.xsd
- BCG_6C1ServiceEntitlementStatusResponse_V01.00.xsd
- BCG_common_V43.xsd

- BCG_ContactInformation_Types.xsd
- BCG_ContactInformation_Types_V43.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalNotificationCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalShippingServiceLevelCode.xsd
- BCG_GlobalWarrantyMethodCode_V43.xsd
- BCG_GlobalWarrantyProgramCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

6C2 Solicitud de derecho de garantía

En el apartado siguiente se describe el contenido de PIP 6C2 Solicitud de derecho de garantía.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 6C2 Solicitud de derecho de garantía. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 96. Archivos ZIP y XML de 6C2 Solicitud de derecho de garantía

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_6C2V01.00.zip	BCG_RNIF1.1_6C2V01.00.xml
BCG_Package_RNIFV02.00_6C2V01.00.zip	BCG_RNIFV02.00_6C2V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_6C2V01.00.zip	BCG_RNSC1.0_RNIF1.1_6C2V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_6C2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_6C2V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 6C2 Solicitud de derecho de garantía:

- BCG_6C2WarrantyClaimConfirmation_V01.00.xsd
- BCG_6CWarrantyClaimRequest_V01.00.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalCurrencyCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalFailureTypeCode_V43.xsd
- BCG_GlobalOperatingSystemCode_V43.xsd
- BCG_GlobalPartnerClassificationCode_V43.xsd
- BCG_GlobalPartnerRoleClassificationCode_V43.xsd

- BCG_GlobalPaymentTypeCode_V43.xsd
- BCG_GlobalServiceDeliveryMethodCode_V43.xsd
- BCG_GlobalWarrantyTypeCode_V43.xsd
- BCG_PartnerDescription_Types_V43.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B1 Distribución de trabajo en curso

En el apartado siguiente se describe el contenido de PIP 7B1 Distribución de trabajo en curso.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 7B1 Distribución de trabajo en curso. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 97. Archivos ZIP y XML de 7B1 Distribución de trabajo en curso

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_7B1V01.00.zip	BCG_RNIF1.1_7B1V01.00.xml
BCG_Package_RNIFV02.00_37B1V01.00.zip	BCG_RNIFV02.00_37B1V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_7B1V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B1V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B1V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B1V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 7B1 Distribución de trabajo en curso:

- BCG_7B1WorkInProcessNotification_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalEquipmentTypeCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalLotQuantityClassificationCode.xsd
- BCG_GlobalLotStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_GlobalWorkInProcessPartTypeCode.xsd

- BCG_GlobalWorkInProcessQuantityChangeCode.xsd
- BCG_GlobalWorkInProcessTypeCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B5 Notificación de pedido de trabajo de fabricación

En el apartado siguiente se describe el contenido de PIP 7B5 Notificación de pedido de trabajo de fabricación.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 7B5 Notificación de pedido de trabajo de fabricación. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 98. Archivos ZIP y XML de 7B5 Notificación de pedido de trabajo de fabricación

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_7B5V01.00.zip	BCG_RNIF1.1_7B5V01.00.xml
BCG_Package_RNIFV02.00_7B5V01.00.zip	BCG_RNIFV02.00_7B5V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_7B5V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B5V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B5V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B5V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 7B5 Notificación de pedido de trabajo de fabricación:

- BCG_7B5NotifyOfManufacturingWorkOrder_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalAttachmentDescriptionCode_V422.xsd
- BCG_GlobalBusinessActionCode_V422.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDevicePackageTypeCode_V422.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalLotCode.xsd
- BCG_GlobalMimeTypeQualifierCode_V422.xsd
- BCG_GlobalPackageTypeCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalPhysicalUnitOfMeasureCode.xsd

- BCG_GlobalPriorityCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_GlobalWorkInProcessLocationCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

7B6 Notificación de respuesta de pedido de trabajo de fabricación

En el apartado siguiente se describe el contenido de PIP 7B6 Notificación de respuesta de pedido de trabajo de fabricación.

Contenido del archivo de paquetes

En la tabla siguiente se muestran los archivos ZIP y los archivos XML correspondientes a PIP 7B6 Notificación de respuesta de pedido de trabajo de fabricación. Las correlaciones de directrices, que son comunes a todas las versiones, se muestran en el siguiente apartado.

Tabla 99. Archivos ZIP y XML de 7B6 Notificación de respuesta de pedido de trabajo de fabricación

Nombre de archivo ZIP	Nombre de archivo XML
BCG_Package_RNIF1.1_7B6V01.00.zip	BCG_RNIF1.1_7B6V01.00.xml
BCG_Package_RNIFV02.00_7B6V01.00.zip	BCG_RNIFV02.00_7B6V01.00.xml
BCG_Package_RNSC1.0_RNIF1.1_7B6V01.00.zip	BCG_RNSC1.0_RNIF1.1_7B6V01.00.xml
BCG_Package_RNSC1.0_RNIFV02.00_7B6V01.00.zip	BCG_RNSC1.0_RNIFV02.00_7B6V01.00.xml

Contenido de la correlación de directrices

En este apartado se enumera el contenido de las correlaciones de directrices para 7B6 Notificación de respuesta de pedido de trabajo de fabricación:

- BCG_7B6NotifyOfManufacturingWorkOrderReply_V01.00.xsd
- BCG_BusinessDescription_Types.xsd
- BCG_BusinessTaxIdentifier_Types.xsd
- BCG_common.xsd
- BCG_ContactInformation_Types.xsd
- BCG_GlobalChangeReasonCode.xsd
- BCG_GlobalCountryCode.xsd
- BCG_GlobalDocumentReferenceTypeCode.xsd
- BCG_GlobalLineItemStatusCode.xsd
- BCG_GlobalPartnerClassificationCode.xsd
- BCG_GlobalPartnerRoleClassificationCode.xsd
- BCG_GlobalProductUnitOfMeasureCode.xsd
- BCG_PartnerDescription_Types.xsd
- BCG_PhysicalAddress_Types.xsd
- BCG_string_len_0.xsd
- BCG_xml.xsd

Capítulo 22. Información adicional de CIDX

Este apéndice proporciona información adicional acerca del soporte de CIDX. Incluye los siguientes temas:

Referencia relacionada

"Soporte de habilitación de procesos CIDX"

"Creación de paquetes de definición de documentos CIDX"

Soporte de habilitación de procesos CIDX

CIDX proporciona los siguientes dos mecanismos para la habilitación de procesos:

- **Habilitación basada en mensajes:** el enlace de documentos se basa en <RequestingDocumentIdentifier> y <ThisDocumentIdentifier>
- **Habilitación basada en infraestructura:** el enlace de documentos se basa en la semántica de cabecera de servicio de RNIF 1.1

Para la habilitación basada en mensajes, son necesarios los paquetes PIP de 1 acción para transacciones ChemXML. Mientras que para la habilitación basada en infraestructura, son necesarios paquetes PIP de 2 acciones para transacciones ChemXML. WebSphere Partner Gateway soporta las dos formas de habilitación de procesos. WebSphere Partner Gateway proporciona paquetes PIP de 1 acción para "E41 Order Create" y "E42 Order Response".

Creación de paquetes de definición de documentos CIDX

Puede que necesite crear sus propios paquetes CIDX para soportar mensajes CIDX. El procedimiento para crear nuevos paquetes de definición de documentos CIDX es el mismo que para RosettaNet.

Para información adicional acerca de RosettaNet, consulte el Capítulo 21, "Información adicional de RosettaNet", en la página 375

Capítulo 23. Atributos

En este apéndice se describen atributos que se pueden establecer desde la Consola de comunidad. Se describen los atributos siguientes:

Atributos de EDI

En este apartado se proporciona una descripción de los atributos de EDI que puede utilizar al configurar los intercambios EDI. Algunos de estos atributos están predefinidos en la serie de control que representa la correlación de transformación asociada al documento EDI. Los valores establecidos en el serie de control (en Data Interchange Services Client) alteran temporalmente cualquier valor que especifique en la Consola de comunidad.

Atributos de perfil de sobre

Puede establecer diversos atributos para un perfil de sobre de EDI. Los atributos que están disponibles dependen del tipo EDI. En general, los atributos corresponden a un estándar de EDI y, los valores que se pueden permitir dependen del estándar EDI que represente el perfil de sobre.

Ninguno de los atributos requiere un valor. En algunos de los atributos se utiliza un valor predeterminado si no especifica ningún valor. En las tablas de este apartado se listan los atributos que tienen asociados valores predeterminados y sus valores predeterminados.

Nota: las propiedades del perfil de sobre que no aparecen en la lista no tienen valores predeterminados. Se utiliza el valor del texto especificado por el usuario siempre que no sea alterado temporalmente por propiedades de sobre genéricas o específicas establecidas en la correlación o en una conexión.

Atributos X12

En las tablas de este apartado se listan los atributos X12 para los que se proporcionan valores predeterminados.

Atributos generales

En la Tabla 100 en la página 436 se enumeran los atributos generales para los que se proporcionan valores predeterminados.

Tabla 100. Atributos generales

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
INTCTLLEN (Longitud de número de control de intercambio)	No	Define una longitud específica para el número de control de intercambio. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
GRPCTLLEN (Longitud de número de control de grupo)	No	Define una longitud específica para el número de control de grupo. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
TRXCTLLEN (Longitud de número de control de transacción)	No	Define una longitud específica para el número de control de transacción. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
ENVTYPE (Tipo de sobre)	No	Este atributo no lo establece el usuario, sino que se obtiene del tipo de perfil de sobre que se está creando.	X12
MAXDOCS (Número máximo de transacciones)	No	Número máximo de transacciones en un sobre. Si especifica un valor, debe ser un entero.	Sin máximo
CTLNUMFLAG (Números de control por ID de transacción)	No	Sí indica que se mantienen conjuntos de números de control separados en función del tipo de transacción EDI. "No" indica que se debe utilizar un conjunto común de números de control para un tipo de transacción de EDI.	No

atributos de intercambio

No es necesario ningún atributo de intercambio X12 y los atributos no tienen valores predeterminados.

Tabla 101. Atributos de grupo

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
GS01 (ID de grupo funcional)	No	El identificador de grupo.	El valor predeterminado procede de la cabecera de la cadena de control. Puede ver este valor en Data Interchange Services Client consultando la columna Grupo funcional de la página Definiciones de documentos EDI.
GS08 (Versión de grupo)	No	La versión de grupo.	El valor predeterminado es el estándar.

Atributos de grupo

En la Tabla 101 se enumeran los atributos de grupo para los que se proporcionan valores predeterminados.

Atributos de transacción

Los atributos de transacción no son obligatorios. Los atributos no tienen valores predeterminados.

Atributos UCS

En este apartado se indica si los valores predeterminados se aplican a un intercambio, grupo o transacción UCS.

Atributos generales

En la Tabla 102 se enumeran los atributos generales para los que se proporcionan valores predeterminados.

Tabla 102. Atributos generales

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
INTCTLLEN (Longitud de número de control de intercambio)	No	Define una longitud específica para el número de control de intercambio. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	5
GRPCTLLEN (Longitud de número de control de grupo)	No	Define una longitud específica para el número de control de grupo. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
TRXCTLLEN (Longitud de número de control de transacción)	No	Define una longitud específica para el número de control de transacción. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
ENVTYPE (Tipo de sobre)	No	Este atributo no lo establece el administrador de concentrador, sino que se obtiene del tipo de perfil de sobre que se crea.	UCS
MAXDOCS (Número máximo de transacciones)	No	Número máximo de transacciones en un sobre. Si especifica un valor, debe ser un entero.	Sin máximo
CTLNUMFLAG (Números de control por ID de transacción)	No	"Sí" indica que se conservan conjuntos de números de control por separado en función del tipo de transacción de EDI. "No" indica que se debe utilizar un conjunto común de números de control para un tipo de transacción de EDI.	No

atributos de intercambio

Los atributos de intercambio no son obligatorios. Los atributos no tienen valores predeterminados.

Atributos de grupo

En la Tabla 103 se enumeran los atributos de grupo para los que se proporcionan valores predeterminados.

Tabla 103. Atributos de grupo

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
GS01 (ID de grupo funcional)	No	El identificador de grupo.	El valor predeterminado procede de la cabecera de la cadena de control. Puede ver este valor en Data Interchange Services Client consultando la columna Grupo funcional de la página Definiciones de documentos EDI.
GS08 (Versión de grupo)	No	La versión de grupo.	El valor predeterminado es el estándar.

Atributos de transacción

Los atributos de transacción no son obligatorios. Los atributos no tienen valores predeterminados.

Atributos EDIFACT

En este apartado se indica si los valores predeterminados se aplican a un intercambio, grupo y mensaje EDIFACT.

Atributos generales

En la Tabla 104 se enumeran los atributos generales para los que se proporcionan valores predeterminados.

Tabla 104. Atributos generales

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
INTCTLLEN (Longitud de número de control de intercambio)	No	Define una longitud específica para el número de control de intercambio. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
GRPCTLLEN (Longitud de número de control de grupo)	No	Define una longitud específica para el número de control de grupo. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
TRXCTLLEN (Longitud de número de control de transacción)	No	Define una longitud específica para el número de control de transacción. Si especifica un valor, debe ser un entero. Si no se especifica ningún valor, se utiliza la longitud predeterminada.	9
ENVTYPE (Tipo de sobre)	No	Este atributo no lo establece el administrador de concentrador, sino que se obtiene del tipo de perfil de sobre que se crea.	EDIFACT

Tabla 104. Atributos generales (continuación)

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
EDIFACTGRP (Crear grupos para EDI)	No	Este valor es sólo para tipos de sobre EDIFACT. (El nivel del grupo ya no se utiliza en EDIFACT). Sí indica que deben crearse grupos funcionales (segmentos UNG/UNE) para EDIFACT DATA. No indica que no deben crearse.	No
MAXDOCS (Número máximo de transacciones)	No	Número máximo de transacciones en un sobre. Si especifica un valor, debe ser un entero.	Sin máximo
CTLNUMFLAG (Números de control por ID de transacción)	No	"Sí" indica que se conservan conjuntos de números de control por separado en función del tipo de transacción de EDI. "No" indica que se debe utilizar un conjunto común de números de control para un tipo de transacción de EDI.	No

atributos de intercambio

Los atributos de intercambio no son obligatorios. Los atributos no tienen valores predeterminados.

Atributos de grupo

En la Tabla 105 se enumeran los atributos de grupo para los que se proporcionan valores predeterminados.

Tabla 105. Atributos de grupo

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
UNG01 (ID de grupo funcional)	No	El identificador de grupo.	El valor predeterminado procede de la cabecera de la cadena de control. Puede ver este valor en Data Interchange Services Client consultando la columna Grupo funcional de la página Definiciones de documentos EDI.

Atributos de mensaje

En la Tabla 106 se enumeran los atributos de mensajes para los que se proporcionan valores predeterminados.

Tabla 106. Atributos de mensaje

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
UNH0201 (Tipo de mensaje)	No	El tipo de mensaje.	El valor predeterminado procede de la cabecera de la cadena de control. Puede ver este valor en Data Interchange Services Client consultando la página Definiciones de documentos EDI.
UNH0202 (Versión de mensaje)	No	La versión del mensaje.	D
UNH0203 (Release de mensaje)	No	La versión del mensaje.	Según el estándar

Tabla 106. Atributos de mensaje (continuación)

Nombre de campo	¿Es obligatorio?	Descripción	Valor predeterminado
UNH0204 (Agencia controladora)	No	El código que identifica una agencia controladora.	UN

Atributos de conexión y definición de documentos

Este apartado lista los atributos de definición de documentos del sobre. Algunos de estos atributos sólo pueden establecerse en el nivel de protocolo o conexión, tal como se indica.

Atributos de delimitadores y separadores

En este apartado se enumeran los caracteres utilizados como delimitadores o separadores dentro de un intercambio EDI. La Tabla 107 muestra el atributo tal como aparece en la Consola de comunidad, el término correspondiente en X12 y EDIFACT (ISO 9735 Versión 4, Release 1) y si es necesario el atributo y una descripción del mismo. A continuación de la tabla hay un ejemplo de cómo aparecen estos caracteres en un documento EDI.

Descripciones de atributos

Los atributos de separadores y delimitadores se listan en la Tabla 107.

Nota: algunos caracteres (como se indica) pueden ser valores hexadecimales. Estos valores pueden ser Unicode o de otro tipo de codificación. En el caso de valores Unicode, utilice el formato \unnnn. En el caso de otro tipo de codificación, utilice el formato 0xnn.

Tabla 107. Atributos de perfil de sobre

Atributo	Término X12	Término en EDIFACT	Descripción
Delimitador de segmento	Terminador de segmentos	Terminador de segmentos	Se trata de un único carácter que aparece al final de un segmento. El carácter puede ser un valor hexadecimal. El valor predeterminado está basado en el tipo de EDI. **X12** ~ (tilde) **EDIFACT** ' (comilla simple) **UCS** ~ (tilde)
Delimitador de elemento de datos	Separador de elementos de datos	Separador de elementos de datos	Se trata de un único carácter que separa los elementos de datos de un segmento. El carácter puede ser un valor hexadecimal. El valor predeterminado está basado en el tipo de EDI. **X12** * (asterisco) **EDIFACT** + (signo más) **UCS** * (asterisco)

Tabla 107. Atributos de perfil de sobre (continuación)

Atributo	Término X12	Término en EDIFACT	Descripción
Delimitador de subelemento	Separador de elementos de componente	Separador de elementos de datos de componente	Se trata de un único carácter que separa los elementos de componente de un elemento de datos compuestos. El carácter puede ser un valor hexadecimal. El valor predeterminado está basado en el tipo de EDI. **X12** \ (barra inclinada invertida) **EDIFACT** : (dos puntos) **UCS** \ (barra inclinada invertida)
Carácter de release		Carácter de release	Se trata de un único carácter, que altera temporalmente el significado del siguiente carácter, permitiendo la aparición de un carácter separador dentro del elemento de datos. El carácter puede ser un valor hexadecimal. Sólo se aplica a EDIFACT. **EDIFACT** ? (signo de interrogación)
Separador de elementos de datos	separador de repetición	separador de repetición	Se trata de un único carácter que separa las instancias de un elemento de datos que se repite. Este carácter puede ser un valor hexadecimal. El valor predeterminado está basado en el tipo de EDI para X12 o EDIFACT. **X12** ^ (acento circunflejo) **EDIFACT** * (asterisco)
Notación decimal		notación decimal (en desuso)	Este atributo se utilizaba en el análisis o formateo decimal y ahora está en desuso. Sólo puede ser un punto o una coma. El valor predeterminado es un punto.

Ejemplo de estructura EDI

En este apartado se muestra un intercambio EDI simple y cómo se utilizan en un intercambio los atributos descritos en la Tabla 107 en la página 440.

Un mensaje EDI consiste en una serie de segmentos establecidos en un determinado orden. Un segmento está formado por una serie de elementos. En un segmento, un elemento puede ser un elemento de datos simple, que sólo contiene un elemento de información. Un elemento también puede ser un elemento de datos compuesto, que contiene dos o más elementos de datos simples. Los elementos simples que forman parte de un elemento compuesto se denominan elementos de datos de componentes.

No hay ninguna anidación de elementos de datos compuestos. Un elemento compuesto puede contener sólo elementos de datos simples, no otros compuestos. Aunque no se indica en este apartado, un elemento de datos compuestos también se puede definir como un elemento que se repite.

Considere el siguiente ejemplo:

```
ABC*123*AA\BB\CC*001^002^003*star?*power~
```

En este ejemplo:

- "ABC" es el nombre de segmento (EDIFACT llama a esto el "identificador de segmento"); esto se llamaría "segmento ABC"
- "*" (asterisco) es el separador de elemento de datos.

  El nombre de atributo correspondiente en la Consola de comunidad es delimitador de segmento.
- "123" es el primer elemento de datos, un elemento de datos simple (que puede denominarse ABC01 en algunos contextos)
- "AA\BB\CC" es el segundo elemento de datos (ABC02), un elemento compuesto formado por elementos de datos de componentes
  - "\ " (barra inclinada invertida) es el separador de elementos de datos de componentes

    El nombre de atributo correspondiente en la Consola de comunidad es el delimitador de elemento de datos.
  - "AA" es el primer elemento de datos de componentes de ABC02 (debería denominarse ABC0201)
  - "BB" es el segundo elemento de datos de componentes de ABC02 (ABC0202)
  - "CC" es el tercer elemento de datos compuestos de ABC02 (ABC0203)
- "001^002^003" es el tercer elemento de datos (ABC03), un elemento de datos que se repite
  - "^" (acento circunflejo) es el separador de repetición

    El nombre de atributo correspondiente en la Consola de comunidad es el Carácter de elemento de datos repetitivo.
  - "001","002", "003" son las repeticiones (todas se denominarían ABC03)
- "star?*power" es el cuarto elemento de datos (ABC04)
  - "?" (signo de interrogación) es el carácter de release, lo que significa que el siguiente asterisco no se trata como separador de elementos de datos
  - "star*power" es el valor que se obtiene como resultado de ABC04
- "~" (tilde) es el terminador de segmento.

  El nombre de atributo correspondiente en la Consola de comunidad es delimitador de segmento.

Atributos de EDI adicionales

Este apartado lista los atributos de EDI adicionales que se pueden establecer en el nivel de definición del documento o en nivel de conexión.

Tabla 108. Atributos de EDI adicionales

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Salida de segmento	No	Se utiliza en la transformación EDI/XML, esto indica si se debe indicar un salto de línea después de cada segmento EDI o elemento XML. **Importante:** 1. Utilice siempre un delimitador de un único carácter. 2. Si utiliza la combinación "/r/n" como delimitador de caracteres y el delimitador de caracteres "/r" se encuentra en la posición de delimitador de segmento de la cabecera de intercambio, se ignorará el delimitador de caracteres "/n". 3. Modifique el árbol de tipo como corresponda.	Limitado al protocolo o a la conexión	Sí
Permitir documentos con ID de documento duplicados	No	Sí indica que se permiten ID de documentos duplicados (números de control de intercambio). "No" indica que los números de control de intercambio duplicados se deberían considerar como error.	Limitado al protocolo o a la conexión	No
Nivel de error máximo en la transformación	No	Indica el número máximo de errores que pueden darse durante una transformación antes de que la transformación falle. Los valores válidos son 0, 1 o 2. Si la correlación de transformación contiene un mandato de error para indicar un error especificado por un usuario y el parámetro de nivel del mandato de error es mayor que este valor, la transformación falla.	Limitado al protocolo o a la conexión	0
Correlación de FA	No	Proporciona la correlación que debe utilizarse para convertir el FA genérico en FA específico. **Nota:** seleccione este atributo en una lista de correlaciones identificadas como correlaciones de FA (tipo de correlación “K”).	Limitado al protocolo o a la conexión	
Perfil de sobre	Sí	El nombre de perfil de sobre EDI que se debe utilizar para el ensobrado. Todos los perfiles de sobre definidos están disponibles en la lista.		
XMLNS activo	No	Realizar el proceso del espacio de nombres para el documento XML de entrada. Este atributo lo utiliza el paso de transformación XML. Los valores válidos son Sí o No.		Esquema: Sí DTD: No

Tabla 108. Atributos de EDI adicionales (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Nivel de error de validación máximo	No	El nivel máximo de error (el grado de error que se puede aceptar antes de considerar que la transacción es errónea). Los valores válidos son 0, 1 o 2. **0** Permitir sólo la validación sin errores. **1** No rechazar los documentos que tienen errores simples de validación de elementos. **2** No rechazar los documentos que tienen errores de elementos o de validación de elementos.		0
Nivel de validación	No	Indica el nivel de comprobación que se tiene que realizar en el nivel de transacción. El valor 2 significa que se deben utilizar los valores establecidos para los atributos de la tabla de validación alfanumérica y de la tabla de validación de conjunto de caracteres. Este atributo también se aplica al atributo Validación detallada de segmentos si está establecido en Sí. Los valores válidos son 0, 1 o 2. **0** Sólo se debe realizar la validación básica, como comprobar si faltan segmentos y elementos obligatorios y las longitudes mínimas o máximas. No valide valores de elementos conforme a los tipos de datos o listas de códigos especificados en la definición de la transacción. **1** Se debe realizar el nivel de validación 0 y la validación de valores de elementos frente a las listas de códigos especificadas para el elemento de datos. **2** Se debe realizar el nivel de validación 1 así como validar que el valor de elemento es correcto para el tipo de datos del elemento.		0
Tabla de validación de juego de caracteres	No	Indica la tabla que se tiene que utilizar para la validación del juego de caracteres. Esta tabla sólo se utiliza cuando el atributo Nivel de validación está establecido en 2. Este atributo hace referencia a la tabla de listas de códigos virtuales. El usuario puede crear nuevas listas de códigos en la pestaña Listas de códigos del área Correlación en Data Interchange Services Client. Esta área también contiene listas de códigos que se utilizan para otros propósitos, como la validación de determinados elementos de EDI.		CHARSET

Tabla 108. Atributos de EDI adicionales (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Tabla de validación alfanumérica	No	Indica la tabla que se tiene que utilizar para la validación alfanumérica. Esta tabla sólo se utiliza cuando el atributo Nivel de validación está establecido en 2. El atributo hace referencia a las tablas de listas de códigos virtuales. El usuario puede crear nuevas listas de códigos en la pestaña Listas de códigos del área Correlación en Data Interchange Services Client. Esta área también contiene listas de códigos que se utilizan para otros propósitos, como la validación de determinados elementos de EDI.		ALPHANUM
Generar información de nivel de grupo sólo en caso de acuse de recibo funcional	No	Este atributo se aplica a EDI-X12. Los valores son Sí o No. **Sí** Genera información de nivel de grupo únicamente para el acuse de recibo funcional. **No** Genera un acuse de recibo funcional detallado (para cada transacción individual y los segmentos y elementos incluidos en una transacción).	Limitado al protocolo o a la conexión	No
Año de control de siglo	No	Cuando las fechas se convierten de años con dos dígitos en años con cuatro dígitos, se supone que los años de dos dígitos superiores a este valor tienen un valor de siglo “19”. Para los años con dos dígitos iguales o inferiores a este valor se supone que tienen el valor de siglo “20”. El rango válido es de 0 a 99.	Limitado al protocolo o a la conexión	10

Tabla 108. Atributos de EDI adicionales (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Validación detallada de segmento	No	Este atributo se aplica a las siguientes cabeceras y colas de segmentos: • X12 – ISA, IEA – GS, GE – ST, SE • EDIFACT – UNA – UNB, UNZ – UNG, UNE – UNH, UNT • UNTUCS – BG, EG – GS, GE – ST, SE Los valores válidos son Sí o No. **Sí** Realiza la validación detallada de segmentos de sobre. La intensidad de la comprobación se controla mediante el atributo Nivel de validación. **No** No se realiza la validación detallada de segmentos de sobre.	Limitado al protocolo o a la conexión	No
Alteración temporal de TA1	No	Permite la generación de una solicitud TA1 si está indicado en el segmento de sobre de intercambio. Se aplica sólo a EDI-X12. Si se establece en Sí, se genera un TA1 si se ha especificado en el segmento de sobre de intercambio. En el caso de que esté establecido en No, no se generará un TA1, aunque esté especificado en el segmento de sobre de intercambio.	Limitado al protocolo o a la conexión	Sí
Descartar en caso de error	No	Este atributo se utiliza en el proceso polimórfico. En el caso de un lote que resulta del desensobrado, este atributo indica si se debe descartar todo el lote en caso de que alguna de las transacciones sufra una anomalía. Los valores válidos son Sí o No.	Limitado al protocolo o a la conexión	No
Calificador 1 de perfil de conexión	No	Este atributo lo utiliza el ensobrador para determinar qué perfil utilizar para una conexión de intercambio. Las transacciones con diferentes valores para este atributo se colocan en diferentes intercambios.		
Calificador de intercambio	No	Código utilizado para identificar el formato del identificador del receptor o remitente del intercambio.		

Tabla 108. Atributos de EDI adicionales (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Identificador de intercambio	No	Identifica el remitente o receptor específico del documento. El tipo de datos especificado lo determina el atributo Calificador de intercambio.		
Indicador de usuario de intercambio	No	Indica si los documentos de origen que se convierten están clasificados como documentos de producción, prueba o información. Los valores válidos son P, T y I.		
Identificador de remitente de aplicación de grupo	No	Identifica el remitente específico de la transacción. Este atributo, cuando lo acuerdan los socios comerciales, facilita la dirección específica dentro de una empresa.		
Identificador de receptor de aplicación de grupo	No	Identifica el receptor o aplicación específicos de la transacción. Este atributo, cuando lo acuerdan los socios comerciales, facilita la dirección específica dentro de una empresa.		
Direccionamiento inverso de intercambio	No	Indica la dirección a la que el destinatario debe dirigir todas las respuestas.		
Dirección de direccionamiento de intercambio	No	Código de subdirección para direccionamiento hacia adelante.		
Calificador de remitente de aplicación de grupo	No	Código utilizado para identificar el formato del identificador del remitente de aplicación de grupo.		
Calificador de receptor de aplicación de grupo	No	Código utilizado para identificar el formato del identificador del receptor de aplicación de grupo.		
Contraseña de aplicación de grupo	No	Este atributo define la información de seguridad.		
Límite de tiempo necesario de FA		Número de minutos después del envío de una transacción en que se requiere que se devuelva un FA. Si el valor está en blanco, no es necesario ningún FA.		

Propiedades de Data Interchange Services Client

En este apartado se listan las propiedades que pueden establecerse como parte de la correlación de transformación en Data Interchange Services Client y sus correspondientes atributos de WebSphere Partner Gateway.

Tabla 109. Propiedades de correlación y sus atributos correspondientes

Propiedad de Data Interchange Services Client	Altera temporalmente atributo de WebSphere Partner Gateway
AckReq	Acuse de recibo solicitado
Alphanum	Tabla de validación alfanumérica

Tabla 109. Propiedades de correlación y sus atributos correspondientes (continuación)

Propiedad de Data Interchange Services Client	Altera temporalmente atributo de WebSphere Partner Gateway
Charset	Tabla de validación de juego de caracteres
CtlNumFlag	Números de control por ID de transacción
EdiDecNot (Notación decimal)	Notación decimal
EdiDeDlm (Separador de elemento de datos)	Delimitador de elemento de datos
EdiDeSep (Separador de elementos de datos repetitivo)	Separador de elementos de datos
EdifactGrp	Crear grupos para EDI
EdiRlsChar (Carácter de release)	Carácter de release
EdiSeDlm (Separador de elemento de datos de componentes)	Delimitador de subelemento
EdiSegDlm (Terminador de segmento)	Delimitador de segmento
EnvProfName	Perfil de sobre
EnvType	Tipo de sobre
MaxDocs	Número máximo de transacciones
Reroute	Direccionamiento inverso de intercambio
SegOutput	Salida de segmento
ValLevel	Nivel de validación
ValErrLevel	Nivel de error de validación máximo
ValMap	Correlación de validación

En la Tabla 110 se enumeran las propiedades adicionales de Data Interchange Services Client y los atributos de WebSphere Partner Gateway asociados.

Tabla 110. Propiedades de Data Interchange Services Client y sus atributos asociados

Propiedad de Data Interchange Services Client	Altera temporalmente atributo de WebSphere Partner Gateway
IchgCtlNum	Número de control del intercambio
IchgSndrQl	Calificador del emisor del intercambio
IchgSndrId	ID del remitente del intercambio
IchgRcvrQl	Calificador del receptor del intercambio
IchgRcvrId	ID del receptor del intercambio
IchgDate	Fecha de intercambio
IchgTime	Hora de intercambio
IchgPswd	Contraseña del intercambio
IchgUsgInd	Indicador de usuario de intercambio
IchgAppRef	Referencia de la aplicación del intercambio
IchgVerRel	Versión y release de Interchange
IchgGrpCnt	Número de grupos del intercambio
IchgCtlTotal	Control total del segmento de cola del intercambio
IchgTrxCnt	Número de documentos del intercambio
GrpCtlNum	Número de control de grupo
GrpFuncGrpId	ID de grupo funcional

Tabla 110. Propiedades de Data Interchange Services Client y sus atributos asociados (continuación)

Propiedad de Data Interchange Services Client	Altera temporalmente atributo de WebSphere Partner Gateway
GrpAppSndrId	ID del remitente de la aplicación de grupo
GrpAppRcvrId	ID del receptor de la aplicación de grupo
GrpDate	Fecha del grupo
GrpTime	Hora del grupo
GrpPswd	Contraseña del grupo
GrpVer Versión del grupo.	Versión de grupo
GrpRel Release del grupo.	Release del grupo
GrpTrxCnt	Número de documentos del grupo
TrxCtlNum	Número de control de la transacción
TrxCode	Código de la transacción
TrxVer	Versión de la transacción
TrxRel	Release de la transacción
TrxSegCnt	Número de segmentos EDI en el documento

atributos de AS

En este apartado se describen los atributos de AS.

Tabla 111. atributos de AS

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Tiempo para el acuse de recibo en min.	No	Intervalo de tiempo que se debe esperar a que llegue un acuse de recibo MDN antes de reenviar la solicitud original. Este atributo se utiliza junto con Recuento de reintentos. El intervalo se especifica en minutos.	Limitado al paquete o a la conexión	30
Recuento de reintentos	No	Número de veces que se debe enviar una solicitud si no se recibe una MDN. Este atributo funciona junto con Tiempo de acuse de recibo. Por ejemplo, si este atributo se establece en 3, la solicitud puede enviarse cuatro veces (la primera vez y los tres reintentos).	Limitado al paquete o a la conexión	3
Compresión de AS antes de firmar	No	Indica si se debe aplicar la compresión AS a la carga y a la firma, o sólo a la carga. Si selecciona Sí, la carga se comprime antes de firmar el mensaje. Este atributo se utiliza junto con el atributo AS comprimida.	Limitado al paquete o a la conexión	Sí
AS comprimido	No	Comprime los datos. Este atributo se utiliza junto con el atributo Compresión de AS antes de firmar.	Limitado al paquete o a la conexión	No

Tabla 111. atributos de AS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
AS cifrado	No	Este atributo se aplica a AS2 y se utiliza para especificar el URL al que un socio debe enviar una MDN asíncrona. Este atributo se utiliza junto con el atributo MDN de AS asíncrona, pero es necesario un valor incluso para MDN síncrono.	Limitado al paquete o a la conexión	No
URL de HTTP de MDN de AS	Sí, si el atributo "MDN de AS asíncrona" tiene el valor Sí y utiliza AS2.	Este atributo se aplica a AS2 y se utiliza para especificar el URL al que un socio debe enviar una MDN asíncrona. Este atributo se utiliza junto con el atributo MDN de AS asíncrona, pero es necesario un valor incluso para MDN síncrono.	Limitado al paquete o a la conexión	
Dirección de correo electrónico de MDN de AS	Sí si el atributo "MDN de AS asíncrona" tiene el valor Sí y utiliza AS1.	Especifica la dirección de correo electrónico que el socio debe utilizar al enviar una MDN asíncrona. Este atributo se utiliza junto con el atributo MDN de AS solicitada. El valor de Dirección de correo electrónico de MDN de AS se utiliza en el campo “Disposition-notification-to”. Para AS1 este atributo se utiliza junto con el atributo MDN de AS asíncrona de formato mailto:xxx@company.com. Para AS2, este atributo aún necesita un valor aunque no se utilice la dirección de correo electrónico.	Limitado al paquete o a la conexión	
MDN de AS asíncrona	No	Especifica si la MDN debe devolverse de forma síncrona o asíncrona. El valor de este atributo indica si se utiliza el atributo URL de HTTP de MDN de AS o el atributo Dirección de correo electrónico de MDN de AS. Los valores válidos son Sí o No. **Sí** Asíncrono **No** Síncrono Si este atributo tiene el valor Sí, el campo "receipt-delivery-option" se rellena en función del atributo URL de HTTP de MDN de AS (para AS2) o del atributo Dirección de correo electrónico de MDN de AS (para AS1).	Limitado al paquete o a la conexión	Sí

Tabla 111. atributos de AS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
MDN de AS solicitada	No	Especifica si es necesaria una respuesta MDN. Si se establece en Sí, este atributo hace que la cabecera "transport Disposition-notification-to" se rellene con el valor del atributo Dirección de correo electrónico de MDN de AS. Los valores válidos son Sí o No. **Sí** Solicitar una MDN. **No** No solicitar una MDN.	Limitado al paquete o a la conexión	Sí
Algoritmo de conversión de mensaje de AS	No	Algoritmo de conversión de mensaje que se debe utilizar al firmar. Este atributo se utiliza junto con los atributos AS firmada y MDN de AS firmada. Para las MDN firmadas, este valor se utiliza para rellenar la cabecera "Disposition-notification-options: signed-receipt-micalg".	Limitado al paquete o a la conexión	sha1
MDN de AS firmada	No	Indica si la solicitud requiere que se devuelva una MDN firmada. Este atributo se utiliza junto con el atributo MDN de AS solicitada. Si el valor es Sí, se rellena la cabecera "Disposition-notification-options: signed-receipt-protocol". Los valores válidos son Sí o No. **Sí** Solicitar MDN firmada. **No** No se solicita la MDN firmada. Si este atributo se establece en Sí, la MDN enviada por el socio debe estar firmada. Si este atributo se establece en No, la MDN puede estar firmada o sin firmar.	Limitado al paquete o a la conexión	No
AS firmada	No	Especifica si se debe firmar el documento. Para el lado receptor de un intercambio (cuando se envían documentos a un socio), especifica si se debe firmar el documento. Para el lado emisor de un intercambio (cuando se reciben documentos de un socio), si el atributo está establecido en Sí, una solicitud de AS enviada desde el socio debe estar firmada. Si el atributo se establece en No, el documento para el socio puede estar firmado o sin firmar. **Sí** Se requiere el documento firmado **No** No se requiere el documento firmado	Limitado al paquete o a la conexión	No

Tabla 111. atributos de AS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
No rechazo necesario	No	Indica si este documento necesita o no ser guardado en el almacén de no rechazo. Se aplicará al documento como origen o destino. Sí – Guarde el documento en el almacén de no rechazo. No – No guardar el documento en el almacén de no rechazo.	Limitado al paquete o a la conexión	Sí
Se requiere almacén de mensajes	No	Indica si este documento necesita o no ser guardado en el almacén de mensajes. Se aplicará a los documentos de origen o de destino. Sí – Guarde el documento en el almacén de mensajes. No – No guardar el documento en el almacén de mensajes.	Limitado al paquete o a la conexión	Sí
ID de empresa de AS	No	El ID de empresa de AS que se debe utilizar en la cabecera “AS2-To” o “AS3-To”. Si no se proporciona ningún valor, WebSphere Partner Gateway utiliza el ID de empresa de destinatario usado en el documento de origen. **Nota:** la cabecera “AS2-From” o “AS3-From” será establecida desde el atributo “ID de empresa de AS” desde la definición del documento de origen o, si no está definida, desde el documento de origen original que se entregó con WebSphere Partner Gateway y que se envía como una AS.	Limitado al paquete o a la conexión	
Dirección FTP de MDN de AS	Sí para AS3 cuando el atributo "MDN AS solicitado" es Sí.	La dirección FTP de MDN de AS cuando se solicite un MDN. Este atributo se utiliza junto con el atributo "MDN AS solicitado". El valor de Dirección FTP de MDN de AS se utiliza en el campo “Disposition-notification-to”. Es necesario que esté en el formato: `ftp://nombre_usuario:contraseña@sistprincipal.com:puerto/nombre-carpeta.`	Limitado al paquete o a la conexión	No
Algoritmo de firma	Sí, si "Firma digital necesaria" es Sí	Algoritmo utilizado para firmar el documento. Este atributo sólo se utiliza si el valor del atributo “Firma digital necesaria” es “Sí”.		dsa-sha1
Algoritmo de cifrado	Sí cuando el valor del atributo “Cifrado necesario” está establecido en “Sí”	El algoritmo utilizado para cifrar cargas. Este valor funciona junto con el atributo "Protocolo de cifrado". Este atributo sólo se utiliza si el valor del atributo “Cifrado necesario” está establecido en “Sí”.		AES-128

Tabla 111. atributos de AS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Protocolo de cifrado	No	El protocolo utilizado para cifrar las cargas. Los posibles valores son XMLEncryption y SMIME. Este atributo sólo se utiliza si el valor del atributo “Cifrado necesario” está establecido en “Sí”. Si EncryptionRequired se establece en "sí" pero no se proporciona ningún valor para este atributo, el documento .		XMLEncryption

Atributos de RosettaNet

En este apartado se describen los atributos de RosettaNet.

Tabla 112. Atributos de RosettaNet

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Tiempo de acuse de recibo	Sí	Intervalo de tiempo que se debe esperar a que llegue un acuse de recibo antes de reenviar la solicitud original. Este atributo se utiliza junto con Recuento de reintentos. El intervalo se especifica en minutos. El valor predeterminado se toma del documento de especificación PIP de RosettaNet.	Limitado al paquete o a la conexión	120
Tiempo de realización	Sí	Intervalo de tiempo que se debe esperar a que llegue una respuesta para una acción de solicitud antes de enviar un mensaje de notificación de anomalía.	Limitado al paquete o a la conexión	
Recuento de reintentos	Sí	Número de veces que se debe enviar una solicitud si no se recibe un acuse de recibo. Este atributo funciona junto con Tiempo de acuse de recibo. Por ejemplo, con el valor 3, la solicitud puede enviarse 4 veces (la primera vez y los tres reintentos). El valor predeterminado se toma del documento de especificación PIP de RosettaNet.	Limitado al paquete o a la conexión	3
Firma digital necesaria	No	Indica si el mensaje PIP requiere una firma digital. El valor predeterminado se toma del documento de especificación PIP de RosettaNet.	Limitado al paquete o a la conexión	Sí

Tabla 112. Atributos de RosettaNet (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
No rechazo necesario	No	Indica si este documento necesita o no ser guardado en el almacén de no rechazo. Se aplicará al documento como origen o destino. Sí – Guarde el documento en el almacén de no rechazo. No – No guardar el documento en el almacén de no rechazo.	Limitado al paquete o a la conexión	Sí
Se requiere almacén de mensajes	No	Indica si este documento necesita o no ser guardado en el almacén de mensajes. Se aplicará a los documentos de origen o de destino. Sí – Guarde el documento en el almacén de mensajes. No – No guardar el documento en el almacén de mensajes.	Limitado al paquete o a la conexión	Sí
No rechazo de recibo necesario	No	Indica si el documento de acuse de recibo se debe guardar en un almacén de no rechazo. El valor predeterminado se toma del documento de especificación PIP de RosettaNet.	Limitado al paquete o a la conexión	Sí
Sinc. soportada		Indica si el PIP da soporte a la comunicación síncrona. El valor predeterminado se proporciona en función de la especificación PIP.	Limitado al paquete o a la conexión. Este atributo sólo está disponible para RNIF 2.0.	
Acuse recibo sinc. necesario		Indica si el PIP requiere un acuse de recibo síncrono. El valor predeterminado se proporciona en función de la especificación PIP.	Limitado al paquete o a la conexión. Este atributo sólo está disponible para RNIF 2.0.	
Código de cadena de suministro global	Necesario para RNIF 1.1	El código que identifica la cadena de suministro de la función del socio. Los valores válidos son: • Componente electrónico • Informática • Tecnología de semiconductores	Limitado al paquete o a la conexión	

Tabla 112. Atributos de RosettaNet (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Cifrado		Este atributo indica si debe realizarse el cifrado. **Nota:** no es lo mismo que el cifrado SSL. Para el lado receptor de un intercambio (cuando se envían documentos a un socio), especifica si se debe cifrar el documento. Para el lado emisor de un intercambio (cuando se reciben documentos de un socio), si el atributo está establecido en Sí, una solicitud de RNIF enviada desde el socio debe estar cifrada. Si el atributo se establece en No, el documento para el socio puede estar cifrado o descifrado. Los valores válidos son: **Ninguno** No es necesario el cifrado. **Carga** Cifrar sólo el contenido de servicio de RosettaNet. **Carga y contenedor** Cifrar unidos la cabecera de servicio y el contenido de servicio de RosettaNet.	Limitado al paquete o a la conexión. Este atributo sólo está disponible para RNIF 2.0.	Ninguno
Texto estándar del mensaje	No	El estándar que debe cumplir el contenido de servicio. Esto debe configurarse si y sólo si este es un mensaje de contenido de servicio especificado no de RosettaNet.		No hay valor predeterminado.
Versión estándar del mensaje	No	La versión del estándar que debe cumplir el contenido de servicio. Esto debe configurarse si y sólo si este es un mensaje de contenido de servicio especificado no de RosettaNet.		No hay valor predeterminado.
Identificador de enlace de carga PIP	No	Este es el identificador de enlace de PIP definido por el socio, que es exclusivo entre socios comerciales. Este atributo sólo se establece en el caso de contenido de servicio no de RosettaNet.		No hay valor predeterminado.
FromGlobalPartner ClassificationCode	Sí para esquemas RNIF 1.1	El código que identifica una función de socio en la cadena de suministro. Sólo necesario cuando se utilice RNIF 1.1 para PIP basados en esquemas. Este valor debe también especificarse para el pip 0A1, cuando se utilicen PIP basados en esquemas.		No hay valor predeterminado.

Tabla 112. Atributos de RosettaNet (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
ToGlobalPartner ClassificationCode	Sí para esquemas RNIF 1.1	El código que identifica una función de socio en la cadena de suministro. Sólo necesario cuando se utilice RNIF 1.1 para PIP basados en esquemas. Este valor debe también especificarse para el pip 0A1, cuando se utilicen PIP basados en esquemas.		No hay valor predeterminado.
Algoritmo de conversión de mensaje de RN	No	Este atributo sólo se utiliza cuando el atributo "Firma digital necesaria" está establecido en Sí. Determina el algoritmo de conversión para utilizar la firma digital. Los valores permitidos son SHA1 y MD5.		SHA1
Algoritmo de cifrado de RN	No	Este atributo sólo se utiliza cuando el atributo "Cifrado" está establecido en "Carga" o "Carga y contenedor". Los valores permitidos son "Triple DES" y "RC2-40".		Triple DES

Atributo de integración de fondo

En este apartado se describe el atributo asociado al empaquetado de integración de programas de fondo.

Tabla 113. Atributo de integración de fondo

Atributo	Descripción	Valor predeterminado
Distintivo de sobre	Este atributo indica si se debe incluir el documento en un sobre XML. Los valores válidos son Sí o No.	No

Atributos de ebMS

Este apartado describe los atributos de ebMS.

Tabla 114. Atributos de ebMS

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Tiempo para el acuse de recibo en min.	No	La cantidad de tiempo que se debe esperar a que llegue una confirmación de recepción antes de reenviar la solicitud original. Este atributo se utiliza junto con Recuento de reintentos. El intervalo se especifica en minutos.	Limitado al paquete o a la conexión	30
Recuento de reintentos	No	El número de veces que se debe enviar una solicitud si no se recibe un acuse de recibo. Este atributo funciona junto con Tiempo de acuse de recibo. Por ejemplo, si este atributo se establece en 3, la solicitud puede enviarse cuatro veces (la primera vez y los tres reintentos).	Limitado al paquete o a la conexión	3

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
No rechazo necesario	No	Indica si este documento necesita o no ser guardado en el almacén de no rechazo. Se aplicará al documento como origen o destino. Sí – Guarde el documento en el almacén de no rechazo. No – No guardar el documento en el almacén de no rechazo.	Limitado al paquete o a la conexión	Sí
Se requiere almacén de mensajes	No	Indica si este documento necesita o no ser guardado en el almacén de mensajes. Se aplicará a los documentos de origen o de destino. Sí – Guarde el documento en el almacén de mensajes. No – No guardar el documento en el almacén de mensajes.	Limitado al paquete o a la conexión	Sí
No rechazo de recibo necesario	No	Indica si el documento de acuse de recibo se debe guardar en un almacén de no rechazo.	Limitado al paquete o a la conexión	Sí
Acuse de recibo solicitado	No	Los posibles valores son siempre, porMensaje y nunca. Si se establece en “siempre”, cuando se envíe un documento ebMS se realizará una solicitud para un acuse de recibo colocando un elemento acknowledgmentRequested en el documento ebMS SOAP. Para el remitente, “porMensaje” y “nunca” quieren decir “No”. Cuando se recibe un documento ebMS si el valor está establecido en “siempre”, el documento entrante debe solicitar el acuse de recibo o fallará en caso contrario. Si el valor está establecido en “porMensaje” en el concentrador del receptor, no hará que el documento falle aún si el documento solicita un acuse de recibo o no. Si el valor se establece como “nunca”, el documento ebMS entrante nunca debe solicitar un acuse de recibo.		nunca

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Firma de acuse de recibo solicitada	No	Los posibles valores son siempre, porMensaje y nunca. "siempre" quiere decir solicitar un acuse de recibo firmado. "porMensaje" y "nunca" implica que puede haber una solicitud de un acuse de recibo sin firma. Esto funciona junto con el atributo "AcknowledgementRequested". Si el valor del atributo AcknowledgmentRequested está establecido en "porMensaje" o "nunca" este atributo no se tendrá en cuenta. . Si no hay valor se utilizará "nunca". Este atributo sólo se utiliza para enviar un documento. Este atributo no se utiliza para un documento recibido.		nunca
Actor	No	No es necesario establecer el atributo en la implementación de ebMS 2.0. El atributo actor es necesario cuando se solicita un acuse de recibo de sincronización. Se coloca en el documento SOAP ebMS. La especificación ebMS 2.0 sugiere un valor constante de http://schemas.xmlsoap.org/soap/actor/next para este atributo (el valor predeterminado). Esto es automático y el usuario no necesita establecer este valor de atributo en ningún caso. Se utilizará en una futura implementación.		http://schemas.xmlsoap.org/soap/actor/next
Compresión necesaria	No	Los posibles valores son "Sí" y "No". Si necesitan comprimirse las cargas ebMS, el valor deberá establecerse en "Sí". Si la compresión no es necesaria, no establezca nada o establézcalo en "No".		No

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Eliminación de duplicados	No	Al enviar un mensaje ebMS, si el valor de este atributo está establecido en “siempre”, colocará un elemento DuplicateElimination en el documento SOAP ebMS. Este elemento DuplicateElimination en el documento SOAP ebMS indica que el concentrador receptor no entregará cargas ebMS a los programas de fondo si el documento ebMS es un duplicado. **Nota:** En un documento SOAP, los valores “porMensaje” y “nunca” no se colocarán en el elemento DuplicateElimination. Al recibir un documento ebMS, si el valor está establecido en “siempre”, el elemento DuplicateElimination debe estar en el documento SOAP ebMS o, en caso contrario, fallará el documento. Si el valor definido es "porMensaje" y el documento recibido tiene el elemento duplicateElimination, se debe realizar la comprobación de duplicados. Para un documento ebMS recibido, si el valor del atributo es “siempre”, y el elemento DuplicateElimination está presente, se comprobará el documento para ver si es un duplicado. Si el documento es un duplicado entonces se fallará el documento. Para el valor "nunca", si el elemento DuplicateElimination está presente en el documento SOAP, el documento fallará. Si no hay ningún valor, se utilizará “nunca”.		nunca
Constituyente de cifrado	No	El valor de este atributo debe ser una lista de tipos de contenidos para cargas separados por signos de punto y coma, por ejemplo, application/xml;text/xml; application/binary:application/edi hará que las cargas con dichos tipos de contenidos se cifren. Este atributo sólo se utiliza si el valor del atributo “Cifrado necesario” está establecido en “Sí”.		application/xml;text/xml; application/EDI-X12; application/EDI-CONSENT; application/EDIFACT; application/binary; application/octet-stream
Parámetro Mime de cifrado	No	Un atributo opcional utilizado para colocar parámetros adicionales como cabeceras MimeMultipart en el documento cifrado. Se aplicará a cada carga cifrada. Valor de ejemplo: smime-type=”enveloped-data” o type=”text/xml” version=”1.0.” Este atributo sólo se utiliza si el valor del atributo “Cifrado necesario” está establecido en “Sí”.		No hay valor predeterminado. **Nota:** Esta variable no se utiliza en la implementación actual. Este valor no afectará al tiempo de ejecución.

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Tipo Mime de cifrado	No	No utilizado en la implementación actual.		No hay valor predeterminado
Cifrado necesario	No	Los posibles valores son “Sí” y “No”. Si se establece en "Sí", se cifrará la carga útil. Este atributo funciona junto con “Constituyente de cifrado”. **Nota:** si “Cifrado necesario” está establecido en “Sí” y no hay tipos de contenido configurados para “Constituyente de cifrado”, no se cifrará nada.		
Transformación de cifrado	No	No utilizado en la implementación actual.		No hay valor predeterminado. **Nota:** Esta variable no se utiliza en la implementación actual. Este valor no afectará al tiempo de ejecución.
Excluir de firma	No	El valor de este atributo será una lista de tipos de contenidos separados por signos de punto y coma, por ejemplo: `application/binary;application/octet-stream`. Las cargas que tienen este tipo de contenido no serán incluidas en la firma. Este atributo sólo se utiliza si el valor del atributo “Firma digital necesaria” es “Sí”.		Si no hay entradas se aplicará la firma a todas las cargas.
Función hash	No	Algoritmo hash que debe utilizarse en la firma XML cuando se realice el hash de las cargas de firmas.Este atributo sólo se utiliza si el valor del atributo “Firma digital necesaria” es “Sí”. Sólo se soporta SHA1 como algoritmo hash para ebMS. Aunque se defina otro algoritmo hash en la conexión para documentos ebMS, SHA1 se utiliza como el algoritmo hash.		SHA1

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Semántica de orden de mensaje	No	Los posibles valores son “Garantizado” y “NoGarantizado”. Cuando se envía un documento, si el valor está establecido en “Garantizado”, se colocará un elemento Orden de mensaje en el documento SOAP. El concentrador de recepción al identificar este elemento en el documento SOAP se asegurará que las cargas se entregan al programa de fondo en secuencia. Para un documento recibido si este atributo está establecido en “Garantizado” el documento ebMS entrante debe tener el elemento MessageOrder presente en él y si falta el documento fallará y se enviará al socio un mensaje de error con el código de error “Inconsistente”.		NoGarantizado
Rol	No	Cuando se envía un documento ebMS este valor de atributo es un valor de elemento de rol en el documento SOAP ebMS. Cuando se recibe un ebMS, este valor de atributo se compara con el valor del elemento de rol en el documento SOAP ebMS y si los valores no coinciden (incluso si el valor del atributo está vacío), el documento fallará y se enviará un mensaje de error al socio con el código de error “Inconsistente”.		No hay valor predeterminado
Duración continua	No	El tiempo en minutos durante el cual el documento debería persistir, por ejemplo 1440 para 24 horas. Cuando se envía un documento, la Duración continua se utiliza para calcular el valor de TimeToLive utilizando la fórmula: TimeToLive = Duración continua + (núm. de reintentos * RetryInterval). Cuando se recibe un documento, la Duración continua se utiliza para eliminar los duplicados. Si se recibe un documento con el ID de mensaje duplicado, se comprobará si se ha pasado o no la Duración continua del documento anterior. Si no se ha pasado la duración continua, se marcará el documento como duplicado o, en caso contrario, no será marcado como duplicado. Si no hay ninguna entrada tomará el valor predeterminado de 0.		0

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Constituyente de empaquetado	No	No utilizado en la implementación actual.		No hay valor predeterminado. **Nota:** Esta variable no se utiliza en la implementación actual. Este valor no afectará al tiempo de ejecución.
Parámetro Mime de paquete	No	No utilizado en la implementación actual.		No hay valor predeterminado. **Nota:** Esta variable no se utiliza en la implementación actual. Este valor no afectará al tiempo de ejecución.
Algoritmo de cifrado	Sí cuando el valor del atributo “Cifrado necesario” está establecido en “Sí”	El algoritmo utilizado para cifrar cargas. Este valor funciona junto con el atributo "Protocolo de cifrado". Este atributo sólo se utiliza si el valor del atributo “Cifrado necesario” está establecido en “Sí”.		AES-128
Protocolo de cifrado	No	El protocolo utilizado para cifrar las cargas. Los posibles valores son XMLEncryption y SMIME. Este atributo sólo se utiliza si el valor del atributo “Cifrado necesario” está establecido en “Sí”. Si EncryptionRequired se establece en "sí" pero no se proporciona ningún valor para este atributo, el documento fallará.		XMLEncryption
Intervalo de reintentos	No	Para un documento enviado el intervalo de reintentos en minutos para esperar un acuse de recibo antes de volver a enviar el documento ebMS. Los documentos ebMS sólo se vuelven a enviar cuando se solicita un acuse de recibo pero el socio no ha recibo un acuse de recibo dentro del intervalo de reintentos. Un valor de 0 indica que no habrá reintentos. Este atributo trabaja junto con el atributo “Recuento de reintentos”.		270
Algoritmo de firma	Sí, si "Firma digital necesaria" es Sí	Algoritmo utilizado para firmar el documento. Este atributo sólo se utiliza si el valor del atributo “Firma digital necesaria” es “Sí”. **Nota:** En ebMS, no se da soporte a hmac-sha1.		dsa-sha1

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Transformación de firma	No	El algoritmo de transformación utilizado para transformar las cargas antes de crear la firma XML. Este atributo sólo se utiliza si el valor del atributo "Firma digital necesaria" es "Sí".		No hay valor predeterminado
Modalidad de respuesta sínc.	No	El tipo de respuesta síncrona necesaria para el documento que se está enviando. Si el valor está establecido como: • **MSHSignalsOnly** - Sólo se enviarán los documentos de acuse de recibo/error MSH a través de una conexión síncrona. Los documentos de respuesta de empresa y de señal de empresa se devolverán asíncronamente. • **signalsOnly** – sólo se enviarán los documentos de señal de empresa y MSH a través de una conexión síncrona. La respuesta de empresa será devuelta asíncronamente. • **responseOnly** – Sólo se enviarán las respuestas de empresa y documentos MSH a través de una conexión síncrona. Los documentos de señal de empresa no serán devueltos. • **signalsAndResponse** - Los documentos de respuestas de empresa y de señal de empresa se enviarán a través de una conexión síncrona. • **ninguno** – no hay documentos de respuesta síncrona del receptor.		ninguno
Comprobación inteligible necesaria	No	El valor de este atributo se envía al programa de fondo como el valor de la cabecera "x-aux-IntelligibleCheckRequired". Los posibles valores son "Sí" y "no". El propósito es indicar al programa de fondo que ReceiptAcknowledgement sólo debe enviarse si el documento ebXML con la carga no contiene ningún error. Depende del programa de fondo interpretar este valor.		No
Método de canonicalización	No	El algoritmo de canonicalización utilizado antes de realizar la firma XML. Este atributo sólo se utiliza si el valor del atributo "Firma digital necesaria" es "Sí".		INCLUSIVE_ CON_ COMENTARIOS
Constituyente de compresión	No	La lista de tipos de contenido de cargas separados por signos de punto y coma que deben comprimirse. Por ejemplo, si es necesario comprimir cargas con el contentType "text/xml" y "application/edi", el valor de este atributo será "text/xml;application/edi". Ninguna entrada querrá decir que no se comprimirá ninguna carga incluso si "Compresión necesaria" está establecido en "Sí" Este atributo sólo se utiliza si el valor del atributo "Compresión necesaria" es "Sí".		application/xml; text/ xml;application/ EDI-X12; application/ EDI-CONSENT; application/ EDIFACT

Tabla 114. Atributos de ebMS (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Service Type	Sí si el valor del elemento Servicio (tipo de documento) no es un URI	Cuando se envía un documento ebMS, el valor del elemento ebMSService en el mensaje SOAP ebMS debe ser un URI o cualquier cadena de texto. Si es una cadena de texto, es necesario este tipo de atributo. Si el valor de Servicio (Tipo de documento) no es un URI, el valor de atributo de este Tipo de servicio se utilizará como valor de atributo de tipo en el documento ebMS.		No hay valor predeterminado

Atributos generales

Este apartado describe los atributos generales.

Tabla 115. Atributos generales

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Correlación de validación	No	La correlación de validación que debe utilizarse para validar este documento. La acción que se utiliza durante el tiempo de ejecución tiene que tener un paso de validación que haga uso de este atributo. Sólo las correlaciones de validación que se hayan subido y asociado con este tipo de documento podrán ser seleccionadas.	Limitado al paquete o a la conexión	No hay valor predeterminado.
Atributo de usuario 1	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán establecidos en el objeto de documento de empresa con el atributo bcg.ro.user.User01 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.
Atributo de usuario 2	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User02 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.
Atributo de usuario 3	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User03 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.

Tabla 115. Atributos generales (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Atributo de usuario 4	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User04 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.
Atributo de usuario 5	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User05 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.
Atributo de usuario 6	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User06 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.
Atributo de usuario 7	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User07 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.
Atributo de usuario 8	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User08 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.
Atributo de usuario 9	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User09 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.

Tabla 115. Atributos generales (continuación)

Atributo	Obligatorio	Descripción	Restricciones	Valor predeterminado
Atributo de usuario 10	No	Para su utilización en salidas definidas por el usuario. El valor queda determinado por el creador de la salida definida por el usuario. Estos serán definidos en el objeto de documento de empresa con el atributo bcg.ro.user.User10 como prefijo De (documento de origen) o A (documento de destino).		No hay valor predeterminado.

Atributos de OpenPGP

Después de crear una conexión entre el socio externo y el socio interno, es necesario definir los atributos de conexión como se describe en este tema.

En la página **Gestionar conexiones**, después de activar una conexión, pulse **Atributos** en el lado de destino de las funciones B2B para definir valores para atributos de conexión específicos de OpenPGP.

Los distintos atributos de conexión de OpenPGP son los siguientes:

Tabla 116. Atributos de OpenPGP

Atributo	Obligatorio	Descripción	Valor predet.
utilizar formato OpenPGP	Sí	Defina el lado de destino de las funciones B2B en la página Gestionar conexiones en "Sí" para utilizar el formato OpenPGP.	No hay valor predet.
Cifrado necesario	Opcional	Puede utilizar este atributo para cifrar las cargas útiles. Para cifrar las cargas útiles, establezca el valor en "Sí".	No hay valor predet.
preferencia de algoritmo simétrico	Obligatorio	Este atributo es el algoritmo de claves preferido que se utiliza para el cifrado de OpenPGP. En la lista desplegable, seleccione la preferencia de algoritmo simétrico. Si el atributo **Cifrado necesario** está establecido en verdadero, es obligatorio definir este atributo.	No hay valor predet.
Detección de modificaciones	Opcional y sólo se selecciona con cifrado	Si desea imponer la comprobación de integridad de mensajes, establezca este atributo en verdadero. Así se verifica si el mensaje se ha manipulado o no durante la transición.	No hay valor predet.
Compresión necesaria	Opcional	Puede utilizar este atributo para comprimir las cargas útiles. Defina este atributo en Sí para la compresión.	No hay valor predet.
preferencia de algoritmo de compresión	Obligatorio	Este atributo es el algoritmo de compresión preferido para OpenPGP. En la lista desplegable, seleccione el algoritmo de compresión preferido. Si el atributo **Compresión necesaria** está establecido en verdadero, es obligatorio definir este atributo.	No hay valor predet.

Tabla 116. Atributos de OpenPGP (continuación)

Atributo	Obligatorio	Descripción	Valor predet.
blindaje	Opcional	OpenPGP codifica datos en blindaje ASCII. Coloca cabeceras específicas en torno a los datos codificados de Radix-64 para que OpenPGP pueda reconstruir los datos más tarde. El blindaje ASCII también se utiliza para proteger datos binarios si formato cuando se transfieren por la conexión. Si lo establece en verdadero en el lado de destino de la conexión, el blindaje se lleva a cabo en el empaquetado de documentos. Definir un valor para este atributo es opcional.	No hay valor predet.

Avisos

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

Puede que IBM no ofrezca los productos, servicios o características que se tratan en este documento en otros países. Póngase en contacto con el representante de IBM para obtener información sobre los productos y servicios actualmente disponibles en su área. Las referencias hechas a productos, programas o servicios IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios IBM. Se puede utilizar en su lugar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ningún derecho de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y comprobar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o aplicaciones de patente pendientes que afecten a los temas tratados en este documento. La entrega de este documento no le otorga ninguna licencia sobre estas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

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

Para consultas sobre licencias en las que se solicite información sobre el juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país o envíe directamente las consultas por escrito a:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106-0032, Japón.

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente:INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO PERO NO LIMITÁNDOSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO. Algunos estados o países no permiten la renuncia a las garantías explícitas o implícitas en ciertas transacciones, por tanto, es posible que esta declaración no resulte aplicable a su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información que contiene este documento está sometida a cambios frecuentes; estos cambios se incorporarán a las nuevas ediciones de la publicación. IBM se reserva el derecho a realizar, si lo considera oportuno, cualquier mejora o modificación en los productos o programas que se describen en esta publicación y sin notificarlo previamente.

Las referencias en este documento a sitios web que no sean de IBM se proporcionan únicamente como ayuda y no se consideran en modo alguno como una recomendación por parte de IBM de dichos sitios web. Los materiales de dichos sitios web no forman parte de este producto de IBM y la utilización de los mismos será por cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que se le suministre de cualquier modo que considere adecuado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de una licencia de este programa que deseen obtener información acerca del mismo con el objeto de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información intercambiada, deben ponerse en contacto con:

Director del laboratorio de Burlingame de IBM
IBM Burlingame Laboratory
577 Airport Blvd., Suite 800
Burlingame, CA 94010
EE.UU.

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

El programa bajo licencia que se describe en esta información, y todos los materiales bajo licencia disponibles para el mismo, los proporciona IBM bajo los términos del Acuerdo de licencia de cliente IBM, del Acuerdo internacional de programas bajo licencia de IBM o de cualquier acuerdo equivalente entre el cliente e IBM.

Cualquier información de rendimiento que aparezca en este documento ha sido determinada en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos podrían ser distintos. Algunas mediciones podrían haberse realizado en sistemas en desarrollo y, por lo tanto, no existe ningún tipo de garantía de que dichas mediciones sean las mismas en los sistemas con disponibilidad general. Además, algunas mediciones podrían haberse estimado mediante extrapolación. Los resultados reales podrían ser diferentes. Los usuarios de este documento deberán verificar los datos aplicables para su entorno específico.

La información relacionada con los productos que no son de IBM se ha obtenido de los proveedores de dichos productos, sus anuncios publicados u otras fuentes de disponibilidad pública. IBM no ha comprobado estos productos y no puede confirmar la precisión de su rendimiento, compatibilidad ni contemplar ninguna otra reclamación relacionada con los productos que no son de IBM. Las preguntas relacionadas con las posibilidades de los productos que no son de IBM deberán dirigirse a los proveedores de estos productos.

Todas las afirmaciones referentes a la dirección o pretensiones futuras de IBM se pueden modificar o retirar sin aviso y representan simplemente metas y objetivos.

Todos los precios de IBM que se muestran son los precios de venta al detalle sugeridos por IBM, están actualizados y están sujetos a cambios sin previo aviso. Los precios de los proveedores pueden variar.

Esta información está destinada a planificación. La información aquí contenida está sujeta a cambios antes de que los productos que se describen estén disponibles.

En esta información aparecen ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlos como realmente posibles, los ejemplos incluyen los nombres de individuos, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con los nombres y las direcciones de una empresa real es pura coincidencia.

LICENCIA DE COPYRIGHT

Esta información contiene programas de aplicación de ejemplo en el idioma origen, en los que encontrará técnicas de programación sobre diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma gratuitamente, con el propósito de desarrollar, utilizar, comercializar o distribuir programas de aplicación compatibles con la interfaz de programas de aplicación para la plataforma operativa para la que se han escrito los ejemplos. Estos no han sido probados en su totalidad ni en todas las situaciones posibles. Por tanto, IBM, no puede garantizar la fiabilidad, la capacidad de servicio ni el funcionamiento de estos programas.

Cada copia o cualquier parte de estos programas de ejemplo o cualquier obra derivada debe incluir un aviso de copyright como el siguiente:

Si ve la copia software de esta información, es posible que no aparezcan las fotografías ni las ilustraciones en color.

Información sobre la interfaz de programación

La información de la interfaz de programación, si se proporciona, está especialmente indicada para ayudarle a crear software de aplicación utilizando este programa. Las interfaces de programación de uso general le ayudan a escribir software de aplicaciones que obtengan los servicios de estas herramientas del programa. Sin embargo, esta información también contiene datos de diagnóstico, modificación y ajuste. La información de diagnóstico, modificación y ajuste se proporciona como ayuda para la depuración del software de aplicación.

Atención: No utilice esta información de diagnóstico, modificación y ajuste como interfaz de programación, puesto que está sujeta a cambios.

Marcas registradas y marcas de servicio

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

IBM	DB2	IMS	MQIntegrator	Tivoli
el logotipo de IBM	DB2 Universal Database	Informix	MVS	WebSphere
AIX	Domino	iSeries	OS/400	z/OS
CICS	IBMLink	Lotus	Passport Advantage	
CrossWorlds	i5/OS	Lotus Notes	SupportPac	

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

MMX, Pentium y ProShare son marcas registradas de Intel Corporation en los Estados Unidos y/o en otros países.

Solaris, Java y todas las marcas registradas basadas en Java son marcas registradas de Sun Microsystems Inc. en los Estados Unidos, otros países o ambos.

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

Los demás nombres de compañías, productos o servicios pueden ser marcas registradas o marcas de servicio de otras empresas.

WebSphere Partner Gateway Enterprise Edition y Advanced Edition incluyen software desarrollado por Eclipse Project (www.eclipse.org)

Índice

Números

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X

Impreso en España