WebSphere®

IBM WebSphere Partner Gateway Enterprise et Advanced Editions

Version 6.2.1

Guide de configuration du concentrateur

IBM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la rubrique «Remarques», à la page 477.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Chapitre 1. A propos de ce guide

Ce document décrit la procédure de configuration du serveur IBM WebSphere Partner Gateway.

Public concerné

Les administrateurs gérant WebSphere Partner Gateway. Ce manuel suppose deux types d'administrateurs :

- Administrateur du concentrateur
- Administrateur de comptes

L'administrateur de concentrateur est le superutilisateur de la communauté. Il est responsable de l'ensemble de la configuration et de la gestion de la communauté du concentrateur, notamment la configuration des partenaires et l'activation des connexions. L'administrateur de comptes a accès à un sous-ensemble des fonctions de l'administrateur de concentrateur et il est le principal utilisateur d'administration pour le partenaire interne ou le partenaire externe.

Remarque : La console de l'administrateur de concentrateur, des partenaires externes et des partenaires internes sera différente selon ses commandes/droits.

Conventions typographiques

Ce document utilise les conventions typographiques suivantes.

Tableau 1. Conventions typographiques

Convention	Description
`Police monospace`	Le texte dans cette police indique qu'il s'agit de texte que vous tapez, de valeurs pour des arguments ou des options de commande, d'exemples et d'exemples de code ou d'informations que le système imprime à l'écran (texte de message ou invite).
gras	Le texte en gras correspond aux commandes de l'interface graphique (par exemple, les noms des boutons en ligne, les noms ou les options de menu) et aux en-têtes de colonne dans des tables et du texte.
italique	Le texte en italique permet la mise en évidence de texte telle que des titres de manuels, des nouveaux termes ou des termes définis dans le texte, des noms de variables ou des lettres de l'alphabet utilisées comme lettres.
`Police monospace en italique`	Le texte figurant dans cette police signale les noms de variable dans le texte de police monospace.
ProductDir	*rép_produit* représente le répertoire dans lequel le produit est installé. Tous les noms de chemins du produit IBM WebSphere Partner Gateway se rapportent au répertoire dans lequel IBM WebSphere Partner Gateway est installé sur le système.

Tableau 1. Conventions typographiques (suite)

Convention	Description
%texte% et *$texte*	Le texte placé entre des signes de pourcentage (%) indique la valeur de la variable système ou utilisateur `text` de Windows(R). La notation équivalente dans un environnement UNIX(R) est $h*text*, ce qui indique la valeur de la variable d'environnement *text* d'UNIX
Texte en couleur souligné	Le texte en couleur souligné indique une référence croisée. Cliquez sur le texte pour atteindre l'objet de référence.
Texte avec contour bleu	(Dans les fichiers PDF uniquement) Un contour bleu autour du texte indique une référence croisée. Cliquez sur le texte avec contour pour atteindre l'objet de référence. Cette convention est l'équivalent pour les fichiers PDF de la convention “texte en couleur souligné” mentionnée dans ce tableau.
“ ” (guillemets)	(Dans les fichiers PDF uniquement) Les guillemets sont placés par part et d'autre de références croisées à d'autres section du document.
{ }	Dans une ligne de syntaxe, des accolades entourent un jeu d'options parmi lesquelles une seule doit être sélectionnée.
[ ]	Dans une ligne de syntaxe, les crochets entourent des paramètres facultatifs.
< >	Des crochets en chevron entourent les éléments variables d'un nom pour les distinguer les uns des autres. For example, *<server_name><connector_name>*`tmp.log`.
/ ou \	Des barres obliques inversées (\) servent de séparateurs dans les chemins d'accès aux répertoires dans les installations Windows. Pour les installations UNIX, remplacez les barres obliques inverses par des barres obliques standard (/).

Documents associés

Toute la documentation disponible sur ce produit comprend des informations détaillées sur l'installation, la configuration, l'administration et l'utilisation de WebSphere Partner Gateway Enterprise Edition et Advanced Edition.

Vous pouvez télécharger ou lire cette documentation en ligne sur le site suivant :

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

Remarque : Des informations importantes relatives à ce produit peuvent être disponibles dans les notes techniques et les lettres d'informations du service d'assistance émises après la publication de ce document. Celles-ci sont disponibles sur le site Web WebSphere Business Integration Support, à l'adresse suivante :

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

Sélectionnez la zone correspondant au composant qui vous intéresse et consultez les sections Technotes (notes techniques) et Flashes (lettres d'informations).

Nouveautés de l'édition 6.2.1

WebSphere Partner Gateway 6.2.1 prend en charge les nouvelles fonctions suivantes :

- La boîte aux lettres Web est une prise en charge Web de l'interaction business-to-business. Les partenaires, clients et fournisseurs interagissent avec le concentrateur WebSphere Partner Gateway en utilisant uniquement le navigateur Internet.
- Le serveur intégré SFTP est pris en charge en plus du serveur intégré FTP.
- Le certificat OpenPGP est pris en charge dans WebSphere Partner Gateway.
- Prise en charge de WebSphere Application Server ND 7.0.0.13, WebSphere Messaging Queue 7.0 et WTX 8.3.
- Prise en charge des plateformes Windows 2008, Windows 7 et SLES 11.
- Prise en charge de Power 7 -mode de tolérance (modes de compatibilité P6/P6+).
- Prise en charge de la virtualisation - VMware® ESX avec Windows et Linux, Power VM avec AIX.

Chapitre 2. Introduction à la configuration du concentrateur

Après avoir installé WebSphere Partner Gateway et avant l'échange de documents entre les partenaires internes et externes, vous devez configurer le serveur WebSphere Partner Gateway (c'est-à-dire le concentrateur).

Ce chapitre contient les rubriques suivantes :

Présentation de la configuration du concentrateur

L'objectif est de permettre au partenaire interne d'envoyer un document ou un ensemble de documents (par voie électronique) à un partenaire externe, ou de recevoir un document ou un ensemble de documents d'un partenaire externe. Le concentrateur gère la réception des documents, leur conversion dans d'autres formats (si nécessaire) et leur livraison. Le concentrateur peut également être configuré afin d'offrir une sécurité dans le cas des documents entrants et sortants.

Les documents échangés entre le concentrateur et un partenaire sont généralement dans un format standard et représentent une interaction métier spécifique. Par exemple un partenaire peut envoyer un bon de commande en tant que a RosettaNet 3A4 PIP, ou d'un document cXML OrderRequest, ou d'un échange EDI-X12 avec une transaction 850. Le concentrateur transforme le document dans un format utilisable par une application du partenaire interne. De même, une application dorsale du partenaire interne peut envoyer une réponse au bon de commande dans son propre format personnalisé qui est converti dans un format standard. Le document converti est ensuite envoyé au partenaire.

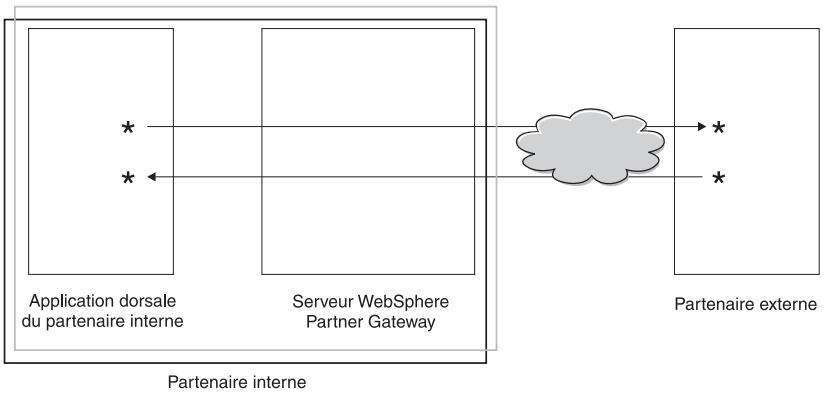


Figure 1. Circulation des documents via le concentrateur

Dans ce guide, vous verrez comment configurer le concentrateur puis comment configurer les partenaires. Vous apprendrez également comment configurer les paramètres de sécurité pour le concentrateur.

Notez dans la figure 1, à la page 5 que le serveur WebSphere Partner Gateway et l'application dorsale du partenaire interne appartiennent tous au partenaire interne. Ce dernier correspond à l'entreprise qui est propriétaire du concentrateur. Comme vous le verrez dans les chapitres suivants, la méthode de définition d'un profil de partenaire interne est la même pour les partenaires externes.

Remarque : Ce document vous apprend à créer les connexions qui circulent de l'application dorsale du partenaire interne vers une destination de partenaire et d'un partenaire externe vers la destination du partenaire interne. Une fois que les documents sont arrivés à la destination du partenaire interne, vous souhaiterez probablement les intégrer à une application dorsale telle que WebSphere InterChange Server ou WebSphere MQ Broker. Les tâches requises pour permettre l'intégration de WebSphere Partner Gateway et de ces applications dorsales sont définies dans le *Guide d'intégration de WebSphere Partner Gateway Enterprise*.

Informations nécessaires à la configuration du concentrateur

Pour configurer le concentrateur, vous devez disposer d'informations concernant les types d'échanges auxquels le partenaire interne participera. Par exemple, vous devez disposer des informations suivantes :

- Quels types de documents (par exemple, EDI-X12 ou langage XML personnalisé) les partenaires internes et externes enverront via le concentrateur ?
- Quels types de transports (par exemple, HTTP ou FTP) les partenaires internes et externes utiliseront pour envoyer les documents ?
- Un document entrant dans le concentrateur devra-t-il être fractionné en plusieurs documents ou les documents individuels devront-ils être regroupés avant d'être envoyés ?
- Les documents subiront-ils une transformation avant d'être livrés ?
- Les documents seront-ils validés avant d'être livrés ?
- Un document sera-t-il vérifié pour voir s'il constitue un double avant d'être livré ?
- Les documents seront-ils chiffrés ou signés numériquement, ou utiliseront-ils une autre technique de sécurité ?

Une fois en possession de ces informations, vous êtes en mesure de débuter la configuration du concentrateur.

Après avoir défini le concentrateur, vous pouvez définir vos partenaires externes à partir des informations (telles que l'adresse IP et les numéros DUNS) qu'ils vous ont fournies. Comme indiqué précédemment, vous définissez également le partenaire interne comme un type spécial de partenaire du concentrateur.

Présentation des transports

Il est possible d'envoyer des documents depuis les partenaires vers WebSphere Partner Gateway (le concentrateur) par le biais de plusieurs transports. Un partenaire peut envoyer des documents sur des réseaux publics via HTTP, HTTPS, JMS, FTP, FTPS, script FTP, SMTP, SFTP ou un fichier-répertoire. Il peut également le faire sur un VAN (Value Added Network), un réseau privé, à l'aide d'un transport de script FTP. Vous pouvez également créer votre propre transport.

Remarque : Lors de l'utilisation d'un fichier-répertoire entre un partenaire et le concentrateur, l'administrateur doit prendre en considération tous les problèmes liés à la sécurité.

De la même façon, le concentrateur envoie des documents aux applications dorsales par le biais de divers transports. Les plus répandus entre le concentrateur et les applications dorsales sont HTTP, HTTPS, JMS, fichier-répertoire, script FTP, FTP, SFTP et SMTP.

La figure 2 affiche les transports HTTP, HTTPS, JMS et de fichier-répertoire.

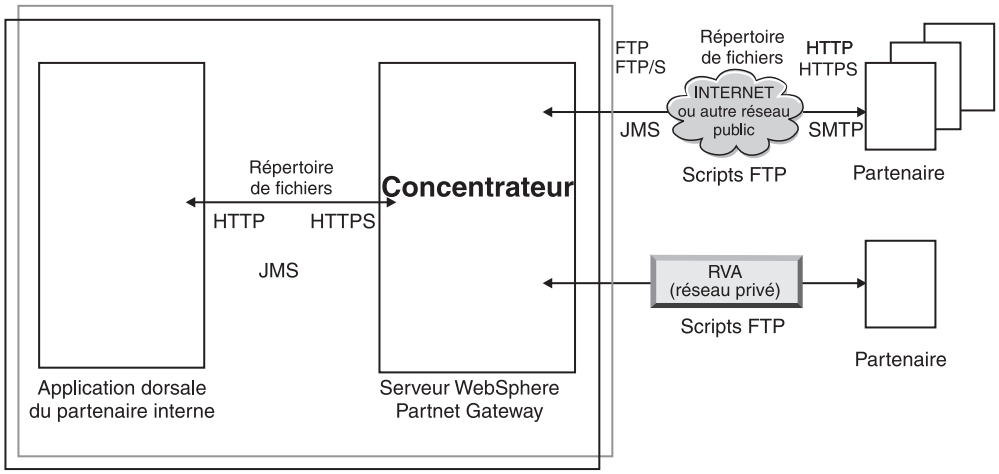


Figure 2. Transports les plus communs pris en charge par WebSphere Partner Gateway

Le type de transport utilisé pour envoyer et recevoir des documents a des répercussions sur la définition des récepteurs et des destinations. Un *Récepteur* est un point d'entrée dans le concentrateur - le lieu où les documents envoyés par les partenaires ou les applications dorsales sont reçus dans le concentrateur. Une *destination* est un point d'entrée dans l'ordinateur ou le système dorsale du partenaire -- l'emplacement où le concentrateur envoie des documents. Avant d'utiliser les transports FTP, FTPS, script FTP, JMS et fichier-répertoire, vous devez procéder à certains paramétrages décrits au Chapitre 4, «Etapes préalables à la configuration du concentrateur», à la page 35.

Présentation des définitions de document

Lorsque vous définissez l'échange de documents entre les partenaires externes et internes, vous devez apporter quelques précisions concernant le document :

- L'*empaquetage* qui entoure le document
- Le *protocole* métier qui définit une classe de documents qui partagent des caractéristiques communes
- Le *type de document* qui identifie un des documents qui sont fournis par le protocole métier

L'empaquetage et le protocole du document ainsi que le type de document constituent la *définition du document*. Supposez que vous utilisez la définition de document fournie par le produit pour :

- Empaquetage : AS
- Protocole : EDI-X12
- Type de document : ISA

Voici ce qui se passe lorsqu'un document conforme à cette définition de routage est reçu. Dès que le concentrateur reçoit le document, l'étape d'empaquetage du flux de travaux entrant détermine que le package AS est utilisé par le document. C'est en raison de la présence d'en-têtes de transport qui ne sont pas spécifiés pour l'empaquetage AS. D'autres types d'empaquetages sont découverts de la même manière par le concentrateur, généralement en examinant les en-têtes de transport fournis avec le document. Lorsqu'il n'y a pas de correspondance avec un type d'empaquetage, le type d'empaquetage None est attribué au document. Dans le cas de l'empaquetage AS, les identificateurs entreprise origine et destination sont obtenus à partir de l'en-tête de transport du message. D'autres en-têtes sont également transportés avec les en-têtes de transport AS, qui peuvent spécifier si le message est chiffré, compressé, signé ou pas.

Après avoir identifié l'empaquetage, l'étape d'analyse du protocole de flux de travaux entrant fixée par le concentrateur détermine le type de protocole et de document du document. Cela est fait en examinant le contenu du message réel et en recherchant les caractéristiques du document qui identifient le type de protocole et de document. L'étape de flux de travaux d'analyse du protocole extrait également d'autres informations du document, en fonction du protocole utilisé.

Une fois que l'on sait que le document utilise un empaquetage, protocole et type de document spécifique, le concentrateur peut passer au traitement du document. A ce stade, parallèlement au type de package, de protocole et de document, il connaîtra également les ID entreprise origine et destination. Compte tenu de cette information, le concentrateur peut rechercher une connexion entre les partenaires d'origine et de destination qui possède le type de document, protocole et package entrant.

Dès que la connexion est trouvée, le concentrateur sait comment router et traiter le document car il peut trouver les informations supplémentaires suivantes :

- Certificats des partenaires d'origine et de destination (si nécessaire)
- Configurations d'attribut pour le routage d'origine et le routage de destination
- L'action à exécuter lors du routage du document
- La mappe de transformation applicable (le cas échéant)
- La mappe de validation applicable (le cas échéant)

Empaquetage

L'empaquetage fournit des informations concernant la transmission du document. Comme indiqué dans la précédente section, si l'empaquetage est de type AS, le concentrateur utilise les informations de l'en-tête AS pour déterminer la source et la destination du document. Si un partenaire envoie un PIP RosettaNet au partenaire interne, le PIP est empaqueté en tant que RNIF.

La figure 3 présente les types d'empaquetages pouvant être définis pour les documents échangés entre le concentrateur et un partenaire externe, et entre le concentrateur et une application dorsale.

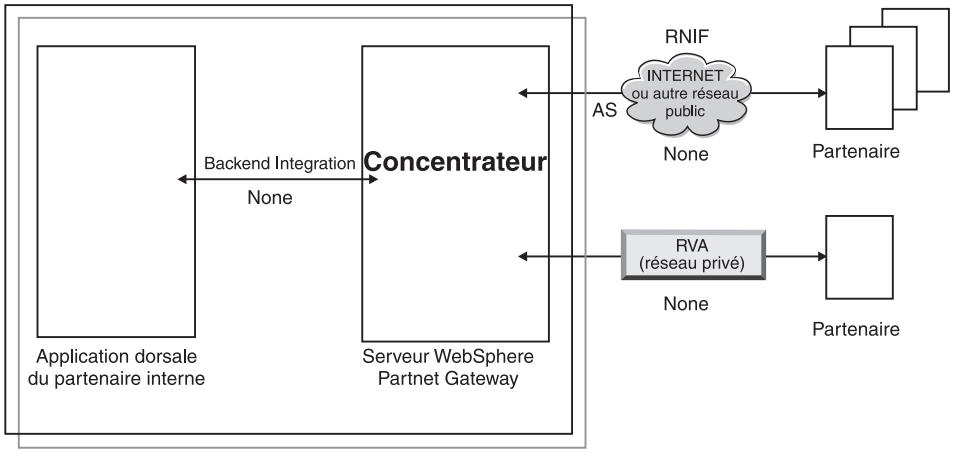


Figure 3. Types d'empaquetages de documents

Des packages sont associés à des protocoles spécifiques. Par exemple, un partenaire doit préciser un package RNIF lors de l'envoi d'un document RosettaNet au concentrateur.

Intégration dorsale : Comme l'indique la figure 3, l'intégration dorsale n'est disponible qu'entre le concentrateur et l'application dorsale. Lorsque vous précisez un package Backend Integration, les documents envoyés par le concentrateur au système dorsal sont accompagnés d'informations d'en-tête supplémentaires. De même, lorsqu'une application dorsale envoie au concentrateur des documents avec un package Backend Integration, elle doit ajouter des informations d'en-tête. Le package Backend Integration et les conditions requises pour les informations d'en-tête sont décrits dans le *Guide d'intégration de WebSphere Partner Gateway Enterprise*.

AS : L'empaquetage AS est plus communément utilisé entre les partenaires et le concentrateur . L'empaquetage AS peut être utilisé pour des documents conformes aux standards AS1, AS2 etAS3. AS1 est un standard utilisé pour sécuriser la transmission des messages par SMTP. De même, AS2 est un standard utilisé pour sécuriser la transmission des messages par HTTP ou HTTPS. AS3 est un nouveau standard utilisé pour sécuriser la transmission des messages sur FTP ou FTPS. Les documents envoyés par un partenaire avec un package AS sont accompagnés d'informations d'en-tête AS1 ou AS3. Les documents envoyés à un partenaire attendant des en-têtes AS1 ou AS2 doivent être empaquetés (au niveau du concentrateur) en tant que AS.

None : L'empaquetage None peut servir à échanger des documents entre le concentrateur et les partenaires, et entre le concentrateur et l'application dorsale. Aucune information d'en-tête n'est ajoutée (ou attendue) pour ce mode d'empaquetage.

RNIF : L'empaquetage RNIF est fourni sur le support d'installation. Téléchargez l'empaquetage RNIF (ainsi que les PIP qui doivent être échangés) en appliquant la procédure décrite dans «Documents RosettaNet», à la page 118. L'empaquetage RNIF sert à envoyer des documents RosettaNet du partenaire au concentrateur ou du concentrateur au partenaire.

ebMS : Le mécanisme Service de Messagerie ebXML (ebMS) fournit un moyen standard d'échanger des messages commerciaux entre partenaires commerciaux ebXML. Il fournit un moyen fiable d'échanger des messages commerciaux sans dépendre de technologies et solutions propriétaires. Un message ebXML contient des structures pour un en-tête de message (nécessaire pour le routage et la livraison) et une section de charge.

ebMS offre un moyen standard d'échanger des messages commerciaux entre partenaires commerciaux ebXML. Un message ebXML est un protocole de communication indépendant MIME/Multipart message envelope.

N/A : Certains types de documents se terminent sur WebSphere Partner Gateway ou sont émis en interne par WebSphere Partner Gateway. Pour les types de documents qui s'arrêtent sur WebSphere Partner Gateway, aucun empaquetage n'est nécessaire. Les types de documents qui prennent leur origine dans WebSphere Partner Gateway n'ont pas d'empaquetage source. Par conséquent, pour ces deux types de flux, l'empaquetage à indiquer est N/A.

Pour la plupart des transmissions unidirectionnelles entre un partenaire externe et le partenaire interne (ou vice-versa), WebSphere Partner Gateway reçoit un document d'un partenaire externe et l'envoie au partenaire interne. Dans WebSphere Partner Gateway, lors de la création de la connexion du partenaire, vous indiquez l'empaquetage dans lequel WebSphere Partner Gateway recevra le document, ainsi que l'empaquetage qu'elle utilisera pour envoyer le document. Dans la figure 4, un document empaqueté en tant que AS circule d'un partenaire externe vers le système dorsal du partenaire interne. Ce document est fourni sans en-tête de transport à la destination du partenaire interne. Dans la figure 4, une activité est associée à l'échange de documents.

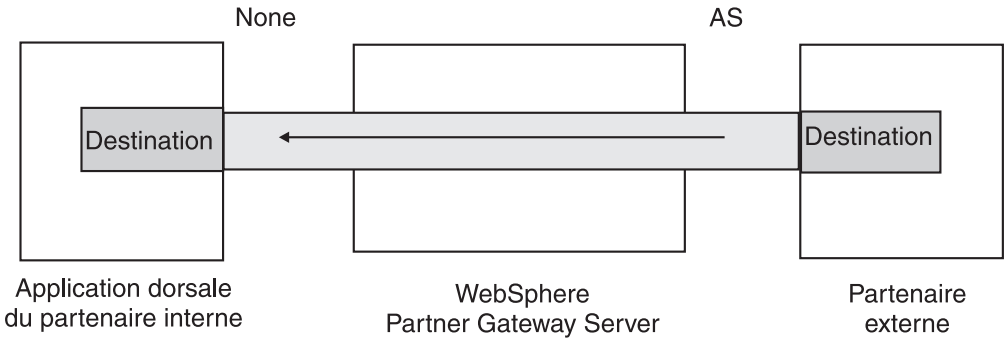


Figure 4. Connexion unidirectionnelle type

Cependant, certains protocoles impliquent de nombreuses activités (telles que désenveloppement et transformation), dont certaines interviennent comme des éléments intermédiaires de l'échange global. Par exemple, si un partenaire envoie un EDI au concentrateur à destination du partenaire interne, cet échange est désenveloppé et les transactions EDI individuelles sont traitées. Un empaquetage est associé à l'EDI d'origine, lors de son envoi à partir du partenaire. Cependant, l'EDI proprement dit n'étant pas distribué au partenaire interne (il est désenveloppé dans le concentrateur sans aucun autre traitement), l'empaquetage n'est pas nécessaire. Lorsque vous définissez l'interaction correspondant à l'étape de désenveloppement, précisez un empaquetage du côté de l'émetteur mais indiquez N/A du côté du destinataire.

Le processus de paramétrage des définitions de documents requis pour un EDI est décrit au Chapitre 10, «Configuration des flux de documents EDI», à la page 179.

Protocoles

Les protocoles fournis avec le système sont les suivants :

- Binaire

  Le protocole Binaire peut être utilisé avec les packages AS, None et Backend Integration. Un document binaire ne contient pas de données sur sa source ou sa destination.

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

  Ces protocoles EDI peuvent être utilisés avec les packages AS ou None. Comme indiqué dans « N/A», à la page 10, si la transaction ou l'EDI est émis par le concentrateur ou lui est destiné, indiquez N/A comme package. Les normes EDI X12 et EDIFACT sont utilisées pour l'échange de données. EDI-Consent fait référence aux types de contenu indiqué dans la spécification EDI-Consent.

- service Web

  Les demandes de Service Web ne peuvent être utilisées qu'avec l'empaquetage None.

- cXML

  Les documents cXML ne peuvent être utilisés qu'avec l'empaquetage None.

- XMLEvent

  XMLEvent est un protocole spécial utilisé pour fournir une notification d'événement pour les documents émis ou reçus par l'application dorsale. Il ne peut être utilisé qu'avec l'empaquetage Backend Integration. Ce protocole est décrit dans le *Guide d'intégration de WebSphere Partner Gateway Enterprise*.

Lorsque vous téléchargez des packages RNIF, vous extrayez également les protocoles associés (RosettaNet et RNSC). RosettaNet (le protocole utilisé entre le partenaire et le concentrateur) est associé au package RNIF. RNSC (protocole utilisé entre le concentrateur et l'application dorsale du partenaire interne) est associé au package Backend Integration.

Pour la transformation transactions EDI, ou de documents XML ou ROD, le client Data Interchange Services (DIS) ou WTX design studio est utilisé pour créer les mappes de transformation.

Dans le client DIS, des dictionnaires sont définis pour le protocole associé à cette transformation. Un dictionnaire contient les informations pour tous les segments, définitions, éléments de données composites et éléments de données du document EDI qui composent le standard EDI. La définition des documents source pour EDI est fournie par WDI, mais pour ROD et XML, vous devez la créer en utilisant le client DIS. Depuis la version 6.2.1, les mappes standard et les mappes de transformation peuvent être compilées séparément. Pour obtenir des informations détaillées sur un standard EDI donné, veuillez consulter les manuels appropriés. Pour plus d'informations sur le client Data Interchange Services, reportez-vous au *Guide de mappage de WebSphere Partner Gateway* ou à l'aide en ligne fournie avec le client Data Interchange Services.

Remarque : Les ID de l'émetteur et du récepteur doivent figurer dans la définition du document ROD associée à la mappe de transformation. Les informations nécessaires à l'identification du type du document et des valeurs du dictionnaire doivent également figurer dans la définition du document. Assurez-vous que le spécialiste de mappage client Data Interchange Services ait connaissance de ces exigences lors de la création de la mappe de transformation.

Vous pouvez créer des protocoles personnalisés pour définir exactement la structure d'un document. Pour des documents XML, vous pouvez définir un format XML, comme décrit dans «Traitement de documents XML personnalisés», à la page 163.

Type de document

Le document lui-même peut se présenter dans divers formats. Les types de documents fournis par le produit et les protocoles qui leur sont associés sont les suivants :

- Binary, qui peut être utilisé avec le protocole Binary.
- ISA, qui représente l'EDI X12 (l'enveloppe) et qui est associé au protocole EDI-X12
- BG, qui représente l'enveloppe EDI Consent et qui est associé au protocole EDI-Consent
- UNB, qui représente l'enveloppe EDIFACT et qui est associé au protocole EDI-EDIFACT
- XMLEvent, qui peut être utilisé avec le protocole XMLEvent.

La liste suivante décrit les autres types de documents et la source de leur définition :

- Un PIP RosettaNet (téléchargé depuis le support d'installation), utilisable avec le protocole RosettaNet
- Un Service Web (que vous téléchargez en tant que fichier WSDL), qui peut être utilisé avec le protocole de Service Web.
- Un document cXML (que vous créez en précisant le type de document cXML)
- Une transaction EDI standard donnée, importée depuis le client Data Interchange Services.
- Un document ROD (Record-Oriented Data) ou XML, importé depuis le client Data Interchange Services.

Vous pouvez également créer vos propres types de documents, en suivant la procédure décrite dans «Traitement de documents XML personnalisés», à la page 163.

Présentation du traitement des documents

Avant d'entreprendre la configuration du concentrateur, il est judicieux de passer en revue les composants de WebSphere Partner Gateway et d'examiner la façon dont ils sont utilisés pour traiter les documents.

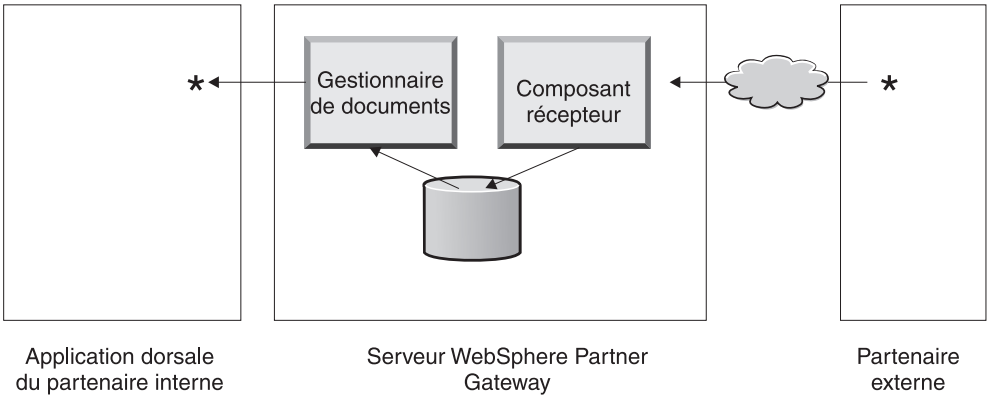


Figure 5. Composants du récepteur et du gestionnaire de documents

La figure 5 montre comment un document est envoyé par un partenaire, reçu et traité par le concentrateur, puis envoyé à une application dorsale du partenaire interne.

Remarque : Pour plus de clarté, le schéma montre un composant Récepteur et un gestionnaire de documents qui sont installés sur le même serveur (le troisième composant n'est pas représenté, il s'agit de la console qui assure l'interface avec WebSphere Partner Gateway). En fait, il est possible d'avoir plusieurs occurrences de ces composants, installées sur différents serveurs. Tous les composants doivent utiliser le même système de fichiers. Pour plus d'informations sur les différentes topologies disponibles pour configurer WebSphere Partner Gateway, reportez-vous au *Guide d'installation de WebSphere Partner Gateway*.

Un document est reçu dans WebSphere Partner Gateway par le composant Récepteur. Ce composant est chargé de surveiller le transport des documents entrants, de récupérer les documents qui arrivent, d'effectuer des opérations de base sur eux et de les placer dans une file d'attente où le gestionnaire de documents peut les extraire.

Les instances de récepteurs sont spécifiques au transport. Vous devez définir un récepteur pour chaque type de transport que le concentrateur devra gérer. Par exemple, s'il est prévu que des partenaires envoient des documents via HTTP, vous devez définir un récepteur HTTP pour pouvoir les réceptionner.

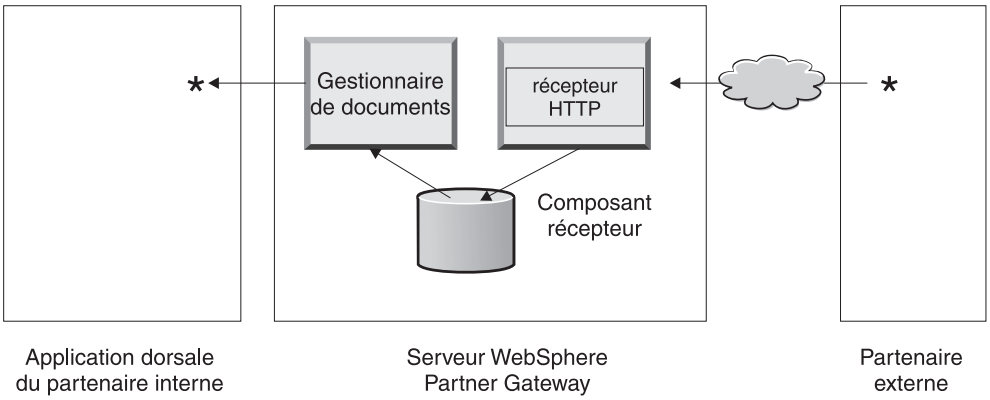


Figure 6. Un récepteur HTTP

Si l'application dorsale du partenaire interne doit envoyer des documents via le JMS, vous devez définir un récepteur JMS au niveau du concentrateur pour les réceptionner.

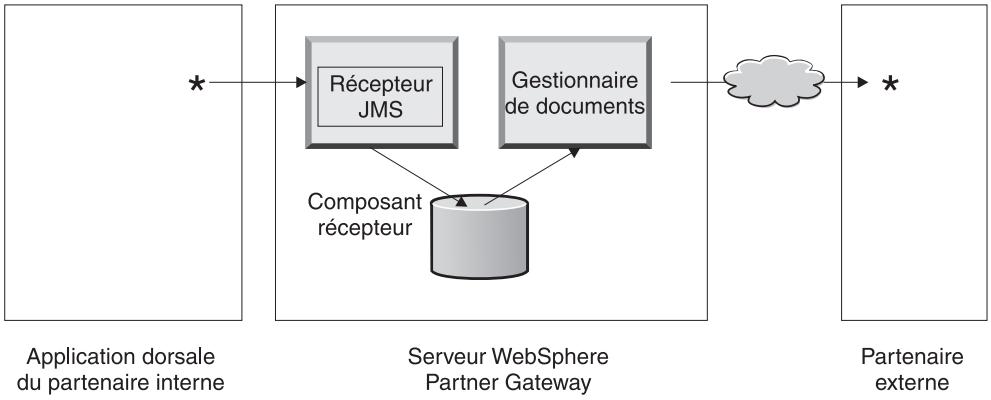


Figure 7. Récepteur JMS

Comme décrit dans «Présentation des transports», à la page 6, WebSphere Partner Gateway Connect prend en charge divers modes de transports, mais vous pouvez télécharger un mode de transport défini par l'utilisateur et l'utiliser pour définir un récepteur (voir procédure dans « Configuration d'un récepteur pour un transport défini par l'utilisateur», à la page 79).

Le composant Récepteur envoie le document à un système de fichiers partagé. Lorsque plusieurs documents sont réunis dans un seul fichier (par exemple, des documents XML ou ROD ou des EDI envoyés ensemble), le récepteur fractionne les documents ou EDI avant de les envoyer au système de fichiers partagé. Le composant Gestionnaire de documents récupère le document auprès du système de fichiers, analyse les informations d'acheminement et détermine s'il convient de procéder à une conversion.

Par exemple, le partenaire interne peut envoyer un document EDI-X12 avec empaquetage None au concentrateur, pour être livré à un partenaire qui attend un document EDI-X12 avec un empaquetage AS2. Le partenaire fournit l'URL HTTP où le document empaqueté AS2 doit être envoyé et le gestionnaire de documents empaquette le document conformément aux attentes du partenaire. Pour envoyer le document au partenaire, le gestionnaire de documents utilise la configuration de la destination de ce partenaire (qui doit avoir été définie avec l'URL HTTP où le partenaire attend des documents AS2).

Configuration des composants de traitement des documents à l'aide de gestionnaires

Cette section décrit plus en détail les composants de WebSphere Partner Gateway et indique les divers points auxquels vous pouvez (ou devez) modifier le comportement fourni par le produit des composants pour le traitement d'un document métier.

Vous utilisez les *gestionnaires* pour modifier le comportement produit des récepteurs, destinations, étapes de flux de travaux fixes et actions. Il existe deux types de gestionnaires -- ceux fournis par WebSphere Partner Gateway et ceux définis par l'utilisateur. Pour plus d'informations sur la création de gestionnaires, reportez-vous au *Guide du programmeur de WebSphere Partner Gateway*.

Une fois qu'un gestionnaire est créé, téléchargez-le pour le rendre disponible. Ne téléchargez que les gestionnaires définis par l'utilisateur. Les gestionnaires fournis par WebSphere Partner Gateway sont déjà disponibles.

Les sections suivantes décrivent les étapes du processus où vous pouvez spécifier des gestionnaires.

Récepteurs

Les récepteurs disposent de trois *points de configuration* pour lesquels des gestionnaires peuvent être spécifiés : Preprocess, SyncCheck et Postprocess.

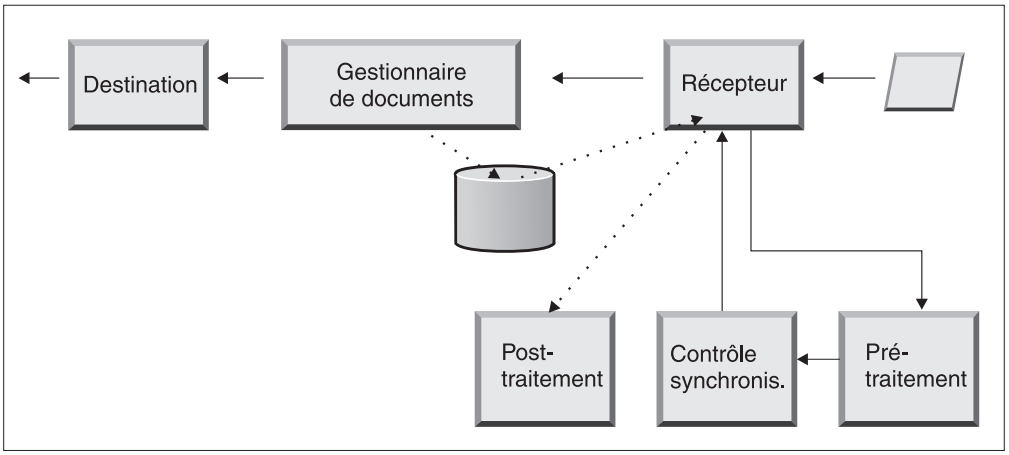


Figure 8. Points de configuration du récepteur

La procédure s'exécute dans l'ordre suivant :

1. Une fois qu'il a reçu le document, le composant Récepteur appelle les étapes Preprocess et SyncCheck.
2. Il appelle ensuite le gestionnaire de documents pour traiter le document.
3. Dans le cas de flux synchrones, le gestionnaire de documents apporte une Réponse synchrone. Le composant récepteur appelle ensuite l'étape Postprocess avec la réponse retournée par le gestionnaire de documents.

Les procédures sont décrites dans les sections suivantes :

- preprocess

  L'étape Preprocess est généralement utilisée pour tout traitement qui doit être effectué avant que le document ne soit traité par le gestionnaire de documents. Par exemple, si vous prévoyez de recevoir plusieurs documents ROD dans un seul fichier, configurez le gestionnaire de fractionnement ROD lorsque vous définissez le récepteur. L'utilitaire de fractionnement ROD, ainsi que deux autres utilitaires de fractionnement fournis par le système vous sont proposés pour définir un récepteur. Si vous créez d'autres gestionnaires pour l'étape preprocess, ils sont également disponibles.

  Voir « Preprocess», à la page 80 pour obtenir des informations sur le paramétrage du point de configuration Preprocess.

- SyncCheck

  SyncCheck sert à déterminer si WebSphere Partner Gateway doit traiter le document de manière synchrone ou asynchrone. Par exemple, dans le cas de documents AS2 reçus via HTTP, il définit s'il faut retourner une MDN (notification de disposition de message) de manière synchrone par la même

connexion HTTP. WebSphere Partner Gateway propose plusieurs gestionnaires pour le contrôle synchrone. Leur liste dépend du transport associé au récepteur.

SyncCheck s'applique uniquement aux transports (tels que HTTP, HTTPS et JMS) qui prennent en charge la transmission synchrone.

Remarque : Pour les documents AS2, cXML, RNIF ou SOAP qui seront utilisés dans les échanges synchrones, vous devez spécifier le gestionnaire SyncCheck associé sur le récepteur HTTP ou HTTPS.

Voir « SyncCheck», à la page 85 pour obtenir des informations sur le paramétrage du point de configuration SyncCheck.

- Postprocess

  Le Postprocess sert à traiter le document de réponse qui est envoyé par le concentrateur comme résultat d'une transaction synchrone.

  Voir « Postprocess», à la page 86 pour obtenir des informations sur le paramétrage du point de configuration Postprocess.

Gestionnaire de documents

Les documents reçus par les récepteurs sont récupérés par le gestionnaire de documents dans le système de fichiers commun, pour être traités. Le gestionnaire de documents utilise les connexions du partenaire pour router les documents. Tous les documents qui transitent par le gestionnaire de documents suivent plusieurs flux de travaux : flux de travaux fixe de communication entrante, flux de travaux variable et flux de travaux fixe de communication sortante. A la fin de ce dernier flux, la connexion avec le partenaire est déterminée. La connexion avec le partenaire indique l'action à effectuer sur ce document. Après avoir effectué le flux de travaux variable, le gestionnaire de documents traite le flux de travaux fixe de communication sortante sur ce document.

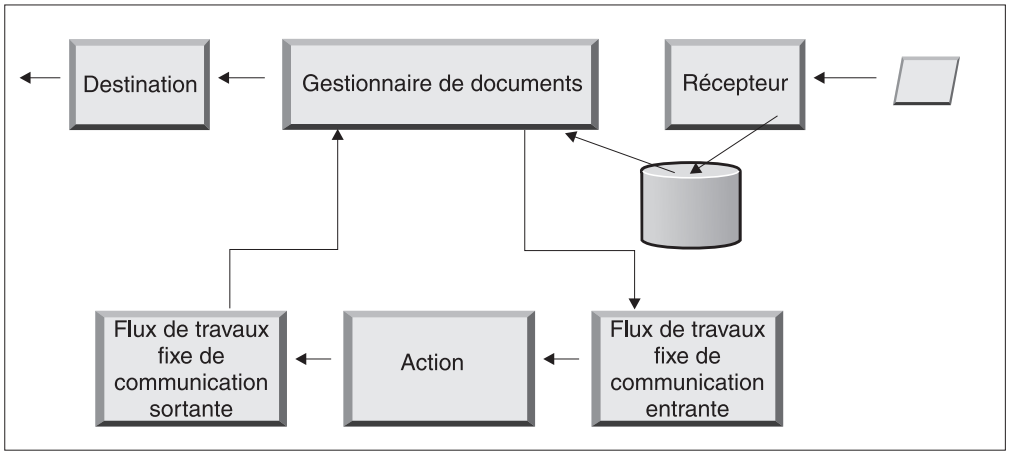


Figure 9. Flux de travaux fixe et actions

La figure 9 montre le cheminement d'un PIP RosettaNet ou d'un service Web. Certains documents exigent néanmoins plusieurs flux configurés. Par exemple, un EDI peut consister en plusieurs transactions. Le premier flux utilise une action pour désenvelopper l'ensemble des transactions individuelles. Chacune de ces transactions est réintroduite et traitée dans son propre flux configuré.

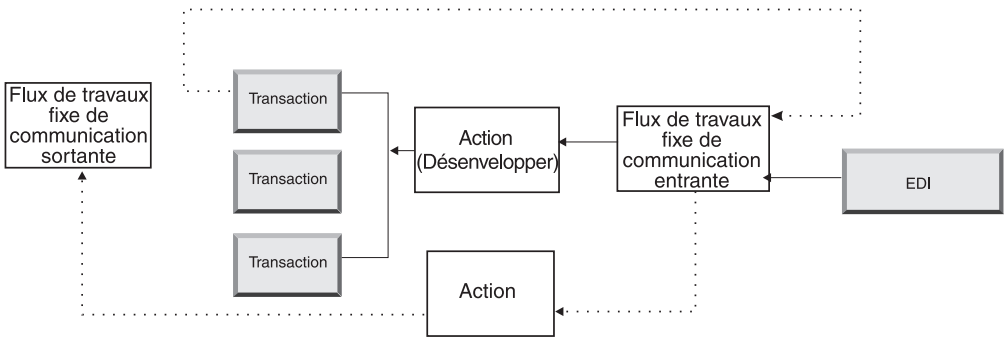


Figure 10. Flux de travaux fixe et actions pour un EDI

Flux de travaux fixe de communication entrante

Le flux de travaux fixe de communication entrante consiste en un ensemble standard d'étapes de traitement, exécutées sur tous les documents émis par un récepteur et reçus par le gestionnaire de documents. Le flux de travaux est fixe car le nombre et le types des étapes sont toujours les mêmes. Toutefois, au moyen d'exits utilisateurs, vous pouvez fournir des gestionnaires personnalisés pour le dégroupement et le traitement de protocole. La dernière étape du flux de travaux fixe de communication entrante consiste à rechercher la connexion du partenaire, qui détermine le flux de travaux variable qui s'exécute pour ce document métier.

Par exemple, si un message AS2 est reçu, il est décrypté, l'ID entreprise de l'expéditeur et du récepteur sont extraits. La procédure de flux de travaux fixe de communication entrante convertit le document AS2 en texte en clair pour les traitements suivants par WebSphere Partner Gateway et extrait les informations de sorte que l'action pour le message puisse être déterminée.

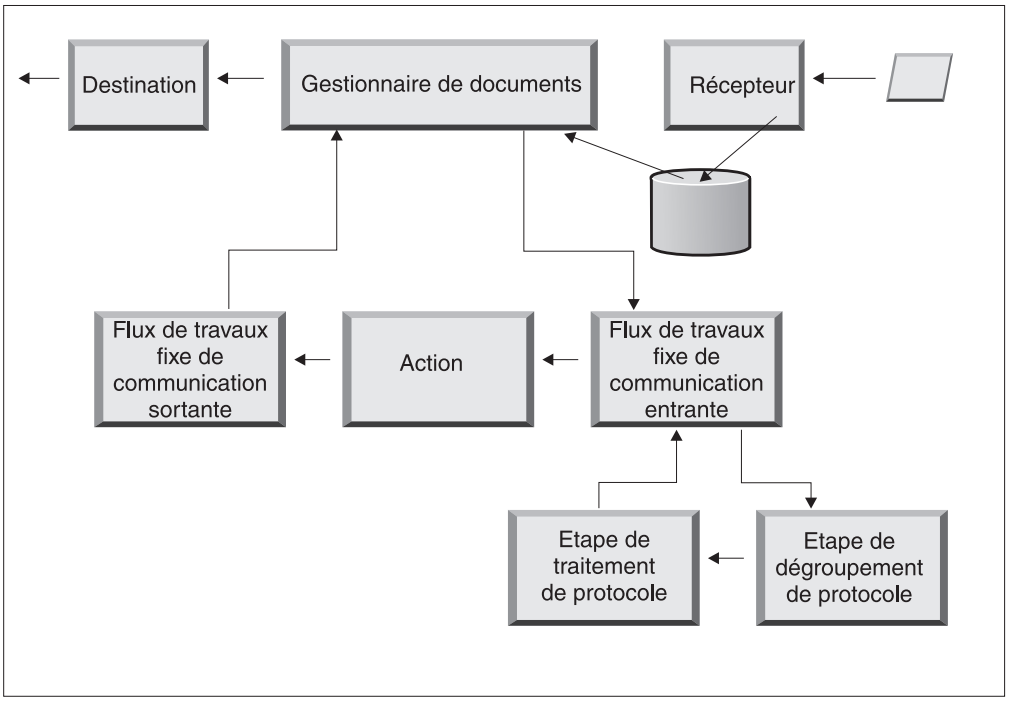


Figure 11. Flux de travaux fixe de la communication entrante

Dégroupement de protocole : Le Dégroupement de protocole consiste à dégrouper un document pour que son traitement puisse se poursuivre. Ce processus peut inclure le déchiffrement, la décompression, la vérification de signature, l'extraction d'informations d'acheminement, l'authentification utilisateur ou l'extraction de parties de documents métiers.

WebSphere Partner Gateway fournit des gestionnaires pour les packages RNIF, AS, Backend Integration et None. Si des gestionnaires d'autres protocoles sont nécessaires, vous pouvez les développer en tant qu'exits utilisateur. Pour plus d'informations sur la programmation d'exits utilisateur, reportez-vous au *Guide du programmeur de WebSphere Partner Gateway*.

Vous ne pouvez pas modifier l'étape de Dégroupement de protocole. Toutefois, vous pouvez lui ajouter une logique métier à l'aide de gestionnaires.

Voir «Configuration des flux de travaux fixes», à la page 90 pour obtenir des informations sur la configuration de cette étape.

Etape de traitement de protocole : Le traitement de protocole implique de déterminer des informations spécifiques au protocole, pouvant aller jusqu'à l'analyse syntaxique du message pour obtenir des informations sur le routage (telles que ID de l'émetteur et du récepteur), sur le protocole et le type de documents. WebSphere Partner Gateway peut traiter plusieurs protocoles, comme indiqué dans « Gestionnaires de traitement de protocole», à la page 91. Le traitement pour d'autres protocoles, par exemple CSV (valeurs séparées par des virgules), peut être assuré grâce à un exit utilisateur.

Vous ne pouvez pas modifier l'étape de Dégroupement de protocole. Toutefois, vous pouvez lui procurer une logique métier en ajoutant des gestionnaires.

Voir «Configuration des flux de travaux fixes», à la page 90 pour obtenir des informations sur la configuration de cette étape.

Vous pouvez utiliser le gestionnaire par défaut qui s'applique au protocole de votre document ou vous pouvez indiquer un autre gestionnaire pour les étapes de flux de travaux fixe de Dégroupement et traitement de protocole.

Actions

L'étape suivante dans la séquence de traitement dépend des actions définies pour l'échange de documents. Les actions sont constituées d'un nombre variable d'étapes qui peuvent être exécutées sur le document. La validation d'un document (pour le rendre conforme à un ensemble de règles déterminé) et sa conversion au format exigé par le destinataire sont autant d'exemples d'action.

Si le document n'est soumis à aucune étape spécifique, il peut utiliser l'action passe-système fournie par le produit, qui n'applique aucune modification au document.

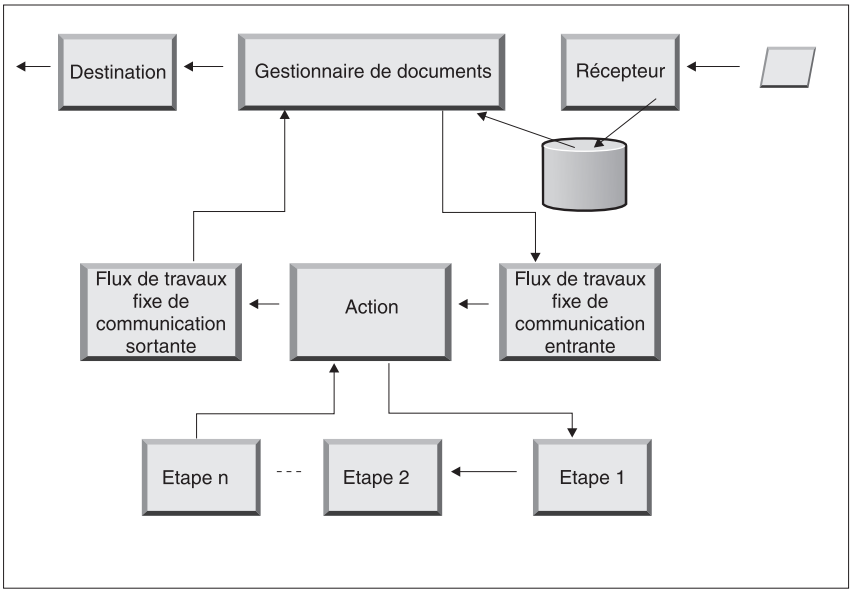


Figure 12. Etapes d'une action

Vous ne pouvez pas modifier une action fournie par le produit. Vous pouvez toutefois créer une action (et ajouter des gestionnaires à la liste des éléments configurés) ou copier une action fournie par le produit puis modifier la liste des gestionnaires.

Consultez «Configuration des actions», à la page 92 pour plus d'informations sur la création ou la copie d'une action fournie par le produit, ainsi que sur la configuration d'une action définie par l'utilisateur.

Concepts associés

«Configuration des actions», à la page 92

Flux de travaux fixe de communication sortante

Le flux de travaux fixe de la communication sortante consiste en une seule étape, l'empaquetage du document et des informations de protocole correspondantes. Par exemple, si ce document a été configuré dans le but d'être reçu par une application dorsale utilisant un package Backend Integration, certaines informations d'en-tête sont ajoutées au document avant qu'il ne soit transmis à la destination.

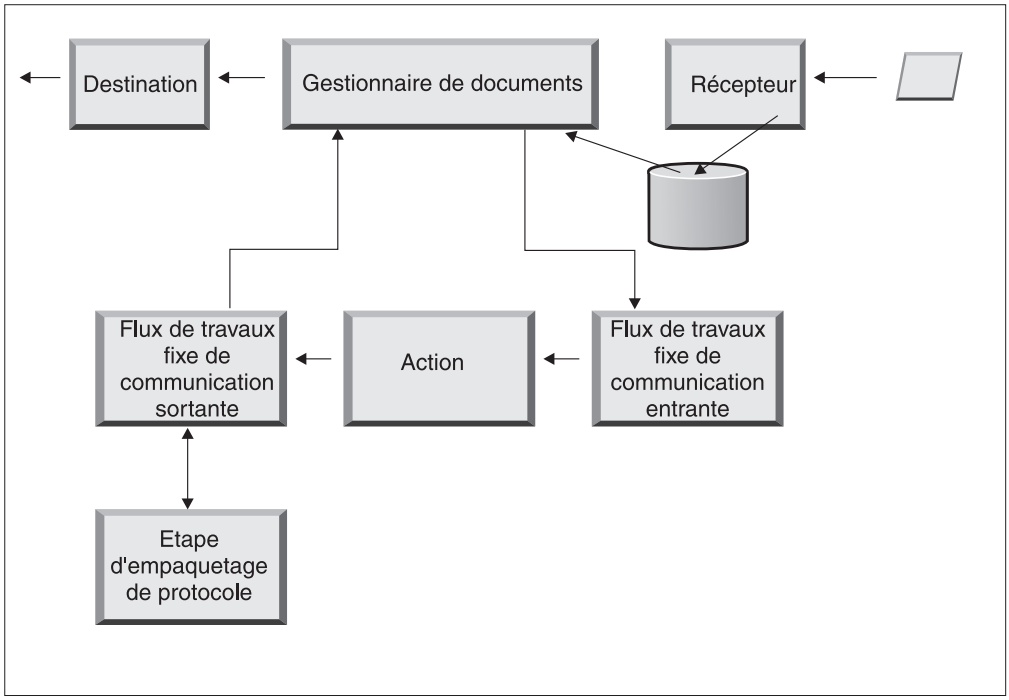


Figure 13. Flux de travaux fixe de la communication sortante

WebSphere Partner Gateway fournit des gestionnaires adaptés à divers packages et protocoles, indiqués dans «Flux de travaux de communication sortante», à la page 92. Si d'autres gestionnaires d'empaquetage sont nécessaires, vous pouvez les développer en tant qu'exit utilisateur. En général, ces étapes prennent en charge un ou plusieurs des processus suivants :

- Assemblage ou enveloppement
- Chiffrement
- Signature
- Compression
- Définition des en-têtes de transport spécifique au protocole métier

Vous ne pouvez pas modifier l'étape d'empaquetage de protocole. Toutefois, vous pouvez lui ajouter une logique métier à l'aide de gestionnaires.

Voir «Configuration des flux de travaux fixes», à la page 90 pour obtenir des informations sur la configuration de cette étape du flux de travaux.

Destinations

Les destinations sont configurées dans la console pour chaque partenaire auquel vous devez envoyer des messages. La configuration d'une destination comprend le transport qui sera utilisé pour envoyer des messages ainsi que la configuration nécessaire pour l'envoyer, telle que l'URL pour le processus de réponse du partenaire.

Après avoir quitté le gestionnaire de documents, le document est envoyé au destinataire prévu à l'aide d'une destination. La destination dispose de deux points de configuration — Preprocess et Postprocess.

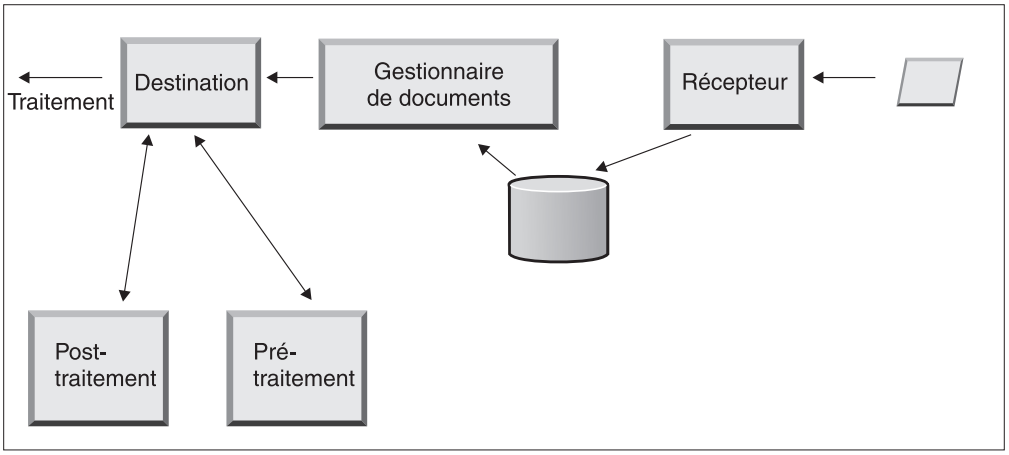


Figure 14. Points de configuration de la destination

- preprocess

  Preprocess intervient dans le traitement d'un document avant qu'il ne soit envoyé au récepteur (le Process est l'envoi réel du document). Aucun gestionnaire n'est fourni par le système pour configurer l'étape Preprocess. Toutefois, vous pouvez télécharger un gestionnaire défini par l'utilisateur.
- Postprocess

  Postprocess agit sur les résultats de la transmission du document (par exemple, sur la réponse reçue du destinataire lors d'une transmission synchrone). Aucun gestionnaire n'est fourni par le système pour configurer l'étape Postprocess. Toutefois, vous pouvez télécharger un gestionnaire défini par l'utilisateur.

Voir «Configuration de gestionnaires», à la page 250 pour obtenir des informations sur le paramétrage des étapes Preprocess et Postprocess.

Vue générale de la configuration du concentrateur

Une fois que vous avez analysé les besoins de votre activité, en appliquant la procédure décrite dans «Informations nécessaires à la configuration du concentrateur», à la page 6, configurez le concentrateur et créez vos profils de partenaires. La présente section apporte des informations précises sur les tâches à effectuer.

Remarque : Lorsque vous configurez le concentrateur,reportez-vous au *Guide d'administration de WebSphere Partner Gateway* pour obtenir des informations sur les codes d'événements et des conseils de dépannage.

Configuration du concentrateur

Pourquoi et quand exécuter cette tâche

En tant qu'administrateur du concentrateur, vous devez réaliser les tâches suivantes pour le configurer :

1. Procédez à toute configuration préliminaire (si nécessaire) pour les transports utilisés. Cette procédure est décrite au Chapitre 4, «Etapes préalables à la configuration du concentrateur», à la page 35.

2. Si vous le souhaitez, vous pouvez personnaliser la console et modifier le mot de passe par défaut ainsi que les règles de droits d'accès. Ces tâches sont décrites au Chapitre 6, «Configuration de la console de communauté», à la page 53.
3. Créez des récepteurs pour les types de transports qui seront utilisés pour recevoir les documents sur le concentrateur (émis par le partenaire interne et des partenaires externes). La création des récepteurs est décrite au Chapitre 7, «Définition des récepteurs», à la page 61.

   Remarque : Si vous prévoyez de configurer le récepteur avec des gestionnaires définis par l'utilisateur, vous devez les télécharger avant de créer le récepteur. Cette procédure est décrite dans « Téléchargement de gestionnaires définis par l'utilisateur», à la page 62.
4. Configurez les étapes ou actions de flux de travaux de communication entrante. Cette étape est *facultative* et nécessaire qu'en cas d'exigences spécifiques de traitement de documents, non assurées par WebSphere Partner Gateway. Si vous n'avez pas besoin de modifier le comportement des flux de travaux et actions fournis par le produit, n'effectuez pas cette étape. Cette procédure est décrite au Chapitre 8, «Configuration des procédures et actions portant sur les flux de travaux fixes», à la page 89.

   Remarque : Vous devez télécharger les gestionnaires définis par l'utilisateur avant de configurer les flux de travaux et actions. Cette procédure est décrite dans « Téléchargement de gestionnaires», à la page 89.
5. Créez des définitions de documents (ou vérifiez que ceux dont vous avez besoin sont déjà disponibles) pour définir les types de documents que vous pouvez envoyer ou recevoir au niveau du concentrateur.
6. Créez des interactions pour indiquer la combinaison valide de deux définitions de documents.

   La création de définitions de documents et la création d'interactions sont décrites dans le Chapitre 9, «Configuration des types de documents», à la page 111 et le Chapitre 10, «Configuration des flux de documents EDI», à la page 179.
7. Créez un profil pour le partenaire interne, en fournissant des informations le concernant et en déterminant les types de documents qu'il peut envoyer et recevoir (ses fonctions business-to-business). La création du profil est décrite au Chapitre 3, «Création et configuration de partenaires», à la page 25.

Création des partenaires

Une fois que vous avez configuré le concentrateur, créez un profil pour chaque partenaire externe qui échangera des documents avec le partenaire interne. Seul l'administrateur du concentrateur peut créer des partenaires.

En tant qu'administrateur du concentrateur, vous pouvez également paramétrer les fonctions business-to-business des partenaires, établir leurs destinations et configurer leurs profils de sécurité. Ces procédures peuvent être réalisées par les partenaires eux-mêmes.

La création des partenaires est décrite dans Chapitre 3, «Création et configuration de partenaires», à la page 25. La création des destinations est décrite au Chapitre 11, «Création de destinations», à la page 229. Cette procédure est décrite au Chapitre 13, «Activation de la sécurité pour les échanges de documents», à la page 257.

Etablissement de connexions de documents

Une fois que vous avez configuré le concentrateur et créé des profils de partenaires, vous pouvez paramétrer des connexions. Les connexions indiquent les combinaisons valides d'émetteurs et récepteurs ainsi que les documents qu'ils peuvent échanger. Cette procédure est décrite au Chapitre 12, «Gestion des connexions», à la page 253.

Présentation des certificats OpenPGP

OpenPGP est pris en charge dans WebSphere Partner Gateway. Ce protocole utilise une combinaison de clé publique solide et de cryptographie symétrique pour fournir des fonctions de sécurité. Les diverses fonctions d'OpenPGP incluses dans cette édition sont les suivantes :

- Messages mis en forme conformément à RFC 4880.

  Remarque : RFC 2440 et RFC 3156 ne sont pas pris en charge dans cette édition.
- Chiffrement, chiffrement avec détection des modifications et compression.

  Remarque : Dans cette édition, WebSphere Partner Gateway ne prend pas en charge la signature avec OpenPGP.
- Les algorithmes de chiffrement pris en charge sont CAST5 (clé 128 bits), TripleDES (clé 168 bits), Blowfish (clé 128 bits), Twofish (clé 256 bits), AES (clés 128, 192 et 256 bits).

  Remarque : Twofish, TripleDES et AES (clés 192 et 256 bits) requièrent des fichiers de règles de juridiction de cryptographie sans limite.
- Les algorithmes de compression pris en charge sont ZIP, ZLIB et BZip2.
- Messages ASCII Armor.
- La fonction de migration de partenaire et de conformité à la norme FIPS a été modifiée pour prendre en charge OpenPGP.
- La gestion partielle de documents n'est pas prise en charge dans OpenPGP.

Certains produits prérequis doivent être exécutés avant d'utiliser des certificats OpenPGP.

Obtenez de manière externe les fichiers de bibliothèque suivants et copiez-les dans le dossier EMPLACEMENT D'INSTALLATION DU CONCENTRATEUR>/lib/openpgp :

- BouncyCastle OpenPGP library ver. 1.45 for JDK 1.5
- BouncyCastle JCE library ver. 1.45 for JDK 1.5

  Important : Obtenez ou procurez-vous ces fichiers de bibliothèque de façon externe, car IBM ne les fournit pas. Pour plus d'informations sur l'obtention des fichiers de bibliothèque, voir le lien de la page d'accueil de Bouncy castle - http://www.bouncycastle.org. Les fichiers jar à extraire sont http://www.bouncycastle.org/download/bcpg-jdk15-145.jar et http://www.bouncycastle.org/download/bcprov-jdk15-145.jar. Pour le mode réparti, placez les fichiers jar sur tous les ordinateurs sur lesquels le gestionnaire de documents et la console sont installés.

Après avoir copié les fichiers dans l'emplacement indiqué, redémarrez le serveur.

Chapitre 3. Création et configuration de partenaires

Il existe deux types de partenaires : les partenaires internes et les partenaires externes. Le partenaire interne est généralement l'entreprise qui est propriétaire du serveur WebSphere Partner Gateway et qui l'utilise pour communiquer avec les autres entreprises. Le partenaire interne possède les applications dorsales (applications internes à l'entreprise propriétaire). Le nombre de partenaires internes n'est pas défini mais le partenaire par défaut est généralement le premier partenaire défini. Les autres entreprises avec lesquelles le partenaire interne communique sont les partenaires externes.

Pour chaque partenaire avec lequel vous échangez des documents, vous devrez créer un profil de partenaire. Parallèlement à la création de profils, vous devrez également les paramétrer, un processus qui comprend plusieurs étapes facultatives et obligatoires.

Ce chapitre présente les étapes de base de la création et de la configuration d'un profil de partenaire. Pour des informations plus détaillées sur une étape, consultez la référence à la fin de cette étape ou section pour plus d'informations. Ce chapitre contient les sections suivantes :

Remarque : Pour effectuer des modifications de configurations sur WebSphere Partner Gateway, vous devez toujours utiliser la même instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Création des profils des partenaires

Pourquoi et quand exécuter cette tâche

Il s'agit de la première étape dans la définition d'un partenaire dans WebSphere Partner Gateway. Cette étape définit les informations de base concernant le partenaire, telles que son nom, son nom de connexion et des ID entreprise.

Pour créer un partenaire, vous devez connaître les informations suivantes concernant le partenaire :

- Le ID entreprise que le partenaire utilise. Il peut prendre la forme de :
  - un numéro DUNS, qui est le numéro Dun & Bradstreet standard associé à une société ;
  - un numéro DUNS+4, qui est une version étendue du numéro DUNS ;

– Un numéro à format libre qui peut consister en tout numéro que le partenaire choisit d'utiliser pour identifier l'entreprise

Pour chaque partenaire que vous voulez ajouter à la communauté du concentrateur, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Créer**.
3. Entrez le **Nom de l'entreprise**. Il s'agit du nom que le partenaire utilisera dans la zone entreprise lorsqu'il se connectera au concentrateur. Les espaces vides ne sont pas autorisés dans le nom de l'entreprise.
4. Pour **Nom affiché du partenaire**, entrez le nom de l'entreprise ou tout autre nom descriptif pour le partenaire. Il s'agit du nom affiché dans la liste **Recherche du partenaire**.
5. Sélectionnez le type du partenaire. S'il s'agit du premier partenaire, vous configurerez probablement l'entreprise qui possède WebSphere Partner Gateway. Vous devez donc sélectionner **Partenaire interne**. Sur l'écran de configuration du partenaire, cochez **Partenaire interne par défaut** si vous souhaitez définir ce partenaire actuel comme partenaire par défaut. Lorsque vous sélectionnez un autre partenaire, la sélection par défaut de ce partenaire interne est automatiquement supprimée. Vous ne pouvez pas supprimer la sélection sur cette page. Pour le premier partenaire interne qui est créé, cette case est cochée par défaut.
6. Entrez éventuellement le nom d'utilisateur de l'administrateur pour l'administrateur. Le nom d'utilisateur de l'administrateur est unique pour tous les partenaires. L'administrateur du partenaire peut effectuer des activités de gestion pour ce partenaire, telles que la gestion des destinations, des fonctions business-to-business et des utilisateurs. L'opérateur du concentrateur bénéficie toujours d'un plein accès à la gestion du partenaire.
7. Sélectionnez le statut du partenaire. Sélectionnez **Activé** si le statut ou le partenaire est désactivé. **Activé** est le statut par défaut du partenaire.
8. Indiquez éventuellement le type de l'entreprise dans la zone **Fournisseur**.
9. Entrez éventuellement le **Site Web** du partenaire.
10. Cliquez sur **ID entreprise** > **Nouveau**.
11. Indiquez un type dans la liste, puis entrez l'identificateur approprié. WebSphere Partner Gateway se base sur le numéro que vous indiquez ici pour acheminer le document depuis et vers le partenaire.

    Veillez à respecter les recommandations suivantes lors de la saisie de l'identificateur :

    a. Les numéros DUNS se composent de neuf chiffres.
    b. Les numéros DUNS+4 se composent de 13 chiffres.
    c. Les numéros d'identification à format libre acceptent jusqu'à 60 caractères alphanumériques et spéciaux.

    Remarque : Vous pouvez attribuer plusieurs ID entreprise à un partenaire. Dans certains cas, plusieurs ID entreprise sont requis. Par exemple, lorsque le concentrateur reçoit ou envoie des documents EDI ou EDIFACT, il utilise l'ID DUNS et l'ID à format libre (Freeform) au cours de l'échange de documents.

    Le partenaire interne et les partenaires externes impliqués dans ce type flux de documents doivent disposer d'un ID DUNS et d'un ID à format libre. L'ID à format libre sert pour représenter les ID d'EDI qui ont à la fois un identifiant et un qualificateur. Par exemple, si le qualificatif de l'EDI est "ZZ" et son

identifiant "810810810", l'ID à format libre pourra être ZZ-810810810. Lorsque vous cliquez sur **Nouveau**, la zone de saisie ID messagerie s'active également et s'affiche pour que vous puissiez créer un ID messagerie.

12. Cliquez sur **Nouveau** pour créer un nouvel ID messagerie et saisissez votre ID messagerie dans la zone Identificateur de messagerie. Vous pouvez aussi cliquer sur Nouveau pour créer plusieurs ID messagerie.
13. Entrez éventuellement une adresse IP pour le partenaire. L'adresse IP est utilisée en conjonction avec une destination lorsque "Valider l'IP client" est configuré. Saisissez une adresse IP en procédant comme suit :
    a. Sous **Adresse IP**, cliquez sur **Nouveau**.
    b. Spécifiez le mode d'Opération.
    c. Saisissez l'adresse IP du partenaire.
14. Cliquez sur **Sauvegarder**.
15. Si vous avez saisi un nom d'utilisateur de l'administrateur, vous obtiendrez un mot de passe qui sera utilisé par le partenaire pour se connecter au concentrateur. Notez-le. Vous l'indiquerez à l'utilisateur d'administration du partenaire.

Création de destinations

Pourquoi et quand exécuter cette tâche

Lorsque vous avez créé un profil pour un partenaire, établissez les destinations qui seront utilisées par le concentrateur pour envoyer des documents au partenaire.

Suivez la procédure ci-dessous pour créer des destinations pour un partenaire :

1. Veillez à ce que le profil du partenaire pour lequel vous voulez créer des destinations soit sélectionné.

   Si vous venez de créer un profil, il est déjà sélectionné. S'il n'est pas sélectionné, suivez les étapes ci-après :
   a. Cliquez sur **Administrateur du compte** > **Profils** > **Partenaire**.
   b. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
   c. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
2. Cliquez sur **Destinations**.
3. Cliquez sur **Créer**.
4. Entrez un **Nom de destination** pour identifier la destination.
5. Indiquez éventuellement le **Statut** de la destination.
6. Indiquez éventuellement si la destination est **En ligne** ou **Hors ligne**.
7. Entrez éventuellement une **Description** de la destination.
8. Sélectionnez un **Transport**.
9. Après avoir sélectionné un transport, la section **Configuration de la destination** de cette page spécifique à ce transport s'affiche. Pour des informations sur le renseignement de cette section pour chaque transport, consultez l'une des sections suivantes :
   - «Définition des valeurs de transport globales», à la page 231

     Remarque : Ces valeurs concernent uniquement la destination de script FTP.
   - «Configuration d'une destination HTTP», à la page 232

- «Configuration d'une destination HTTPS», à la page 234
- «Configuration d'une destination FTP», à la page 236
- «Configuration d'une destination SMTP», à la page 237
- «Configuration d'une destination JMS», à la page 239
- «Configuration d'une destination fichier-répertoire», à la page 241
- «Configuration d'une destination FTPS», à la page 242
- «Configuration d'une destination de script FTP», à la page 245
- «Configuration d'une destination SFTP», à la page 244

Configuration des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

Chaque partenaire a des Fonctions business-to-business qui définissent les types de documents que le partenaire peut envoyer et recevoir.

En tant qu'administrateur du concentrateur, vous pouvez définir les fonctions business-to-business de vos partenaires. Vous pouvez également leur laisser le soin d'effectuer cette opération. Fonctions business-to-business permet d'associer les fonctions business-to-business d'un partenaire à une définition de documents.

Pour définir les fonctions business-to-business de chaque partenaire, procédez comme suit :

1. Veillez à ce que le profil du partenaire pour lequel vous voulez configurer les fonctions business-to-business soit sélectionné. Le profil sélectionné s'affiche en haut de la page après **Profil**.

   Si vous venez de créer un profil, il est déjà sélectionné. S'il n'est pas sélectionné, suivez les étapes ci-après pour le faire :

   a. Cliquez sur **Administrateur du compte**.
   b. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
   c. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
2. Cliquez sur **Fonctions B2B**. La page des fonctions business-to-business s'affiche. Dans la partie de droite apparaissent les packages, les protocoles et les types de documents pris en charge par le système en tant que définitions de documents.
3. Cliquez sur l'icône **Rôle inactif** dans la colonne **Définir source** pour les packages. Le package contient des documents que les partenaires externes enverront au partenaire interne.
4. Si les partenaires vont envoyer et recevoir ces mêmes documents, sélectionnez à la fois **Définition de la source** et **Définition de la cible**. La console de communauté indique par une coche que la définition de documents est activée.

   Remarque : La sélection de la Définition de la source sera la même pour toutes les actions d'un processus PIP bidirectionnel même si la requête provient d'un partenaire et la confirmation associée d'un autre. Cela vaut également pour la colonne Définition de la cible.
5. Cliquez sur l'icône **Développer** au niveau **Package** pour développer un noeud jusqu'au niveau Définition de documents approprié, ou sélectionnez un nombre de **0 à 4**, ou cliquez sur **Tous** pour développer toutes les définitions de documents affichées, jusqu'au niveau sélectionné.

6. Sélectionnez à nouveau **Définition de la source**, **Protocole** ou les deux rôles à la fois pour les niveaux inférieurs **Protocole** et **Type de documents**, pour chaque définition de documents prise en charge par votre système.

   Si une définition est activée au niveau **Type de documents**, les définitions **Action** et **Activité** (s'il en existe) seront activées automatiquement.
7. Cliquez éventuellement sur **Activé** sous la colonne **Activé** pour mettre une définition de documents hors ligne (lorsque vous sélectionnez **Définition de la source** ou **Définition de la cible**, l'enregistrement est automatiquement activé). Cliquez sur **Désactivé** pour la mettre en ligne.

   Si un package est désactivé, toutes les définitions de documents de niveau inférieur de ce même noeud sont également désactivées, même si leur état respectif était Activé. Si une définition de documents de niveau inférieur est désactivée, toutes les définitions de niveau supérieur appartenant au même contexte restent activées. Lorsqu'une définition de documents est désactivée, tous les connexions et attributs existants cessent de fonctionner.
8. Cliquez éventuellement sur l'icône **Edition** si vous souhaitez modifier l'un des attributs d'un protocole, d'un package, d'un type de documents, d'une action, d'une activité ou d'un signal. Vous pouvez alors consulter la configuration des attributs (s'ils existent). Vous pouvez modifier les attributs en entrant une valeur ou en sélectionnant une valeur dans la colonne **Mettre à jour** puis en cliquant sur **Sauvegarder**.

Chargement de certificats

Pourquoi et quand exécuter cette tâche

Les certificats permettent aux partenaires d'envoyer et de recevoir des documents à l'aide de plusieurs méthodes : chiffrement, signature numérique, ou SSL. Dès qu'un partenaire a reçu un certificat d'un autre partenaire, ce partenaire peut utiliser ces méthodes pour envoyer le document.

Utilisez les étapes indiquées dans «Téléchargement de certificats à l'aide de l'assistant», à la page 292 pour télécharger les certificats pour un partenaire.

Pour plus d'informations sur l'utilisation des certificats, voir Chapitre 13, «Activation de la sécurité pour les échanges de documents», à la page 257.

Création d'utilisateurs

Pourquoi et quand exécuter cette tâche

Les utilisateurs sont les personnes qui se connecteront pour effectuer des tâches d'administration pour ce partenaire. Les nouveaux utilisateurs qui sont ajoutés au serveur LDAP et à la console d'administration WAS doivent également être ajoutés dans la console WebSphere Partner Gateway pour être actifs.

Suivez la procédure ci-dessous pour créer des utilisateurs pour un partenaire :

1. Veillez à ce que le profil du partenaire pour lequel vous voulez créer des utilisateurs soit sélectionné. Le profil sélectionné s'affiche en haut de la page après **Profil >**. Si le Nom de profil n'est pas sélectionné, suivez les étapes ci-dessous pour créer un profil :
   a. Cliquez sur **Administrateur du compte > Profils > Partenaire**.

b. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
c. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.

2. Cliquez sur **Utilisateurs**.
3. Cliquez sur **Créer**.
4. Sélectionnez le nom de l'utilisateur.

   Remarque : Le nom d'utilisateur doit être unique pour chaque partenaire du système.
5. Attribuez au statut la valeur **Activé**.
6. Entrez éventuellement le nom donné, le nom de famille et autres informations personnelles de l'utilisateur.
7. Sélectionnez la **Langue**, les **Environnements de format** et le **Fuseau horaire** de l'utilisateur.
8. Faites passer le statut d'Alerte de l'utilisateur sur **Activé**.
9. Sélectionnez la visibilité souscrite de l'utilisateur.
10. Cliquez soit sur **Générer automatiquement un mot de passe** pour créer un mot de passe pour cet utilisateur ou saisissez en un et retapez-le.
11. Cliquez sur **Sauvegarder**.

Remarque :

1. Dans la mesure où des noms d'utilisateur uniques sont requis sur un serveur LDAP, les noms d'utilisateur doivent être uniques également sur WebSphere Partner Gateway. Si vous créez un nouvel utilisateur et que le nom d'utilisateur existe déjà, dans ce même partenaire ou pour un autre, un message d'erreur indiquant `Un utilisateur portant ce nom existe déjà` s'affichera.
2. Si vous migrez vers WebSphere Partner Gateway depuis une version antérieure dans laquelle les noms d'utilisateur n'étaient pas restreints, une double astérisque (**) s'affiche à côté de tout nom d'utilisateur en double, indiquant qu'il existe également dans le même profil partenaire ou dans un autre. Modifiez l'un des noms d'utilisateur afin qu'ils soient uniques. Les nouveaux utilisateurs et groupes, qui sont ajoutés au serveur LDAP et à la console d'administration WAS, doivent également être ajoutés dans la console WebSphere Partner Gateway pour être actifs.

Pour permettre à LDAP de fonctionner avec WebSphere Partner Gateway, vous devez définir une authentification de serveur LDAP à l'aide de la console WebSphere Application Server et de l'autorisation utilisateur LDAP à l'aide de la console WebSphere Partner Gateway Community. Pour plus d'informations sur la configuration de l'authentification LDAP, consultez le *Guide d'installation de WebSphere Partner Gateway*. Pour plus d'informations sur la gestion des utilisateurs et la configuration de l'autorisation d'utilisateur LDAP, voir le *Guide d'administration de WebSphere Partner Gateway*.

Pour plus d'informations sur la gestion des utilisateurs, voir "Gestion des utilisateurs" dans le *Guide du partenaire WebSphere Partner Gateway*.

Configuration FTP

Pour configurer un utilisateur FTP ou SFTP, utilisez une des deux procédures suivantes :

- «Création d'utilisateurs FTP et SFTP»Créer un utilisateur dans l'écran de gestion FTP de la console.
- «Activation d'utilisateurs existants pour FTP et SFTP», à la page 32

Création d'utilisateurs FTP et SFTP

Dans cette étape, lors de la création, les utilisateurs sont configurés comme des utilisateurs FTP ou comme des utilisateurs SFTP.

Pourquoi et quand exécuter cette tâche

Vous pouvez créer des utilisateurs FTP et SFTP dans la page **Gestion des utilisateurs FTP** de la console.

Procédure

1. Cliquez sur **Administrateur du compte > Gestion des utilisateurs FTP**.
2. Cliquez sur **Créer**.
3. Entrez les coordonnées de l'utilisateur et cliquez sur **Enregistrer**. Pour plus d'informations sur la création des utilisateurs, voir «Création d'utilisateurs», à la page 29. Les informations de l'utilisateur créé avec succès s'affichent en mode lecture seule.
4. Cliquez sur le lien **Configuration FTP**.
5. Dans l'écran Configuration FTP, sélectionnez `Activé` pour **Utilisateur FTP activé** ou pour **Utilisateur SFTP activé**. Vous pouvez activer un utilisateur à la fois pour les serveurs FTP et SFTP.
6. Entrez les caractéristiques suivantes de la configuration FTP :
   a. Entrez le **Répertoire de base**, qui est le chemin relatif de la valeur spécifiée pour bcg.ftp.config.rootdirectory.
   b. Activez ou désactivez les **Droits en écriture** du répertoire de base.
   c. Activez ou désactivez les droits de **Créer/Supprimer un répertoire**.
   d. Sélectionnez **Nombre max de connexions**. C'est le nombre maximum de fois que vous pouvez effectuer une connexion simultanée.
   e. Sélectionnez **Nb de connexions max. de la même adresse IP**. C'est le nombre maximum de fois que vous pouvez effectuer une connexion simultanée depuis la même adresse IP.
   f. Sélectionnez **Délai d'inactivité max. (secondes)**. C'est le temps maximal d'inactivité, en secondes, au bout duquel la connexion utilisateur est abandonnée.
   g. Sélectionnez **Maximum téléchargement vers l'amont (octets/sec)**. C'est le débit maximal de téléchargement vers l'amont en octets/sec.
   h. Sélectionnez **Maximum téléchargement vers l'aval (octets/sec)**. C'est le débit maximal de téléchargement vers l'aval en octets/sec.

   Remarque : Certaines zones ont une valeur `Limite personnalisée` dans la liste déroulante. Si vous sélectionnez `Limite personnalisée` dans la liste déroulante, entrez la valeur personnalisée dans la zone de saisie.

7. Pour la configuration SFTP, entrez **Clé (SFTP uniquement)**. Le fichier téléchargé est utilisé pour l'authentification par clé. L'icône du dossier indique qu'une clé est déjà téléchargée. Vous pouvez aussi utiliser **Parcourir** pour télécharger une clé.
8. Cliquez sur **Sauvegarder**.

Activation d'utilisateurs existants pour FTP et SFTP

Dans cette étape, vous pouvez définir un utilisateur existant comme un utilisateur FTP ou comme un utilisateur SFTP.

Pourquoi et quand exécuter cette tâche

Pour configurer un utilisateur FTP ou SFTP, activez les propriétés FTP ou SFTP pour un utilisateur existant.

Procédure

1. Cliquez sur **Administrateur du compte > Profils > Utilisateurs**.
2. Entrez les critères de recherche, puis cliquez sur **Rechercher**.
3. Dans les résultats de la recherche, si la colonne **Etat** est désactivée pour le contact, cliquez sur l'icône `Activé`. L'icône permet de basculer entre les états activer et désactiver.
4. Cliquez sur l'**icône Afficher les caractéristiques** pour l'utilisateur dont vous voulez configurer l'accès FTP.
5. Dans l'écran Détails de l'utilisateur, cliquez sur le **lien Configuration FTP.**
6. Dans l'écran **Configuration FTP**, sélectionnez `Activé` pour **Utilisateur FTP activé** ou pour **Utilisateur SFTP activé**. Un utilisateur peut être activé à la fois pour les serveurs FTP et SFTP.
7. Entrez les caractéristiques de la configuration FTP ou SFTP. Voir «Création d'utilisateurs FTP et SFTP», à la page 31 pour les détails d'un utilisateur FTP ou SFTP.
8. Cliquez sur **Sauvegarder**.

Création de groupes

Pourquoi et quand exécuter cette tâche

Le regroupement des utilisateurs vous permet de gérer les droits d'accès des nombreux utilisateurs de manière simultanée. Les nouveaux groupes qui sont ajoutés au serveur LDAP et à la console d'administration WebSphere Application Server doivent également être ajoutés dans la console WebSphere Partner Gateway pour être actifs.

Suivez la procédure ci-dessous pour créer des groupes pour chaque partenaire :

1. Veillez à ce que le profil du partenaire pour lequel vous voulez créer des groupes soit sélectionné.

   Si vous venez de créer un profil, il est déjà sélectionné. S'il n'est pas sélectionné, suivez les étapes ci-après pour le faire :

   a. Cliquez sur **Administrateur du compte** > **Profils** > **Partenaire**.
   b. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
   c. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.

2. Cliquez sur **Groupes**.
3. Cliquez sur **Créer**.
4. Sélectionnez le nom de ce groupe.
5. Cliquez sur **Sauvegarder**.
6. Pour ajouter des utilisateurs à ce groupe, cliquez sur le lien **Appartenance**.

   Les utilisateurs associés à ce partenaire sont affichés sous **Utilisateurs hors du groupe** ou **Utilisateurs dans le groupe**. Pour ajouter un utilisateur à un groupe, procédez comme suit,

   a. Cliquez sur l'icône **Modifier l'enregistrement** à côté du groupe.
   b. Sélectionnez l'utilisateur que vous voulez ajouter et cliquez sur **Ajouter au groupe**.
   c. Cliquez sur **Sauvegarder**.
7. Pour modifier les droits d'accès des utilisateurs dans ce groupe, cliquez sur le lien **Droits d'accès**.

   Les droits d'accès des utilisateurs de ce groupe sont affichés par **Module**. Pour modifier les droits d'accès de ce groupe, procédez comme suit,

   a. Cliquez sur l'icône **Modifier l'enregistrement** à côté du groupe.
   b. Cliquez sur les boutons radio à la droite de chaque module en spécifiant le droit d'accès en tant que **Pas d'accès**, **Lecture seule**, ou **Lecture/Ecriture**.
   c. Cliquez sur **Sauvegarder**.

   Remarque : Les utilisateurs peuvent appartenir à plusieurs groupes. Dans ces cas, lorsque les droits d'accès diffèrent selon les groupes, l'utilisateur hérite du plus haut niveau de droit d'accès assigné aux utilisateurs dans tous les groupes.

Remarque : Tous les membres du groupe des administrateurs du concentrateur peuvent avoir des permissions de superutilisateur. Cela permet à de nombreuses personnes de partager des responsabilités d'administrateur de concentrateur tout en préservant la sécurité du mot de passe.

Pour plus d'informations sur la gestion des groupes, voir "Gestion des groupes" dans le *Guide du partenaire WebSphere Partner Gateway*.

Création de contacts

Pourquoi et quand exécuter cette tâche

WebSphere Partner Gateway vous permet de créer des contacts qui peuvent être informés lorsque différents types d'événements se produisent. Suivez la procédure ci-dessous pour créer des contacts pour chaque partenaire:

1. Veillez à ce que le profil du partenaire pour lequel vous voulez créer des contacts soit sélectionné. Le profil sélectionné s'affiche en haut de la page après **Profil >**.

   Si le profil n'est pas sélectionné, procédez comme suit :

   a. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
   b. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
   c. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
2. Cliquez sur **Contacts**.

3. Cliquez sur **Créer**.
4. Entrez le **Nom donné** et **Nom de famille** de ce contact.
5. Entrez éventuellement l'**Adresse** de ce contact.
6. Sélectionnez éventuellement le **Type de contact**.
7. Entrez éventuellement l'**Adresse E-mail**, le numéro de **téléphone** et le **Numéro de fax** de ce contact.
8. Sélectionnez la **Langue**, les **Environnements de format** et le **Fuseau horaire** du contact.
9. Modifiez le **Statut d'alerte** de l'utilisateur sur **Activé**.
10. Sélectionnez la **Visibilité souscrite** de l'utilisateur.
11. Cliquez sur **Sauvegarder**.

Pour plus d'informations sur la gestion des contacts, voir "Gestion des contacts" dans le *Guide du partenaire de WebSphere Partner Gateway*.

Création d'adresses

Pourquoi et quand exécuter cette tâche

WebSphere Partner Gateway vous permet de créer des adresses pour les partenaires. Suivez la procédure ci-dessous pour créer des adresses pour un partenaire:

1. Veillez à ce que le profil du partenaire pour lequel vous voulez créer des adresses soit sélectionné. Le profil sélectionné s'affiche en haut de la page après **Profil >**.

   Si vous venez de créer un profil, il est déjà sélectionné. S'il n'est pas sélectionné, suivez les étapes ci-après pour le faire :

   a. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
   b. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
   c. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
2. Cliquez sur **Adresses**.
3. Cliquez sur **Créer une nouvelle adresse**.
4. Sélectionnez le **Type d'adresse**.
5. Vous pouvez également entrer l'**Adresse**.
6. Cliquez sur **Sauvegarder**.

Pour plus d'informations sur la gestion des adresses, voir "Gestion des adresses" dans le *Guide du partenaire WebSphere Partner Gateway*.

Chapitre 4. Etapes préalables à la configuration du concentrateur

Dans les chapitres suivants, vous allez configurer les récepteurs et les destinations décrits dans le Chapitre 2, «Introduction à la configuration du concentrateur», à la page 5. Selon les types de transport utilisés pour envoyer et recevoir des documents, vous devez configurer les récepteurs et les destinations.

Ce chapitre contient les rubriques suivantes :

- « Création d'une destination fichier-répertoire»
- «Configuration du serveur FTP pour la réception de documents»
- «Configuration du concentrateur pour le protocole de transport JMS», à la page 39
- «Configuration de la compression RNIF», à la page 45

Il propose également une présentation rapide des scripts FTP exigés par les récepteurs et destinations de script FTP, et décrit le client Data Interchange Services utilisé pour créer des mappes de transformation, validation et acceptation fonctionnelle pour les documents EDI, XML et ROD (record-oriented-data).

- «Utilisation des scripts FTP pour les récepteurs et destinations de scripts FTP», à la page 46
- «Utilisation de mappes à partir du client Data Interchange Services», à la page 46

Si vous ne prévoyez pas de configurer ce type de récepteurs ou destinations, passez directement au Chapitre 5, «Démarrage du serveur et affichage de la console de communauté», à la page 49.

Création d'une destination fichier-répertoire

Le répertoire que vous spécifiez pour une destination fichier-répertoire sera créé pour vous si nécessaire. S'il existe déjà, il sera utilisé par la destination.

Configuration du serveur FTP pour la réception de documents

Remarque : Cette section s'applique uniquement à la réception de documents via FTP ou FTPS provenant de partenaires. L'envoi de documents à des partenaires est décrit dans «Configuration d'une destination FTP», à la page 236 et «Configuration d'une destination FTPS», à la page 242.

Si vous avez l'intention d'utiliser le protocole de transport FTP ou FTPS pour les documents entrants, vous devez installer un serveur FTP. Si vous envisagez d'utiliser le protocole FTP mais que vous n'avez pas encore installé de serveur, installez-en un avant de poursuivre. Assurez-vous que l'une des conditions ci-après s'applique à votre installation :

- Le serveur FTP est installé sur la même machine que WebSphere Partner Gateway.
- Le bcguser de la machine WebSphere Partner Gateway dispose d'un accès en lecture/écriture à l'emplacement où le serveur FTP procédera au stockage des fichiers.

Remarque : Si l'installation s'effectue sur plusieurs machines, le serveur FTP doit être installé à l'endroit où le récepteur est installé.

Configuration de la structure de répertoire requise sur le serveur FTP

Pourquoi et quand exécuter cette tâche

Après avoir installé le serveur FTP, l'étape suivante consiste à créer la structure de répertoires requise sous le répertoire principal du serveur FTP. WebSphere Partner Gateway requiert une structure de répertoire particulière que le composant Récepteur et les composants Gestionnaire de documents utilisent pour identifier correctement le partenaire envoyant le document entrant. La structure est décrite à la figure 15.

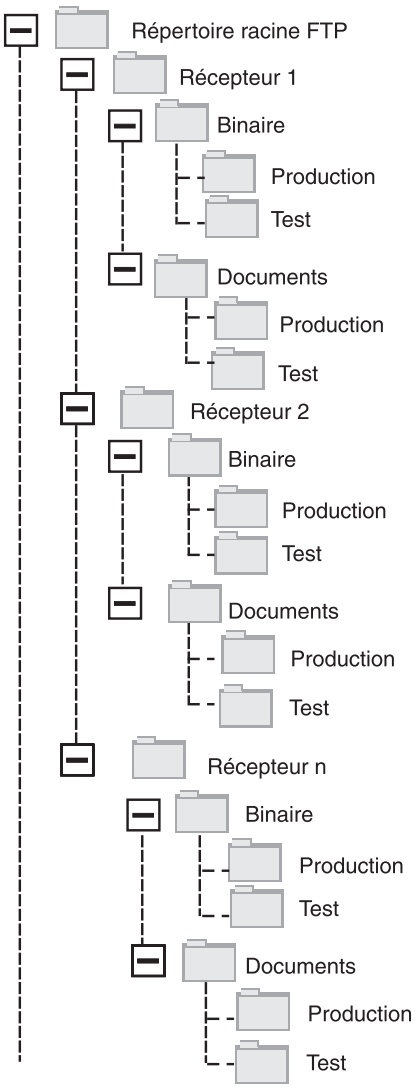


Figure 15. Structure de répertoire FTP

Chaque répertoire de partenaire contient un répertoire Binary et un répertoire documents. Chacun de ces deux répertoires contient un répertoire Production et un répertoire Test.

Le Répertoire documents est utilisé lorsqu'un partenaire envoie un document XML contenant des informations de routage complètes (via un FTP) vers le concentrateur. Il convient dans ce cas de créer une définition XML personnalisée. Les documents d'échange de données informatisé (EDI) peuvent également être envoyés via ce répertoire.

Le Répertoire Binary est utilisé lorsqu'un partenaire envoie tout autre document (via FTP) au concentrateur.

Pour chaque partenaire qui utilisera le FTP pour envoyer ou recevoir des documents, créez les dossiers suivants depuis le répertoire racine de votre serveur FTP :

1. Créez un dossier pour le partenaire.

   Remarque : Le nom du dossier doit correspondre au nom que vous spécifiez pour le **Nom de connexion de l'entreprise** lorsque vous créez le partenaire. La création des partenaires est décrite dans «Création des profils des partenaires», à la page 25.
2. Créez des sous-dossiers dans le dossier du partenaire intitulé `Binary` et `Documents`.
3. Sous les dossiers Binary et Documents, créez les sous-dossiers `Production` et `Test`.

Traitement des fichiers envoyés via FTP

Il est important de comprendre comment les fichiers binaires et XML sont traités par le serveur FTP.

Fichiers binaires

Les noms de fichiers binaires doivent être structurés selon un modèle précis, car les fichiers ne sont pas du tout inspectés par le gestionnaire de documents.

La structure des noms de fichier est :
<IDpartenaire_destinataire>.<Nom_fichier_unique>

Lorsqu'un fichier binaire est détecté par le composant Récepteur, il est écrit dans la mémoire partagée, puis transmis au gestionnaire de documents pour être traité.

Le nom du répertoire dans lequel le fichier a été détecté est utilisé pour évaluer le Nom du partenaire d'origine et la première partie du nom du fichier est utilisée pour évaluer le Nom du partenaire de destination. Par ailleurs, la position du répertoire dans l'arborescence permet de déterminer s'il s'agit d'une transaction de Production ou de Test.

Par exemple, un fichier nommé 123456789.abcdefg1234567 est détecté dans le répertoire `\ftproot\partenaireB\binary\production`. Le gestionnaire de documents a pris connaissance des informations suivantes :

- Le `Nom du partenaire d'origine` est `partenaireB` (car le fichier a été trouvé dans la partie partenaireB de l'arborescence).
- Le `Nom du partenaire de destination` est `partenaireA` (car la première partie du nom du fichier est 123456789, qui est l'ID DUNS du partenaireA).

  Remarque : Ici comme partout ailleurs dans ce document, les numéros DUNS ne sont que des exemples. WebSphere Partner Gateway requiert

l'<IDpartenaire_destinataire> pour correspondre au DUNS du partenaire destinataire. Si l'ID Duns n'est pas trouvé, la recherche de canaux échoue.
- La transaction est de type Production.

Le gestionnaire de documents recherche une connexion de partenaire de production entre le partenaireB et le partenaireA pour:
- Package : None (N/A)
- Protocole : Binary (1.0)
- Type de document : Binary (1.0)

Le gestionnaire de documents traite alors le fichier.

Les fichiers binaires peuvent également être transférés via FTP en utilisant le gestionnaire de prétraitement générique ou le gestionnaire FileNamePartnerId. Voir «Modification du point de configuration preprocess», à la page 82 pour plus de détails.

Fichiers XML

Un fichier XML qui est routé à l'aide de vos spécifications XML personnalisées n'a aucune règle d'appellation de fichier car le fichier est inspecté par le gestionnaire de documents et les informations de routage sont extraites du document lui-même.

Lorsqu'un fichier XML est détecté par le composant Récepteur, il est écrit dans la mémoire partagée puis transmis au gestionnaire de documents pour être traité.

Le gestionnaire de documents compare le fichier XML aux formats XML définis et sélectionne le format XML qui convient (le paramétrage des formats XML est décrit dans «Traitement de documents XML personnalisés», à la page 163). Le nom du partenaire d'origine, le Nom du partenaire de destination et les informations de routage sont extraits du fichier XML.

Par ailleurs, la position du répertoire dans l'arborescence permet de déterminer s'il s'agit d'une transaction de Production ou de Test.

Le gestionnaire de documents utilise ensuite ces informations pour localiser la bonne connexion de partenaire avant de traiter le fichier.

Configuration supplémentaire du serveur FTP

Pourquoi et quand exécuter cette tâche

Après avoir créé la structure de répertoire requise, vous configurez votre serveur FTP pour chacun des partenaires de la communauté du concentrateur. La façon dont vous allez configurer le serveur FTP dépend du serveur que vous utilisez. Consultez la documentation du serveur FTP, puis effectuez les opérations suivantes :

Procédure

1. Ajoutez un nouveau groupe (par exemple Partenaires).
2. Ajoutez un utilisateur au groupe nouvellement créé pour chaque partenaire qui enverra ou recevra des documents sur FTP.
3. Pour chaque partenaire, configurez le serveur FTP pour mapper le partenaire entrant à la structure de répertoire que vous avez créée pour le partenaire dans la section précédente « Configuration de la structure de répertoire requise sur

le serveur FTP», à la page 36. Pour plus d'informations, reportez-vous à la documentation relative à votre serveur FTP.

Considérations relatives à la sécurité du serveur FTP

Si vous utilisez un serveur FTP pour recevoir des documents entrants, les considérations relatives à la sécurité pour les sessions SSL sont gérées uniquement par le serveur FTPS et le client utilisés par le partenaire. Il n'existe pas de configuration de sécurité spécifique à WebSphere Partner Gateway pour les documents FTPS entrants. WebSphere Partner Gateway extrait les documents du récepteur FTP (décrit dans « Configuration d'un récepteur FTP», à la page 66) une fois que le serveur a négocié des canaux sécurisés et reçu le document. Pour configurer un canal sécurisé qui puisse être contacté par un partenaire, reportez-vous à la documentation relative au serveur FTPS pour connaître les certificats requis (et où ils sont nécessaires).

Pour authentifier le serveur, fournissez le certificat du composant Récepteur aux partenaires. Si ce certificat est fourni par une Autorité de certification, fournissez également la chaîne de certificat de CA. Si l'authentification client est prise en charge par le serveur FTPS, les certificats d'authentification client des partenaires doivent être spécifiés dans le serveur FTP. Consultez la documentation du serveur FTPS pour obtenir des informations sur l'authentification client et les certificats.

Configuration du concentrateur pour le protocole de transport JMS

Cette section indique comment paramétrer le concentrateur pour utiliser le transport JMS. Si vous comptez utiliser le transport JMS pour envoyer des documents à partir du concentrateur ou en recevoir, procédez de la façon indiquée ici. Dans le cas contraire, passez à la section suivante.

Remarque : Cette section indique comment utiliser l'implémentation JMS de WebSphere MQ pour paramétrer l'environnement JMS. Ces procédures décrivent également comment définir les files d'attente locales. Si vous voulez définir les files d'attente éloignées et de transmission, consultez la documentation de WebSphere MQ.

Bien que cette section soit spécifique à WebSphere MQ, d'autres fournisseurs JMS vont exiger des procédures similaires. Pour WebSphere Platform Messaging, consultez le chapitre 5 "Configuration du JMS lorsque WebSphere Partner Gateway est installé sur WebSphere Application Server". "Intégration de WebSphere Process Server avec JMS comme transport" dans le *Guide d'intégration de WebSphere Partner Gateway*.

Dans les sections suivantes de ce document, vous apprendrez comment configurer des récepteurs ou destinations JMS (ou les deux). Ces tâches sont décrites dans « Configuration d'un récepteur JMS», à la page 69 et «Configuration d'une destination JMS», à la page 239.

Création d'un répertoire pour JMS

Pourquoi et quand exécuter cette tâche

Vous devez tout d'abord créer un répertoire pour JMS. Par exemple, supposons que vous vouliez créer un répertoire nommé JMS sous le répertoire temporaire c:\temp d'une installation Windows. Voici comment procéder :

Procédure

1. Ouvrez l'Explorateur Windows.
2. Ouvrez le répertoire C:\temp.
3. Créez un nouveau dossier nommé JMS.

Modification de la configuration JMS par défaut

Pourquoi et quand exécuter cette tâche

Cette section vous indique comment mettre à jour le fichier JMSAdmin.config, qui fait partie de l'installation de WebSphere MQ, afin de modifier la fabrique de contextes et l'URL du fournisseur.

1. Accédez au répertoire `Java\bin` de WebSphere MQ. Par exemple, dans le cas d'une installation Windows, accédez au répertoire C:\IBM\MQ\Java\bin
2. Ouvrez le fichier JMSAdmin.config dans un éditeur de texte en clair, tel que le Bloc-Notes ou vi.
3. Ajoutez le caractère # au début des lignes suivantes :

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

4. Supprimez le caractère # situé au début des lignes suivantes :

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

5. Modifiez la ligne `PROVIDER_URL=file:/C:/JNDI-Directory` de sorte qu'elle indique le nom du répertoire JMS défini à l'étape « Création d'un répertoire pour JMS», à la page 39. Par exemple, si vous avez défini le répertoire `c:/temp/JMS` la ligne doit se présenter comme suit :

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

6. Enregistrez le fichier.

Création des files d'attente et du canal

Cette section vous indique comment utiliser WebSphere MQ pour créer les files d'attente qui serviront à l'envoi et à la réception de documents, ainsi que le canal pour cette communication. On suppose que le gestionnaire de files d'attente a été créé. Le nom du gestionnaire de files d'attente doit être remplacé à l'emplacement où le *<nom du gestionnaire de files d'attente>* apparaît dans les étapes suivantes. On suppose également qu'un programme d'écoute a été démarré pour cette file d'attente sur le port TCP 1414.

1. Ouvrez une invite de commande.
2. Entrez la commande suivante pour lancer le serveur de commande WebSphere MQ :

   ```
   strmqcsv <nom du gestionnaire de files d'attente>
   ```

3. Entrez la commande suivante pour lancer l'environnement de commande WebSphere MQ :

   ```
   runmqsc <nom du gestionnaire de files d'attente>
   ```

4. Entrez la commande suivante pour créer la file d'attente WebSphere MQ où seront mis en attente les documents entrants envoyés au concentrateur :

   ```
   def ql(<nom_file_attente>)
   ```

   Ainsi, pour créer une file d'attente appelée JMSIN, vous devez entrer :

   ```
   def ql(JMSIN)
   ```

5. Entrez la commande suivante pour créer la file d'attente WebSphere MQ où seront mis en attente les documents envoyés à partir du concentrateur :

   ```
   def ql(<nom_file_attente>)
   ```

   Par exemple, pour créer une file d'attente nommée JMSOUT, vous devriez entrer :

   ```
   def ql(JMSOUT)
   ```

6. Entrez la commande suivante pour créer un canal WebSphere MQ qui sera utilisé pour les documents envoyés à partir du concentrateur :

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

   Par exemple, pour créer un canal appelé java.channel, vous devez entrer :

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

7. Entrez la commande suivante pour quitter l'environnement de commande WebSphere MQ :

   ```
   end
   ```

Ajout d'une phase d'exécution Java à votre environnement

Pourquoi et quand exécuter cette tâche

Saisissez la commande suivante pour ajouter une phase d'exécution Java™ à votre chemin système :

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

où *ProductDir* indique le répertoire dans lequel WebSphere Partner Gateway est installé.

Définition de la configuration JMS

Pourquoi et quand exécuter cette tâche

Pour définir la configuration JMS, procédez comme suit :

1. Passez dans le répertoire WebSphere MQ Java (répertoire *<chemin d'accès au répertoire d'installation Websphere MQ>*\java\bin)
2. Démarrez l'application JMSAdmin en tapant la commande suivante :

   ```
   JMSAdmin
   ```

3. Définissez un nouveau contexte JMS en tapant les commandes suivantes à partir de l'invite InitCtx> :

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

   Par exemple, si le *nom_contexte* est JMS, les commandes seront du type :

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

4. A partir de l'invite InitCtx/jms>, entrez la configuration JMS suivante :

   ```
   define qcf(nom_de_fabrique_de_connexion)
       tran(CLIENT)
       host(<votre_adresse_IP>)
       port(1414)
       chan(java.channel)
       qmgr(<nom_du_gestionnaire_de_file_d'attente>)
   define q(<nom>) queue(<nom_file>) qmgr(<nom_du_gestionnaire_de_file_d'attente>)
   define q(<nom>) queue(<nom_file>) qmgr(<nom_du_gestionnaire_de_file_d'attente>)
   end
   ```

Remarque :

- Si MQ et WebSphere Partner Gateway sont installé sur deux machines différentes, sélectionnez le type de transport en tant que CLIENT.
- Si MQ et WebSphere Partner Gateway sont installés sur la même machine, le type de transport doit être BINDINGS.

Les étapes précédentes ont créé le fichier .bindings, qui se trouve dans un sous-dossier du dossier indiqué à l'étape 5, à la page 40. Le nom du sous-dossier et le nom indiqué pour votre contexte JMS.

Ainsi, la session JMSAdmin suivante sert à définir la fabrique de connexions aux files d'attente sous le nom `Hub`, avec l'adresse IP `sample.ibm.com` où réside le gestionnaire de files d'attente MQ (<*nom du gestionnaire de file d'attente*> de `sample.queue.manager`). L'exemple utilise les noms de file d'attente JMS et le nom de canal créé dans «Création des files d'attente et du canal», à la page 40. Notez que les informations entrées par l'utilisateur suivent l'invite >.

```
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
```

Dans cet exemple, le fichier .bindings se trouvera dans le répertoire `c:/temp/JMS/JMS` , où `c:/temp/JMS` est le PROVIDER_URL et `JMS` le nom de contexte.

Configuration des bibliothèques d'exécution

En ce qui concerne le récepteur JMS ou la destination JMS, plusieurs fichiers JAR de WebSphere MQ doivent être visibles pour WebSphere Partner Gateway. Ces fichiers JAR deviennent visibles une fois placés dans le chemin de classes. Si vous utilisez le mode Liaison MQ pour accéder à MQ, alors les bibliothèques natives MQ doivent également apparaître dans le chemin d'accès. Pour plus d'informations sur les fichiers JAR MQ et les bibliothèques natives pour JMS, reportez-vous à la documentation de WebSphere MQ.

Il existe plusieurs méthodes pour ajouter des fichiers JAR au chemin de classes Websphere Partner Gateway. La première consiste à les placer dans le répertoire d'exits utilisateur et la seconde consiste à les associer via les bibliothèques partagées de WebSphere Application Server.

Méthode appliquée au répertoire Exits utilisateurs

Pour utiliser cette méthode, placez les fichiers JAR spécifiés dans le répertoire Exits utilisateur adéquat :

- Pour le récepteur JMS, placez les fichiers dans le répertoire <WPG-Install root>/receiver/lib/userexits
- Pour la destination JMS, placez les fichiers dans le répertoire <WPG-Install root>/router/lib/userexits

Méthode des bibliothèques partagées WebSphere Application Server

Pourquoi et quand exécuter cette tâche

Pour utiliser cette méthode, créez une variable pour la bibliothèque partagée, puis associez-la au récepteur ou à l'application du gestionnaire de documents comme indiqué brièvement dans les étapes suivantes. Pour plus d'informations sur cette procédure, reportez-vous à la documentation de WebSphere Application Server.

1. Connectez-vous à la console d'administration WebSphere Application Server.
2. Créez une variable pour les bibliothèques partagées en effectuant les actions suivantes :
   a. Naviguez jusqu'à **Environnement** > **Bibliothèques partagées**.
   b. Sélectionnez une **Portée** (probablement un noeud), puis cliquez sur **Nouveau**.
   c. Saisissez le nom de la variable (par exemple, MQ_LIBRARIES), renseignez les entrées du chemin de classes pour les fichiers JAR MQ, puis cliquez sur **OK**.
3. Associez la variable de la bibliothèque partagée que vous venez de créer aux composants de WebSphere Partner Gateway en effectuant les actions suivantes :
   a. Naviguez jusqu'à **Applications** > **Applications d'entreprise**.
   b. Sélectionnez **BCGReceiver** (pour les récepteurs JMS) ou **BCGDocMgr** (pour les destinations JMS).
   c. Sélectionnez **Références de la bibliothèque partagée**.
   d. Sélectionnez l'application, puis cliquez sur **Bibliothèques partagées de référence**.
   e. Dans la liste Disponible, sélectionnez la variable de la bibliothèque partagée que vous venez de créer (par exemple, MQ_LIBRARIES) et placez-la dans la liste Sélectionné. Cliquez ensuite sur **OK**.

Configuration du récepteur et de la passerelle JMS avec MQ externe

Pourquoi et quand exécuter cette tâche

Procédez de la manière suivante pour créer un pont de communication entre WebSphere Partner Gateway et MQ via la console d'administration WebSphere Application Server :

1. Créez la fabrique de connexions de file d'attente JMS.
   a. Connectez-vous à la console d'administration WebSphere Application Server.
   b. Naviguez jusqu'à **Ressources > JMS > Fabriques de connexions de file d'attente**.
   c. Sélectionnez une **Portée** et cliquez sur **Nouveau**
      - Pour la configuration de la passerelle, sélectionnez la portée du noeud/serveur du gestionnaire de documents. (La portée du noeud est utile en présence de clusters. En mode simple, sélectionnez une portée de serveur.)
      - Pour la configuration du récepteur, sélectionnez la portée du noeud/serveur du récepteur. (La portée du noeud est utile en présence de clusters. En mode simple, sélectionnez une portée de serveur.)
   d. Sélectionnez l'option **Fournisseur de messagerie WebSphere MQ** et cliquez sur **OK**.

e. Entrez le **Nom** et **Nom JNDI**. Ces valeurs sont obligatoires.

f. Entrez les valeurs appropriées pour **Gestionnaire de files d'attente**, **Hôte** (IP de la machine sur laquelle fonctionne le gestionnaire de files d'attente), **Port**, **Canal** et **Type de transport**. Les autres zones sont facultatives.

Remarque :

- Si MQ et WebSphere Partner Gateway sont installé sur deux machines différentes, sélectionnez le type de transport en tant que CLIENT.
- Si MQ et WebSphere Partner Gateway sont installés sur la même machine, le type de transport doit être BINDINGS.

Pour plus de détails, référez-vous au centre de documentation de WebSphere Application Server à l'adresse suivante : http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multipla...

2. Créez une file d'attente JMS.
   a. Connectez-vous à la console d'administration WebSphere Application Server.
   b. Naviguez jusqu'à **Ressources > JMS > Files d'attente**.
   c. Sélectionnez une **Portée** et cliquez sur **Nouveau**
      - Pour la configuration de la passerelle, sélectionnez la portée du noeud/serveur du gestionnaire de documents. (La portée du noeud est utile en présence de clusters. En mode simple, sélectionnez une portée de serveur.)
      - Pour la configuration du récepteur, sélectionnez la portée du noeud/serveur du récepteur. (La portée du noeud est utile en présence de clusters. En mode simple, sélectionnez une portée de serveur.)
   d. Entrez le **Nom** et **Nom JNDI**. Ces valeurs sont obligatoires.
   e. Entrez les valeurs appropriées pour **Gestionnaire de files d'attente**, **Hôte** (IP de la machine sur laquelle fonctionne le gestionnaire de files d'attente), **Port**, **Canal** et **Type de transport**. Les autres zones sont facultatives.
   f. Redémarrez les serveurs ayant subi des modifications, par exemple DocumentManager/Receiver/bcgserver dans la cas d'une installation répartie simple.
3. Configurez JMS Gateway sur WebSphere Partner Gateway.
   a. Connectez-vous à la console d'administration de WebSphere Partner Gateway.
   b. Cliquez sur **Administrateur du compte > Profils > Destinations**.
   c. Cliquez sur **Créer**.
   d. Entrez le **Nom de destination**. Cette zone est obligatoire.
   e. Sélectionnez **JMS** dans la zone de transport.
   f. Entrez des valeurs pour les zones obligatoires suivantes :
      - Adresse : entrez l'adresse de destination en fournissant le port et le nom d'hôte corrects de la fabrique de connexions de file d'attente ou des objets de file d'attente ayant été créés dans WebSphere Application Server. L'adresse doit être au format corbaloc:iiop: <hostname>: <bootstrapportnumber> , où :
        – corbaloc:iiop - correspond au protocole utilisé pour la communication entre le client (WebSphere Partner Gateway) et le serveur (WebSphere Application Server).
        – <hostname> - Nom d'hôte ou adresse IP de la machine où WebSphere Application Server est installé, pour laquelle la fabrique de connexions de file d'attente et les objets de file d'attente ont été créés.

– <bootstrapportnumber> - Numéro de port d'amorce du serveur où la fabrique de connexions de file d'attente et les objets de file d'attente sont liés. Pour obtenir le numéro de port d'amorce, vous pouvez vous connecter à la console d'administration WebSphere Application Server, naviguez jusqu'à **Serveurs > Serveur d'applications > <nom de serveur> Ports** vérifiez l'adresse du port d'amorce. Dans le cas d'un mode réparti, les numéros de port sont différents pour le récepteur et la passerelle. Accédez au serveur correspondant (bcgreceiver pour le récepteur et bcgdocmgr pour la passerelle) afin d'obtenir le numéro de port d'amorce correct.

- Nom de fabrique JMS : nom JNDI fourni pour la fabrique de connexions de file d'attente JMS.
- Nom de file d'attente JMS : nom JNDI fourni pour la file d'attente JMS.
- Nom de fabrique JNDI JMS : fabrique à utiliser pour la communication JNDI. Puisque vous utilisez WebSphere Application Server, vous pouvez spécifier la valeur comme étant com.ibm.websphere.naming.WsnInitialContextFactory.

4. Configurez le récepteur JMS sur WebSphere Partner Gateway.
   a. Connectez-vous à la console d'administration de WebSphere Partner Gateway.
   b. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
   c. Cliquez sur **Créer le récepteur**.
   d. Entrez le **Nom du récepteur**. Cette zone est obligatoire.
   e. Sélectionnez **JMS** dans la zone de transport.
   f. Entrez les valeurs appropriées pour les zones requises comme indiqué à l'étape :3f, à la page 44.

Configuration de la compression RNIF

Les messages Rosettanet Business Message et leurs pièces jointes sont compressés et mis en package avec l'enveloppe S/MIME pour transférer des documents volumineux. La décompression est également prise en charge. Une option de compression de la charge, seule ou avec des pièces jointes, vous est fournie. Pour une performance accrue, compressez le contenu du service et ses pièces jointes avant de procéder au chiffrement, à la signature ou au codage du transfert selon la spécification Technical Advisory de Rosettanet 2.0. Sous le canal WebSphere Partner Gateway de Rosettanet approprié, sélectionnez la valeur suivante pour la compression de l'attribut d'objet de routage :

- None
- Charge
- Charge et pièces jointes

Vous pouvez également sélectionner des attributs supplémentaires de critère de filtrage comme **Compresser le type de contenu** et **Compresser la taille**. Les critères de filtrage permettent de sélectionner la charge ou les pièces jointes à partir du pool des pièces jointes. L'attribut **Compresser le type de contenu** peut avoir pour valeur “Tout” ou des types MIME valides séparés par une virgule. Si vous sélectionnez l'option **Charge** dans votre option de compression de base, celle-ci sera alors compressée indépendamment de la valeur de l'attribut **Compresser le type de contenu**. Seules les pièces jointes sont sélectionnées pour compression en tenant compte des types de contenu indiqués. L'attribut **Compresser la taille** peut

avoir pour valeur “Tout” ou une limite de taille valide. Cette dernière indique la taille minimum acceptable pour la compression.

Lorsqu'un document Rosettanet compressé est envoyé, la décompression S/MIME concerne le contenu de service et ses pièces jointes.

Utilisation des scripts FTP pour les récepteurs et destinations de scripts FTP

Le transport de script FTP permet d'envoyer des données à tout service FTP, y compris à un VAN (réseau privé). Vous contrôlez les opérations sur le serveur FTP à l'aide d'un fichier de script contenant des commandes FTP.

Vous définissez ce script lorsque vous créez le récepteur ou la destination de script FTP. WebSphere Partner Gateway met à jour les éléments remplaçables du script FTP avec les valeurs réelles entrées lorsque vous créez le récepteur ou la destination.

Les opérations définies dans le script d'entrée sont traduites en actions sur le serveur FTP. Le script de saisie est constitué d'un groupe de commandes FTP prises en charge. Les paramètres de ces commandes peuvent être des variables, renseignées lors de l'exécution.

Pour des informations sur la création d'un script FTP pour un récepteur de script FTP, consultez « Configuration d'un récepteur de script FTP», à la page 72. Pour des informations sur la création d'un script FTP pour une destination de script FTP, consultez «Configuration d'une destination de script FTP», à la page 245.

Utilisation de mappes à partir du client Data Interchange Services

Pour procéder au désenveloppement, à la transformation ou à la validation EDI, ou pour exécuter des transformations entre ROD, XML et EDI, vous devez importer les mappes associées depuis le client Data Interchange Services. Data Interchange Services est un programme installé séparément qui réside généralement sur un ordinateur différent de celui sur lequel WebSphere Partner Gateway est exécuté.

Le spécialiste de mappage Data Interchange Services crée des mappes décrivant la transformation et la validation de documents spécifiques.

Pour créer une mappe, la définition des documents source et cible est requise. La définition des documents source pour EDI est fournie par WDI, mais pour ROD et XML, vous devez la créer en utilisant le client DIS. Pour EDI, importez le fichier .eif, le fichier standard, dans le client DIS. Pour ROD, créez le standard à l'aide du client DIS. Importez DTD/XSD pour créer le standard pour XML. Le standard et les mappes de transformation peuvent être compilés séparément.

Par exemple, vous souhaiterez peut-être qu'un bon de commande créé par une application dorsale soit transformé et envoyé à un partenaire externe en tant que bon de commande X12 EDI standard (850). Le spécialiste des mappages Data Interchange Services écrit une mappe décrivant la transformation de chaque zone ou élément de données du programme au format X12. La mappe doit ensuite être exportée directement dans WebSphere Partner Gateway, ou dans un fichier que vous importerez à l'aide d'un script de commande.

Des informations détaillées sur l'importation de mappes à partir d'un client Data Interchange Services sont proposées dans « Importation manuelle de mappes», à la page 213.

Remarque : Le client DIS possède sa propre base de données. Une fois que vous avez terminé une mappe dans le client DIS, exportez-la en tant que fichier .EIF. Depuis la console de WebSphere Partner Gateway, importez ce fichier . EIF. Il stockera les informations dans la base de données WebSphere Partner Gateway.

Exécution des tâches de configuration de post-installation

Une fois que vous avez installé WebSphere Partner Gateway, vous devez le configurer. En général, la configuration de votre concentrateur implique l'utilisation de la console d'administration WebSphere Partner Gateway. Selon les exigences de votre communauté d'échange, il se peut que vous deviez configurer l'infrastructure de WebSphere Application Server qui héberge les composants de WebSphere Partner Gateway. Plusieurs de ces tâches sont répertoriées ici, ainsi que des liens vers des instructions détaillées permettant d'effectuer chaque tâche.

- «Modification de la puissance du chiffrement», à la page 268
- «Configuration du protocole SSL avec authentification du client», à la page 270

Chapitre 5. Démarrage du serveur et affichage de la console de communauté

Ce chapitre indique comment démarrer le serveur WebSphere Partner Gateway et comment afficher la console de communauté. Il contient les rubriques suivantes :

Pour plus d'informations sur la procédure de lancement des clusters à partir de la console d'administration de WebSphere Application Server Network Deployment, reportez-vous au chapitre 1. "Gestion des applications du composant de WebSphere Partner Gateway" du *Guide d'administration de WebSphere Partner Gateway*.

Démarrage des composants de WebSphere Partner Gateway

Pourquoi et quand exécuter cette tâche

Pour démarrer le serveur, vous devez lancer chacun des trois composants de WebSphere Partner Gateway, à savoir la console, le gestionnaire de documents et le récepteur.

En mode simple, tous les composants WebSphere Partner Gateway sont installés sur la même instance de WebSphere Application Server. Vous démarrez et arrêtez l'ensemble des composants à l'aide de scripts et de la console d'administration WebSphere Application Server. Pour démarrer les composants WebSphere Partner Gateway dans un système en mode simple, exécutez le script suivant :

```
<REP INSTALL>/bin/bcgStartServer.sh
```

Pour arrêter les composants WebSphere Partner Gateway dans un système en mode simple, exécutez le script suivant :

```
<REP INSTALL>/bin/bcgStopServer.sh
```

Remarque : Vous n'êtes pas tenu de spécifier un nom de serveur pour l'installation en mode simple. En mode simple, le nom de serveur est toujours server1.

Remarque : Si le programme d'installation est exécuté alors que le répertoire **temp** dispose d'un espace insuffisant et que le produit n'est pas installé correctement, augmentez la quantité d'espace du répertoire **temp**, puis désinstallez et réinstallez le produit.

1. Saisissez http://<nom de l'ordinateur ou adresse IP>:58080/console, le navigateur affiche la page d'accueil. Connectez-vous à WebSphere Partner Gateway à l'aide des informations suivantes :
   - dans la zone **Nom d'utilisateur**, entrez :
     ```
     hubadmin
     ```
   - Dans la zone **Mot de passe**, entrez :
     ```
     Pa55word
     ```
   - Dans la zone **Nom de l'entreprise**, entrez :
     ```
     Operator
     ```

   Cliquez sur **Connexion**.

2. Lorsque vous vous connectez pour la première fois, vous devez créer un nouveau mot de passe. Entrez un nouveau mot de passe, puis confirmez-le en le saisissant une seconde fois dans la zone **Vérifier**.
3. Cliquez sur **Sauvegarder**. Le système affiche la fenêtre d'entrée de la console de communauté.

Lorsque vous installez WebSphere Partner Gateway Application, les applications Premières étapes et Test de Vérification de l'Installation (IVT) sont installées par défaut. Elles resteront installées tant que le moindre composant WebSphere Partner Gateway réside dans la machine. La page des Première étapes renseigne les données des composants installés afin d'exécuter séparément un test de vérification pour chaque composant.

Vous pouvez appeler la page des Premières étapes à l'aide de la commande **bcgFirstSteps. sh**, disponible dans le dossier <install_dir>/FirstSteps/bin.

Depuis la page Premières étapes de la console, le démarrage et l'arrêt des options peuvent être basculés pour tous les composants installés. Par exemple, si le concentrateur est en cours d'exécution, l'option arrêt sera répertoriée. Sinon, l'option démarrer est répertoriée. Ce qui suit répertorie les options d'arrêt et démarrage des composants en fonction de leurs topologies :

- Le démarrage et l'arrêt pour Web Sphere Process Gateway sont disponibles pour les topologies en mode simple et réparti simple.
- Le démarrage et l'arrêt pour le MAS sont disponibles pour les topologies en mode simple et entièrement réparti.
- Le démarrage et l'arrêt pour le gestionnaire de déploiement sont disponibles pour les topologies en mode simple et entièrement réparti.

  Remarque : Cette option ne sera disponible que si le gestionnaire de déploiement est installé à l'aide du programme d'installation de WebSphere Partner Gateway.
- Le démarrage et l'arrêt de la console, du Récepteur et du routeur sont disponibles pour les topologies en mode entièrement réparti.
- Le démarrage et l'arrêt du gestionnaire de FTP sont disponibles pour toutes les topologies.

Les options ci-dessus sont disponibles pour les topologies répertoriées dans la mesure où elles sont installées sur cette machine. Vous devez consulter les journaux du serveur pour contrôler le succès de l'action. Vous pouvez également faire référence à la fenêtre de ligne de commande pour vérifier le statut. Lorsque vous cliquez sur le lien **Démarrer WPG** dans l'écran Premières étapes, la commande de démarrage est émise dans une invite de commande DOS. L'écran Première étapes ne vous transmettra pas de notification sur le succès (ou l'échec) de la commande.

Lorsque l'option du test de vérification de l'installation (IVT) est appelée, elle vérifie la validité des composants de WebSphere Partner Gateway installés sur la machine. Ce test de vérification peut être également appelé depuis une ligne de commande utilisant la commande **LaunchIVT.sh**. Cette commande se trouve dans le dossier <installdir>/FirstSteps/ivt/bin. A l'issue de la vérification, l'IVT génère un rapport contenant les détails de tous les composants de WebSphere Partner Gateway installés. Il nettoie également les fichiers temporaires qui ont été créés pendant cette opération et arrête tout serveur/noeud qui a été démarré pour cette opération. Pour indiquer la défaillance de tout composant, les fichiers journaux nécessaires sont générés dans le dossier <installdir>/FirstSteps/ivt/logs.

Remarque : Dans la topologie répartie, l'IVT ne vérifiera pas les composants installés sur différentes machines.

Lorsque vous essayez de télécharger des certificats avec une cryptographie plus évoluée que la cryptographie par défaut, le téléchargement risque d'échouer.

Connexion à la console de communauté

Pourquoi et quand exécuter cette tâche

Cette section présente les étapes d'affichage et de connexion à la console de communauté. Il est recommandé d'utiliser la résolution d'écran 1024x768.

Remarque : La console de communauté de WebSphere Partner Gateway requiert que la prise en charge de cookies soit activée pour la gestion des informations de la session. Aucune information personnelle n'est stockées dans le cookie et celui-ci expire à la fermeture du navigateur.

1. Ouvrez un navigateur Web et entrez l'URL suivante pour afficher la console :

   http://<*nom d'hôte*>.<*domaine*>:58080/console (unsecure)

   https://<*nom d'hôte*>.<*domaine*>:58443/console (secure)

   Où <*nom d'hôte*> et <*domaine*> correspondent au nom et à l'emplacement de la machine hébergeant la console de communauté.

   Remarque : Ces URL supposent que les numéros de port par défaut sont utilisés. Si vous les avez modifiés, remplacez les numéros par défaut par ceux que vous avez indiqués.

Dans la plupart des cas, votre administrateur de concentrateur vous a transmis le nom d'utilisateur, le mot de passe initial et le nom de connexion de l'entreprise nécessaires pour vous connecter à la console de communauté. Ces informations vous seront utiles pour la procédure qui suit. Si vous ne disposez pas de ces informations, contactez votre administrateur de concentrateur.

Pour vous connecter à la console de communauté, procédez comme suit (ces instructions concernent aussi bien les partenaires internes qu'externes) :

1. Entrez le **Nom d'utilisateur** de votre entreprise.
2. Entrez le **Mot de passe**.
3. Entrez le **Nom de connexion de l'entreprise**, comme IBM, par exemple.
4. Cliquez sur **Connexion**. Lors de votre première connexion, vous devez créer un nouveau mot de passe.
5. Entrez ce nouveau mot de passe. Entrez-le une seconde fois dans la zone de texte de vérification.
6. Cliquez sur **Sauvegarder**. Le système affiche l'écran d'entrée de la console.

Remarque : Si WebSphere Partner Gateway a été configuré avec le protocole LDAP, vous devez alors saisir le nom d'utilisateur et le mot de passe LDAP. Le nom de connexion de l'entreprise indiqué dans cet exemple est mentionné à titre d'exemple. Il ne vous sera pas demandé d'utiliser cette information. Le système ne vous demandera pas non plus de changer votre mot de passe.

Chapitre 6. Configuration de la console de communauté

Ce chapitre indique comment configurer la console de communauté pour préciser ce que voient les partenaires, la façon dont ils se connectent à la console, ainsi que leur accès aux diverses tâches de la console. Ce chapitre contient les rubriques suivantes :

- «Définition des informations concernant l'environnement local et le marquage de la console»
- «Définition des règles sur les mots de passe», à la page 55
- «Configuration des droits d'accès», à la page 57
- «Configuration de la valeur du délai d'attente de la console», à la page 59

Vous n'avez pas besoin d'effectuer ces opérations si vous utilisez les paramètres par défaut proposés par WebSphere Partner Gateway.

Remarque : Pour effectuer des modifications de configurations sur WebSphere Partner Gateway, vous devez toujours utiliser la même instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Définition des informations concernant l'environnement local et le marquage de la console

Pourquoi et quand exécuter cette tâche

Par défaut, les pages de la console de communauté s'affichent en anglais. IBM met à disposition ces pages dans d'autres langues, sous forme de fichiers téléchargeables. Les autres éléments de la console qui sont proposés par IBM pour d'autres paramètres nationaux sont les bannières. Vous pouvez également télécharger votre propre logo, ainsi que vos feuilles de style personnalisées pour mettre en forme le texte sur les pages.

Pour effectuer ces tâches, utilisez la page Téléchargement de l'environnement local. Pour afficher la page Téléchargement de l'environnement local, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration de la console > Configuration de l'environnement local**.
2. Cliquez sur **Créer**.
3. Sélectionnez un environnement local dans la liste **Environnement local**.

La console affiche la page Téléchargement de l'environnement local.

Dans cette page, vous pouvez effectuer les opérations suivantes :

- marquer la console en téléchargeant une bannière ou un logo unique (ou les deux à la fois) ;
- télécharger des fichiers fournis par IBM, que vous pouvez utiliser pour localiser le contenu des éléments de la console.

Marquage de la console

Pourquoi et quand exécuter cette tâche

Vous pouvez personnaliser l'aspect de la console de communauté en remplaçant les images de marquage. Le marquage de la console de communauté consiste à importer deux images principales : l'arrière-plan de l'en-tête et le logo de la société.

- Le arrière-plan de l'en-tête s'étend sur la partie supérieure de la console de communauté.
- Le logo de la société s'affiche en haut à droite de la console de communauté.

Pour être intégrées dans la fenêtre de la console de communauté, les images doivent être des fichiers au format .JPG et respecter certaines spécifications.

- Pour connaître les spécifications auxquelles doivent répondre la bannière et le logo, cliquez sur **Spécifications d'image** dans la fenêtre Téléchargement de l'environnement local.
- Pour visualiser un exemple d'image d'en-tête ou de logo, faites défiler l'écran jusqu'à la zone de la page intitulée **Modèles d'image**, puis cliquez sur **sample_headerback.jpg** ou sur **sample_logo.jpg**.
- Pour télécharger des exemples de bannière ou de logo et les utiliser comme modèles pour créer votre propre bannière ou logo, cliquez sur **Modèles d'image (arrière-plan d'en-tête et logo de la société)**.

Après avoir créé la bannière ou le logo (ou les deux), procédez comme suit :

1. Pour télécharger la bannière personnalisée, effectuez l'une des opérations suivantes :
   - Dans la zone **Bannière**, indiquez le chemin et le nom du fichier image que vous voulez utiliser pour l'en-tête et/ou la bannière.
   - Cliquez sur **Parcourir** pour naviguer jusqu'au fichier .jpg contenant la bannière, puis sélectionnez-le.
2. Pour télécharger le logo personnalisé, effectuez l'une des opérations suivantes :
   - Dans la zone **Logo**, indiquez le chemin et le nom du fichier que vous voulez utiliser pour le logo de la société.
   - Cliquez sur **Parcourir** pour naviguer jusqu'au fichier .jpg contenant le logo, puis sélectionnez-le.
3. Cliquez sur **Télécharger**.

Remarque : Lorsque vous remplacez l'arrière-plan de l'en-tête et le logo de la société, vous devez redémarrer la console de communauté pour que les modifications prennent effet.

Modification de la feuille de style

Pourquoi et quand exécuter cette tâche

Si vous souhaitez préciser une feuille de style différente de la valeur par défaut (par exemple, pour utiliser des tailles de polices et couleurs différentes), procédez comme suit :

1. Selon votre cas, appliquez les étapes suivantes :
   - Dans la zone **CSS**, indiquez le chemin et le nom du fichier contenant la feuille de style personnalisée.

- Cliquez sur **Parcourir** pour accéder au fichier contenant la feuille de style, puis sélectionnez-le.

2. Cliquez sur **Télécharger**.

Localisation des données de la console

Pourquoi et quand exécuter cette tâche

Si IBM vous fournit des regroupements de ressources ou d'autres fichiers d'environnement local, vous pourrez les télécharger à partir de la page Téléchargement de l'environnement local. Les informations suivantes figurent dans les packages de ressource :

- les **libellés de la console**, qui contiennent des chaînes texte représentant l'ensemble du texte de l'interface
- les **descriptions d'événements**, qui contiennent des chaînes texte utilisées pour afficher des détails sur les événements (par exemple, “Tentative de création d'une connexion en double”)
- les **noms d'événement**, qui contiennent des chaînes texte représentant les noms d'événement (par exemple, “La connexion existe déjà”)
- les **descriptions d'événements EDI**, qui contiennent des chaînes texte utilisées pour afficher des détails sur les événements EDI (par exemple, “Echec de la réconciliation de l'accusé de réception. Aucun ID d'activité trouvé pour les transactions de l'accusé de réception EDI) “)
- les **noms d'événement EDI**, qui contiennent des chaînes texte représentant les noms d'événement EDI (par exemple, “Echec de la réconciliation de l'accusé de réception”)
- le **texte d'événement étendu**, qui contient des chaînes de texte fournissant des informations supplémentaires sur les événements (par exemple, cause de l'événement et informations de résolution des incidents) ;

Pour télécharger un regroupement de ressources ou un autre fichier d'environnement local, procédez comme suit :

1. Pour chaque regroupement de ressources ou fichier d'environnement local, effectuez l'une des opérations suivantes :
   - Entrez le chemin et le nom du fichier.
   - Cliquez sur **Parcourir** pour naviguer jusqu'au fichier, puis sélectionnez-le.
2. A l'issue du téléchargement des fichiers, cliquez sur **Télécharger**.

Définition des règles sur les mots de passe

Vous pouvez définir une règle de mot de passe pour la communauté du concentrateur si vous avez l'intention d'utiliser des valeurs différentes de celles définies par défaut (par le système). La règle de mot de passe s'applique à tous les utilisateurs qui se connectent à la console de communauté.

Vous pouvez modifier les éléments suivants de la règle de mot de passe :

- La longueur minimale, qui représente le nombre minimum de caractères que doit comporter le mot de passe du partenaire. La valeur par défaut est 8 caractères.
- Le délai d'expiration, qui correspond au nombre de jours au bout duquel le mot de passe expire. La valeur par défaut est 30 jours.

- Le caractère unique, qui indique le nombre de mots de passe pouvant être consignés dans un fichier historique. Un partenaire ne peut pas utiliser un ancien mot de passe si celui-ci est présent dans le fichier historique. La valeur par défaut est 10 mots de passe.
- Le paramètre Caractères spéciaux qui, lorsqu'il est activé, indique que les mots de passe doivent contenir au moins trois des types de caractères spéciaux suivants :
  - majuscules ;
  - minuscules ;
  - caractères numériques ;
  - caractères spéciaux.

  Ce paramètre permet d'accroître le niveau de sécurité lorsque les mots de passe se composent de caractères anglais (ASCII). Par défaut, ce paramètre est désactivé. Il est recommandé de désactiver le paramètre Caractères spéciaux lorsque les mots de passe se composent de caractères internationaux. Il est possible en effet que les jeux de caractères non anglais ne contiennent pas les trois types de caractères obligatoires sur les quatre existants.

  Les caractères spéciaux pris en charge par le système sont les suivants : '#', '@', '$', '&', '+'.
- Le paramètre Vérification de la variation du nom, qui, lorsqu'il est activé, empêche l'utilisation de mots de passe qui sont une variante facilement extrapolable du nom d'utilisateur ou du nom complet de l'utilisateur. Ce paramètre est activé par défaut.

Pour modifier les valeurs par défaut :

1. Cliquez sur **Administrateur du concentrateur > Configuration de la console > Règle de mot de passe**. La page Règle de mot de passe s'affiche.
2. Cliquez sur l'icône **Edition**.
3. Remplacez les valeurs par défaut de votre choix par celles que vous souhaitez appliquer à votre règle de mot de passe.
4. Cliquez sur **Sauvegarder**.

Configuration des droits d'accès

Les droits d'accès sont des privilèges que doit posséder un utilisateur pour pouvoir accéder aux divers modules de la console.

Conditions d'attribution des droits d'accès aux utilisateurs

Avant de configurer les droits d'accès, il est très utile de comprendre comment ces droits sont accordés aux utilisateurs individuels. Les trois types d'entités figurant dans la communauté du concentrateur – l'administrateur du concentrateur, le partenaire interne et les partenaires externes – peuvent disposer d'un utilisateur administrateur. Lorsque vous créez un partenaire interne ou un partenaire, vous pouvez également créer l' l'utilisateur d'administration pour cette entité.

Remarque : Dans le cas du partenaire de l'opérateur du concentrateur, deux utilisateurs d'administration sont automatiquement créés lors de l'installation : un utilisateur administrateur et l'utilisateur administrateur du concentrateur.

Lorsque vous créez le partenaire (comme défini dans «Création des profils des partenaires», à la page 25), vous fournissez au partenaire des informations des connexion (nom et mot de passe de connexion). Une fois que le partenaire est connecté, il crée des utilisateurs supplémentaires au sein de l'organisation. Le partenaire crée également des groupes et affecte des utilisateurs à ces groupes. Par exemple, une organisation peut souhaiter créer un groupe composé de personnes chargées de superviser le volume de documents. Le partenaire crée alors un groupe Volume et y ajoute des utilisateurs.

Remarque : En tant qu'administrateur du concentrateur, vous pouvez également définir les utilisateurs et les groupes d'un partenaire.

L'utilisateur d'administration du partenaire va alors accorder des droits d'accès à ce groupe d'utilisateurs. Par exemple, l'utilisateur d'administration peut décider que le groupe Volume peut avoir accès uniquement aux rapports du volume de document ou d'analyse de document. Sur la page Détails du groupe, l'utilisateur d'administration peut activer le module de rapports de document, mais, ce faisant, il désactive tous les autres modules pour le groupe Volume.

Les paramètres que vous définissez sur la page Droits d'accès, en tant qu'administrateur du concentrateur, permettent de déterminer si un module est répertorié dans la page Détails du groupe.

Certains modules sont réservés à certains membres de la communauté du concentrateur (par exemple, les administrateurs du concentrateur). Par conséquent, même si vous les activez pour un partenaire, ils ne seront pas affichés sur la page Détails du groupe du partenaire.

Activation et désactivation des droits d'accès

Pourquoi et quand exécuter cette tâche

A partir de la page Liste des droits d'accès, vous pouvez déterminer les droits à accorder aux groupes d'utilisateurs en activant ou désactivant ces droits. Toutefois, vous ne pouvez pas définir de nouveaux droits d'accès.

Pour modifier les droits par défaut, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration de la console > Autorisations**. La liste des droits d'accès s'affiche.
2. Pour modifier les valeurs par défaut, procédez comme suit :
   a. Cliquez sur **Activé** ou sur **Désactivé** pour modifier le paramètre.
   b. Lorsque vous serez invité à confirmer la modification, cliquez sur **OK**.

Configuration de la valeur du délai d'attente de la console

La valeur d'expiration de la session par défaut de 30 minutes peut ne pas être acceptable dans les scénarios suivants :

- Les utilisateurs dans les environnements sécurisés peuvent avoir besoin de périodes d'expiration de session plus courtes pour assurer la sécurité. Ceci peut également s'appliquer dès lors qu'ils quittent leur machine et oublient de se déconnecter de la console.
- Les utilisateurs peuvent avoir besoin de périodes d'expiration de session plus longues s'ils répondent plus lentement que les utilisateurs typiques, pour des raisons d'accessibilité.

Pour définir la valeur d'expiration de la console WebSphere Partner Gateway, procédez comme suit :

1. Ouvrez la console WebSphere Application Server.
2. Accédez à **Serveurs** > **Serveurs d'application** > **bcgserver** > **Paramètres du conteneur Web** > **Conteneur Web** > **Gestion de la session**.
3. Dans la page **Gestion de la session**, sélectionnez **Définir expiration** dans la section **Expiration de la session**.
4. Entrez la valeur en minutes. La valeur par défaut est 30 minutes.
5. Cliquez sur **Appliquer**.

Chapitre 7. Définition des récepteurs

Ce chapitre explique comment paramétrer des récepteurs sur WebSphere Partner Gateway. Il contient les rubriques suivantes :

Remarque : Pour effectuer des modifications de configurations sur WebSphere Partner Gateway, vous devez toujours utiliser la même instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Présentation des récepteurs

Comme l'explique la section «Présentation du traitement des documents», à la page 12, le *Récepteur* est chargé d'accepter les documents entrants en provenance d'un transport donné. Il s'agit d'une instance de récepteur configuré pour un déploiement particulier.

Les documents reçus sur un récepteur du concentrateur peuvent provenir de partenaires externes (pour être remis au partenaire interne) ou de l'application dorsale du partenaire interne (pour être remis aux partenaires externes).

La figure 16, à la page 62 illustre un serveur WebSphere Partner Gateway sur lequel quatre récepteurs sont paramétrés. Deux des récepteurs (HTTP/S et FTP/S) reçoivent les documents émis par des partenaires. Ces deux récepteurs représentent un URI HTTP et un répertoire FTP. Vous fournissez à vos partenaires des informations sur ces récepteurs pour leur indiquer où ils doivent vous envoyer des documents. Les deux autres récepteurs (JMS et le répertoire de fichiers) concernent des documents émis par l'application dorsale du partenaire interne. Ces récepteurs représentent une file d'attente et un répertoire.

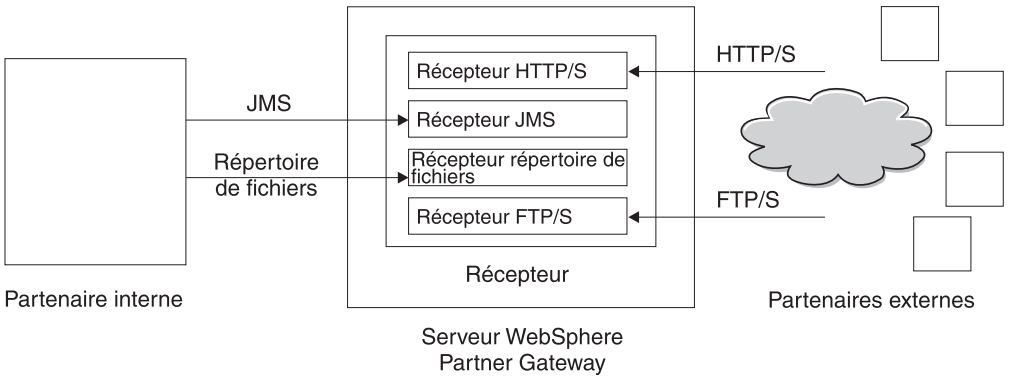


Figure 16. Transports et récepteurs associées

Vous devez définir au moins un récepteur pour chaque type de transport utilisé pour acheminer les documents qui seront envoyés au concentrateur. Par exemple, il doit exister un récepteur HTTP pour recevoir les documents envoyés par transport HTTP ou HTTPS. Si vos partenaires externes sont appelés à envoyer des documents via FTP, vous devez définir un récepteur FTP.

Si vous avez des exigences spéciales pour certains documents qui sont reçus, vous pouvez devoir configurer plus d'un récepteur pour un transport donné. Dans ce cas, vous indiquez ces exigences à vos partenaires et leur demandez d'envoyer ces documents à des adresses spécifiques afin que le traitement par le récepteur adéquat puisse être effectué.

Le composant Récepteur détecte l'arrivée des messages sur l'un des récepteurs. Pour déterminer si de nouveaux messages sont arrivés, certains récepteurs interrogent leurs transports à intervalles réguliers ou de façon planifiée. Les récepteurs WebSphere Partner Gateway basés sur une interrogation sont : JMS, FTP, SMTP, File et script FTP. Le récepteur HTTP/S utilise le rappel, c'est-à-dire qu'il reçoit une notification du transport lorsque des messages arrivent. Les transports définis par l'utilisateur peuvent être de type interrogation ou rappel.

Téléchargement de gestionnaires définis par l'utilisateur

Pourquoi et quand exécuter cette tâche

Vous pouvez modifier les points de configuration des récepteurs en spécifiant un gestionnaire. Le gestionnaire peut être fourni par WebSphere Partner Gateway ou il peut être défini par l'utilisateur. Cette section indique comment télécharger un gestionnaire défini par l'utilisateur. Suivez ses consignes uniquement pour les gestionnaires définis par l'utilisateur. Les gestionnaires fournis par WebSphere Partner Gateway sont prêts à l'utilisation.

Pour télécharger un gestionnaire, procédez comme suit :

1. Dans le menu principal, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Gestionnaires**.
2. Cliquez sur **Récepteur**.

   La liste des gestionnaires actuellement définis pour les récepteurs s'affiche. Notez que les gestionnaires fournis par WebSphere Partner Gateway sont associés à l'ID fournisseur **Produit**.
3. Dans la page Liste des gestionnaires, cliquez sur **Importer**.

4. Sur la page d'importation de gestionnaire, indiquez le chemin d'accès au fichier XML qui décrit le gestionnaire, ou utilisez **Parcourir** pour rechercher ce fichier XML.

Une fois le gestionnaire téléchargé, vous pouvez l'utiliser pour personnaliser les points de configuration des récepteurs.

Gestionnaires de prétraitement génériques

Le gestionnaire de configuration de prétraitement est disponible pour tous les types de récepteurs, mais n'est pas applicable aux récepteurs SMTP. Le tableau suivant décrit les attributs que vous pouvez définir pour un gestionnaire de prétraitement générique :

Tableau 2. Gestionnaire de prétraitement générique

Attributs	Description
Nom de l'empaquetage d'origine	Cet attribut indique l'empaquetage associé au document. La valeur doit correspondre à l'empaquetage indiqué dans la définition de documents.
Version du package d'origine	Cet attribut indique la version de l'empaquetage spécifié dans **Nom de l'empaquetage d'origine**. Par exemple, pour un document dont l'empaquetage est None, alors cette valeur sera N/A.
Nom du protocole d'origine	Cet attribut indique le protocole associé au document. La valeur doit correspondre au protocole indiqué dans la définition de documents.
Version du protocole d'origine	Cet attribut indique la version du protocole spécifié dans **Nom du protocole d'origine**.
Code du processus d'origine	Cet attribut indique le processus (type de document) associé à ce document. La valeur doit correspondre au type de document indiqué dans la définition de documents.
Version du processus d'origine	Cet attribut indique la version du processus spécifié dans **Code de processus d'origine**.
METADICTIONARY	Cet attribut indique le nom du dictionnaire auquel la définition de document est associée. Cette valeur doit correspondre au protocole spécifié dans la zone Nom de protocole d'origine.
METADOCUMENT	Cet attribut indique le nom de la définition de document associé à ce document. Cette valeur doit correspondre au processus spécifié dans la zone Code de processus d'origine.
METASYNTAX	Cet attribut indique la syntaxe du document qui sera traité dans ce récepteur ; les valeurs autorisées sont ediIchg (échange de données informatisé) / xml / rod (fichier à plat).
ENCODING	Cet attribut indique le codage de caractères du document. La valeur par défaut est ASCII.
BCG_BATCHDOCS	Cet attribut est défini sur **ON** si vous voulez que les documents soient traités dans un lot.
SenderId, ReceiverId	Cet attribut indique l'ID de récepteur et d'émetteur qui sont les ID métier des participants comme configuré dans leurs profils.

Définition de valeurs globales de transport

Pourquoi et quand exécuter cette tâche

Vous définissez les attributs globaux de transport qui s'appliquent aux récepteurs de script FTP. Si vous ne définissez pas de récepteurs de script FTP, cette section ne vous concerne pas.

1. Pour afficher la liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Cliquez sur le lien **Attributs de transport globaux**.
3. Si les valeurs par défaut sont correctes pour votre configuration, cliquez sur **Annuler**. Dans le cas contraire, suivez le reste des étapes de la section.
4. Cliquez sur l'icône **Edition** en regard de **Attributs globaux listés par catégorie**
5. Si nécessaire, modifiez les valeurs **Transport de scripts FTP** et **Récepteurs et destinations de scripts FTP**.

   Le transport de script FTP utilise un mécanisme de verrouillage qui empêche que plusieurs instances de script FTP n'accèdent au même récepteur au même moment. Lorsqu'un transport de script FTP est prêt à envoyer des documents, il demande ce verrouillage. Des valeurs par défaut sont fournies pour des éléments tels que la durée d'attente des instances de récepteur pour obtenir le verrouillage et le nombre de tentatives si le verrou est en cours d'utilisation. Vous pouvez utiliser ces valeurs par défaut ou les modifier. Pour modifier une ou plusieurs valeurs, saisissez-les. Vous pouvez modifier :

   - Les valeurs du **Transport de script FTP**
     - **Nombre de relances du verrouillage**, le nombre de tentatives du récepteur pour obtenir un verrouillage s'il est en cours d'utilisation. La valeur par défaut est 3.
     - **Intervalle entre relances de verrouillage (secondes)**, le temps d'attente entre les tentatives pour obtenir le verrouillage. La valeur par défaut est 260 secondes.
   - Valeurs des **Récepteurs et destinations de script FTP**
     - **Délai maximal de verrouillage (secondes)**, la durée pendant laquelle le récepteur peut maintenir le verrouillage. La valeur par défaut est 240 secondes.
     - **Délai maximal des files d'attente (secondes)**, la durée pendant laquelle le récepteur attendra dans une file d'attente pour obtenir le verrou. La valeur par défaut est 740 secondes.
6. Cliquez sur **Sauvegarder**.

Configuration d'un récepteur HTTP/S

Pourquoi et quand exécuter cette tâche

Le composant Récepteur intègre un servlet prédéfini appelé bcgreceiver, qui sert à recevoir les messages POST HTTP/S. Pour accéder aux messages reçus par le servlet, vous devez créer un ou plusieurs récepteurs HTTP.

La procédure suivante indique comment définir un récepteur HTTP/S.

1. Pour afficher la liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Dans la page Liste des récepteurs, cliquez sur **Créer le récepteur**.

Caractéristiques du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

Procédure

1. Attribuez un nom au récepteur. Par exemple, vous pourriez le nommer RécepteurHttp1. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.
2. Indiquez éventuellement le statut du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
3. Entrez éventuellement une description du récepteur.
4. Sélectionnez **HTTP/S** dans la liste des **transports**.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration du récepteur**, procédez comme suit :

1. Indiquez éventuellement le mode d'opération. Le mode d'opération définit la nature de la transmission. Par exemple, si vous voulez tester un échange de document avant de le mettre en production, vous devez entrer **Test**. La valeur par défaut est **Production**.
2. Indiquez l'identificateur URI du récepteur HTTP/S. Le nom doit commencer par **bcgreceiver**. Par exemple, vous pouvez entrer /bcgreceiver/Receiver. Les documents entrant dans le serveur via HTTP/S seront alors reçus dans /bcgreceiver/Receiver.
3. Pour authentifier un récepteur HTTP/S avec l'attribut d'en-tête, paramétrez l'indicateur **Activer l'authentification de base** sur vrai. La valeur par défaut est faux.
4. Si nécessaire, modifiez les valeurs pour **Transport HTTP/S**. Vous pouvez modifier :
   - **Délai d'attente synchrone maximum (secondes)**, pour indiquer le nombre de secondes pendant lequel une connexion synchrone peut rester ouverte. La valeur par défaut est 300 secondes.
   - **Nombre maximal de connexions synchrones simultanées**, pour indiquer le nombre de connexions synchrones autorisées par le système. La valeur par défaut est 100 connexions.

Remarque : Vous pouvez éditer les valeurs **Sync Routing**.

Gestionnaires

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le gestionnaire de fractionnement approprié dans le point de configuration Preprocess.

Si vous envisagez d'envoyer ou de recevoir certains types de documents métiers (RosettaNet, cXML, SOAP et AS2) par le biais d'un échange synchrone, indiquez un récepteur pour le protocole associé dans le point de configuration SyncCheck.

Vous pouvez également modifier les points de configuration Postprocess pour le récepteur.

Pour modifier un point de configuration, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Configuration d'un récepteur FTP

Pourquoi et quand exécuter cette tâche

Un récepteur FTP interroge votre serveur FTP selon un intervalle prédéfini, pour rechercher de nouveaux documents.

La procédure suivante indique comment définir un récepteur FTP.

Procédure

1. Pour afficher la liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Dans la page Liste des récepteurs, cliquez sur **Créer le récepteur**.

Résultats

Caractéristiques du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

Procédure

1. Attribuez un nom au récepteur. Par exemple, vous pourriez le nommer RécepteurFTP1. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.
2. Indiquez éventuellement l'état du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
3. Entrez éventuellement une description du récepteur.
4. Sélectionnez **Répertoire FTP** dans la liste des **transports**.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration du récepteur**, procédez comme suit :

1. Dans la zone **Répertoire principal FTP**, indiquez le répertoire racine du serveur FTP. Pour router les documents, le gestionnaire de documents interroge automatiquement les sous-répertoires du partenaire dans le répertoire racine FTP. Cette zone est obligatoire. Pour plus d'informations sur la configuration d'un répertoire pour un serveur FTP, reportez-vous à la section «Configuration du serveur FTP pour la réception de documents», à la page 35.

   Remarque : Saisissez le chemin d'accès au répertoire FTP racine. N'incluez pas les sous-répertoires du partenaire.
2. Entrez éventuellement une valeur dans la zone **Intervalle de fichier non modifié** pour indiquer le nombre de secondes durant lesquelles la taille du fichier ne devra pas changer, tant que le gestionnaire de documents n'aura pas récupéré le document pour le traiter. Cet intervalle donne l'assurance que la

transmission du document est terminée (qu'il n'est plus en transit) lorsque le gestionnaire de documents procède à son extraction. La valeur par défaut est 3 secondes.

3. Entrez éventuellement une valeur dans la zone **Nombre d'unités d'exécution**, pour indiquer le nombre de documents que le gestionnaire de documents traitera simultanément. Il est recommandé de conserver la valeur par défaut (1).
4. Entrez éventuellement une valeur dans la zone **Exclure l'extension de fichier** pour indiquer les types de documents que le gestionnaire de documents devra ignorer (c'est-à-dire exclure du traitement) s'il trouve des documents correspondants dans le répertoire FTP. Par exemple, si vous souhaitez que le gestionnaire de documents ignore les fichiers d'un tableur, indiquez l'extension correspondante. Cliquez ensuite sur **Ajouter**. L'extension est alors ajoutée à la liste des extensions de fichier à ignorer. Par défaut, aucun type de fichier n'est exclu.

   Remarque : N'utilisez pas de point avant l'extension de nom de fichier (par exemple : .exe or . txt). Indiquez uniquement les caractères qui composent l'extension.

Gestionnaires

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le gestionnaire de fractionnement approprié dans le point de configuration Preprocess.

Pour modifier le point de configuration Preprocess, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Configuration d'un récepteur SMTP (POP3)

Pourquoi et quand exécuter cette tâche

Un récepteur SMTP interroge votre serveur de courrier POP3 (selon la planification précisée) pour rechercher de nouveaux documents.

La procédure suivante indique comment définir un récepteur SMTP (POP3).

Procédure

1. Pour afficher la page liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Dans la page Liste des récepteurs, cliquez sur **Créer le récepteur**.

Résultats

Caractéristiques du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

Procédure

1. Attribuez un nom au récepteur. Par exemple, vous pourriez le nommer Récepteur1POP3. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.

2. Indiquez éventuellement l'état du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
3. Entrez éventuellement une description du récepteur.
4. Sélectionnez **POP3** dans la liste des **transports**.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration du récepteur**, procédez comme suit :

Procédure

1. Indiquez éventuellement le mode d'opération. Le mode d'opération définit la nature de la transmission. Par exemple, si vous voulez tester un échange de document avant de le mettre en production, vous devez entrer **Test**. La valeur par défaut est **Production**.
2. Indiquez l'emplacement du serveur POP3 où le courrier est remis. Par exemple une adresse IP.
3. Indiquez un numéro de port (facultatif). Si vous n'en indiquez pas, c'est la valeur 110 qui est utilisée.
4. Indiquez l'ID utilisateur et le mot de passe requis pour accéder au serveur de courrier, dans la mesure où ceux-ci sont obligatoires.
5. Le **Nombre d'unités d'exécution** est en mode lecture seule. Cela indique le nombre de documents que le gestionnaire de documents peut traiter simultanément.

Planification

Pourquoi et quand exécuter cette tâche

Dans la section **Planification**, procédez comme suit :

1. Sélectionnez **Planification en fonction de l'intervalle** ou **Planification en fonction du calendrier**.
2. Selon le cas, appliquez les étapes suivantes :
   - Si vous avez sélectionné **Planification en fonction de l'intervalle**, sélectionnez le nombre de secondes qui doivent s'écouler avant que le serveur POP3 ne soit de nouveau interrogé (ou acceptez la valeur par défaut). Si vous avez sélectionné la valeur par défaut, le serveur POP3 est interrogé toutes les 5 secondes.
   - Si vous sélectionnez **Planification en fonction du calendrier**, choisissez le type de planification (**Planification quotidienne**, **Planification hebdomadaire**, ou **Planification personnalisée**).
     - Si vous sélectionnez **Planification quotidienne**, choisissez l'heure de la journée (heures et minutes) à laquelle le serveur POP3 doit être interrogé.
     - Si vous sélectionnez **Planification hebdomadaire**, choisissez un ou plusieurs jours de la semaine, en plus de l'heure.
     - Si vous sélectionnez **Planification personnalisée**, choisissez l'heure de la journée puis **Intervalle** ou **Sélection des jours** pour indiquer la semaine et le mois. Dans **Intervalle**, indiquez une date de début et de fin Par exemple, vous pouvez cliquer sur **Lun** et **Ven**, si vous souhaitez que le

serveur soit interrogé à une certaine heure uniquement les jours ouvrés. L'option **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.

Gestionnaires

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le gestionnaire de fractionnement approprié dans le point de configuration Preprocess.

Pour modifier le point de configuration Preprocess, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Configuration d'un récepteur JMS

Pourquoi et quand exécuter cette tâche

Un récepteur JMS interroge une file d'attente JMS (selon la planification précisée) pour rechercher de nouveaux documents.

La procédure suivante indique comment définir un récepteur JMS.

1. Pour afficher la liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Dans la page Liste des récepteurs, cliquez sur **Créer le récepteur**.

Remarque : Pour plus d'informations sur la configuration des bibliothèques d'exécution afin que les fichiers JAR requis de WebSphere MQ soient visibles pour WebSphere Partner Gateway, reportez-vous à la section «Configuration des bibliothèques d'exécution», à la page 42.

Caractéristiques du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

1. Attribuez un nom au récepteur. Par exemple, vous pourriez le nommer RécepteurJMS1. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.
2. Indiquez éventuellement l'état du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
3. Entrez éventuellement une description du récepteur.
4. Sélectionnez **JMS** dans la liste **Transport**.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration du récepteur**, procédez comme suit :

1. Indiquez éventuellement le **Type d'opération**. Le type d'opération définit la nature de la transmission. Par exemple, si vous voulez tester un échange de document avant de le mettre en production, vous devez entrer **Test**. La valeur par défaut est *Production*.

2. Indiquez l'**URL du fournisseur JMS**. Elle doit correspondre à la valeur indiquée (le chemin de système de fichiers vers le fichier bindings) lors de la configuration de WebSphere Partner Gateway pour JMS (étape 5, à la page 40. Vous pouvez également indiquer le sous-dossier pour le contexte JMS, comme partie de l'URL de fournisseur JMS.

   Par exemple, et sans le contexte JMS, vous entreriez `c:/temp/JMS`. Avec le contexte JMS, vous entreriez `c:/temp/JMS/JMS` .
3. Indiquez l'**ID utilisateur** et le **Mot de passe** requis pour accéder à la file d'attente JMS, dans la mesure où ceux-ci sont obligatoires.
4. Entrez une valeur pour le **Nom de file d'attente JMS**. Cette zone est obligatoire. Le nom doit correspondre à celui que vous avez indiqué par la commande `define q`, lors de la création du fichier de liaison, le fichier de liaison (étape 4, à la page 41).

   Si vous avez entré le sous-dossier pour le contexte JMS à l'étape 2, n'entrez ici que le nom de file d'attente (par exemple `inQ`). Dans le cas contraire (si vous n'avez pas indiqué le sous-dossier du contexte JMS dans l'URL du fournisseur JMS), indiquez ici le sous-dossier, devant le nom de la fabrique (par exemple `JMS/inQ`).
5. Entrez une valeur pour le **Nom de la fabrique JMS**. Cette zone est obligatoire. Le nom doit correspondre à celui que vous avez indiqué par la commande `define qcf`, lors de la création du fichier de liaison (étape 4, à la page 41).

   Si vous avez entré le sous-dossier pour le contexte JMS à l'étape 2, n'entrez ici que le nom de fabrique (par exemple `Hub`). Dans le cas contraire (si vous n'avez pas indiqué le sous-dossier du contexte JMS dans l'URL du fournisseur JMS), indiquez ici le sous-dossier, devant le nom de la fabrique (par exemple `JMS/Hub`).
6. Entrez éventuellement le **Package URL du fournisseur**.
7. Entrez le **Nom de la fabrique JNDI**. Cette zone est obligatoire. Vous utiliserez probablement la valeur com.sun.jndi.fscontext.RefFSContextFactory, si vous définissez votre configuration JMS pour WebSphere MQ comme indiqué dans la section «Configuration du concentrateur pour le protocole de transport JMS», à la page 39.
8. Entrez le **Nom d'utilisateur JMS** et le **Mot de passe JMS**.
9. Entrez éventuellement une valeur dans la zone **Délai d'inactivité**, pour indiquer le nombre de secondes durant lesquelles le récepteur vérifiera la présence de documents sur le serveur JMS. Cette zone est facultative.
10. Entrez éventuellement une valeur dans la zone **Nombre d'unités d'exécution**, pour indiquer le nombre de documents que le gestionnaire de documents traitera simultanément. Il est recommandé de conserver la valeur par défaut (1).

Par exemple, pour configurer un récepteur JMS analogue à celui de l'exemple dans «Configuration du concentrateur pour le protocole de transport JMS», à la page 39, vous indiquerez les valeurs suivantes :

1. Entrez la valeur **RécepteurJMS** dans la zone **Nom du récepteur** ;
2. Entrez l'une des valeurs suivantes dans la case **URL du fournisseur JMS** :
   - **file:///C:/TEMP/JMS/JMS** pour Windows.
   - **file:///opt/temp** pour UNIX.
3. **enFA** dans la zone **Nom de file d'attente JMS** ;
4. **Hub** dans la zone **Nom de la fabrique JMS**.

Gestionnaires

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le gestionnaire de fractionnement approprié dans le point de configuration Preprocess.

Pour modifier des points de configuration, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Configuration d'un récepteur Répertoire de fichiers

Pourquoi et quand exécuter cette tâche

Un récepteur Répertoire de fichiers interroge un répertoire selon un intervalle prédéfini, pour rechercher de nouveaux documents.

La procédure suivante indique comment définir un tel récepteur.

1. Pour afficher la liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Dans la page Liste des récepteurs, cliquez sur **Créer le récepteur**.

Caractéristiques du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

1. Attribuez un nom au récepteur. Par exemple, vous pourriez le nommer RécepteurFichier1. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.
2. Indiquez éventuellement l'état du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
3. Entrez éventuellement une description du récepteur.
4. Sélectionnez **Répertoire de fichiers** dans la liste **Transport**.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration du récepteur**, procédez comme suit :

1. Entrez une valeur dans la zone **Chemin principal du document** pour indiquer le répertoire dans lequel les documents seront reçus.

   Si le répertoire principal n'existe pas, alors un nouveau répertoire est créé pour le récepteur. Mais, si le répertoire principal existe déjà, alors il sera utilisé par le récepteur. Cela n'est applicable qu'à partir de WebSphere Partner Gateway 6.1.1.

   Le préfixe `file://` est facultatif.

   Par exemple, si vous voulez spécifier le répertoire `c:\wpg\receivers\file1` comme Chemin principal du document, entrez `c:\wpg\receivers\file1` ou`file://c:\wpg\receivers\file1`.
2. Renseignez éventuellement la zone **Intervalle d'interrogation** pour indiquer la fréquence de recherche de nouveaux documents dans le répertoire. Si vous n'indiquez aucune valeur, le répertoire sera interrogé toutes les 5 secondes.
3. Entrez éventuellement une valeur dans la zone **Intervalle de fichier non modifié** pour indiquer le nombre de secondes durant lesquelles la taille du

fichier ne devra pas changer, tant que le gestionnaire de documents n'aura pas récupéré le document pour le traiter. Cet intervalle donne l'assurance que la transmission du document est terminée (qu'il n'est plus en transit) lorsque le gestionnaire de documents procède à son extraction. La valeur par défaut est 3 secondes.

4. Entrez éventuellement une valeur dans la zone **Nombre d'unités d'exécution**, pour indiquer le nombre de documents que le gestionnaire de documents traitera simultanément. Il est recommandé de conserver la valeur par défaut (1).

Gestionnaires

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le gestionnaire de fractionnement approprié dans le point de configuration Preprocess.

Pour modifier le point de configuration Preprocess, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Configuration d'un récepteur de script FTP

Pourquoi et quand exécuter cette tâche

Un récepteur de script FTP est un récepteur d'interrogation qui s'exécute d'après la planification que vous avez définie. Le comportement d'un récepteur de script FTP est régi par un script de commande FTP.

Contrairement au récepteur FTP qui interroge un répertoire sur le serveur FTP, le récepteur de script FTP interroge les répertoires d'un autre serveur (par exemple un VAN).

Remarque :

1. Si la base de données est en panne et que Verrouiller l'utilisateur est configuré sur "Oui", le récepteur de script peut ne pas fonctionner car il ne pourra pas obtenir le verrou de la base de données.
2. Le partenaire doit s'assurer que le document est complet afin que le récepteur de script FTP puisse le recevoir. Pour cela, le serveur FTP peut conserver le document verrouillé jusqu'à ce que le document soit complet ou le partenaire enregistre le document dans un répertoire temporaire, puis déplace le document complet vers le répertoire actuellement utilisé par le récepteur de script FTP.

Création du script FTP

Pourquoi et quand exécuter cette tâche

Les serveurs FTP peuvent avoir certaines exigences spécifiques pour les commandes qu'ils acceptent. Pour utiliser un récepteur de script FTP, vous devez créer un fichier incluant toutes les commandes FTP exigées par le serveur FTP sur lequel vous vous connectez. Vous devez vous procurer ces informations auprès de l'administrateur du serveur FTP.

1. Créez un script pour les récepteurs de façon à indiquer les actions que vous souhaitez effectuer. Le script suivant est un exemple pour se connecter au serveur FTP indiqué (le nom et le mot de passe étant précisés), passer au répertoire indiqué sur le serveur FTP et récupérer tous ces fichiers dans ce répertoire :

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

   Lorsque le récepteur est mis en service, les paramètres fictifs (par exemple %BCGSERVERIP%) sont remplacés par les valeurs que vous avez saisies lors de la création d'une instance spécifique de récepteur de script FTP. Dans cet exemple, %BCGOPTION% est le nom du répertoire dans la commande `cd`. Les paramètres de script et les zones de récepteur de script FTP qui leur sont associées sont indiqués dans le tableau 3:

Tableau 3. Mappage des paramètres de script avec les entrées de zone de récepteur de script FTP

Paramètre de script	**Informations des zones de récepteur de script FTP**
%BCGSERVERIP%	IP serveur
%BCGUSERID%	ID utilisateur
%BCGPASSWORD%	Mot de passe
%BCGOPTIONx%	Option*x*, sous **Attributs définis par l'utilisateur**

2. Enregistrez le fichier.

Commandes de script FTP

Vous pouvez utiliser les commandes suivantes pour créer le script :

- ascii, binary, passive, epsv

  Ces commandes ne sont pas envoyées au serveur FTP. Elles modifient le mode de transfert (ascii, binary ou passive) vers le serveur FTP.

- cd

  Cette commande permet de passer au répertoire indiqué.

- delete

  Cette commande supprime un fichier du serveur FTP.

- get

  Cette commande utilise un seul argument, le nom du fichier à récupérer du système éloigné. Le fichier requis est ensuite transféré dans WebSphere Partner Gateway. N'utilisez cette commande que si vous récupérez un seul fichier dont le nom est connu. Sinon, utilisez la commande `mget`, avec des caractères génériques.

- getdel

  Cette commande est comparable à la commande `get`, mais le fichier est supprimé du système distant lorsque WebSphere Partner Gateway le récupère pour le traiter.

- mget

  Cette commande utilise un seul argument, qui décrit un groupe de fichiers à extraire. La description peut inclure les caractères génériques standard ('*' et '?'). Un ou plusieurs fichiers sont ensuite extraits du système éloigné.
- mgetdel

  Cette commande utilise un seul argument, qui décrit un groupe de fichiers à extraire et à supprimer du serveur FTP. La description peut inclure les caractères génériques standard (* et ?). Un ou plusieurs fichiers sont ensuite extraits et supprimés du système éloigné.
- mkdir

  Cette commande permet de créer un répertoire sur le serveur FTP.
- mputren

  Cette commande est une combinaison des commandes mput et rename. Par exemple, la commande **mputren * *.tmp /destination/*** copie le fichier de la destination vers le serveur FTP avec l'extension **.tmp**. Une fois le processus de téléchargement du document terminé, le fichier est renommé et copié dans le répertoire **/destination** sur la racine FTP.
- open

  Cette commande utilise trois paramètres : l'adresse IP du serveur FTP, le nom de l'utilisateur et un mot de passe. Ces paramètres correspondent aux variables %BCGSERVERIP%, %BCGUSERID% et %BCGPASSWORD%.

  Par conséquent, la première ligne du script de récepteur FTP doit être :

  ```
  open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
  ```
- quit

  Cette commande permet de fermer une connexion existante à un serveur FTP.
- quote

  Cette commande indique que tout élément après la commande QUOTE doit être envoyé en tant que commande au système éloigné. Elle permet d'envoyer, à un serveur FTP éloigné, des commandes qui ne seraient pas définies dans le protocole FTP standard.
- rename

  Cette commande renomme un fichier sur le serveur FTP.
- rmdir

  Cette commande permet de supprimer un répertoire du serveur FTP.
- site

  Cette commande peut servir à lancer des commandes spécifiques à un site sur un système éloigné. Celui-ci détermine si le contenu de la commande est valide.

Caractéristiques du récepteur

Pourquoi et quand exécuter cette tâche

La procédure suivante indique ce dont vous avez besoin pour spécifier un récepteur de script FTP.

1. Pour afficher la liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Dans la page Liste des récepteurs, cliquez sur **Créer le récepteur**.

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

1. Attribuez un nom au récepteur. Par exemple, vous pourriez le nommer RécepteurScriptFTP1. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.
2. Indiquez éventuellement l'état du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
3. Entrez éventuellement une description du récepteur.
4. Sélectionnez **Script FTP** dans la liste Transport.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration du récepteur**, procédez comme suit :

Procédure

1. Indiquez éventuellement le **Mode d'opération**. Le Type d'opération définit la nature de la transmission. Par exemple, si vous voulez tester un échange de document avant de le mettre en production, vous devez entrer **Test**. La valeur par défaut est **Production**.
2. Entrez l'adresse **IP serveur** du serveur FTP auquel vous vous connectez. La valeur indiquée ici remplacera %BCGSERVERIP% lorsque le script FTP sera exécuté.
3. Indiquez l'**ID utilisateur** et le **Mot de passe** pour accéder au serveur. Les valeurs indiquées ici remplaceront %BCGUSERID% et %BCGPASSWORD% lorsque le script FTP sera exécuté.
4. Pour le **Mode FTPS**, sélectionnez *Oui* ou *Non* pour indiquer si le récepteur fonctionnera en mode SSL (Secure Sockets Layer). Si oui, vous devrez échanger des certificats avec vos partenaires, comme indiqué au Chapitre 13, «Activation de la sécurité pour les échanges de documents», à la page 257.
5. Chargez le fichier script en procédant comme suit :
   a. Cliquez sur **Charger un fichier script**.
   b. Entrez le nom du fichier contenant le script de traitement des documents, ou utilisez **Parcourir** pour accéder au fichier.
   c. Sélectionnez le **Type de codage de fichier script**.
   d. Cliquez sur **Charger le fichier** pour charger le fichier de script dans la zone de texte **Fichier de script actuellement chargé**.
   e. Si le fichier script est celui que vous souhaitez utiliser, cliquez sur **Sauvegarder**.
   f. Cliquez sur **Fermer la fenêtre**.
6. Dans **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion pourra rester ouverte en l'absence de trafic.
7. Dans la zone **Verrouiller l'utilisateur**, indiquez si le récepteur demandera un verrouillage pour qu'aucune autre instance d'un récepteur de script FTP ne puisse accéder simultanément au même répertoire du serveur FTP.

Résultats

Remarque : Les valeurs **Attributs de script FTP globaux** sont déjà renseignées et ne peuvent être modifiées dans cette page. Pour les modifier, utilisez la page Attributs de transport globaux, de la façon indiquée dans la section « Définition de valeurs globales de transport», à la page 64.

Attributs définis par l'utilisateur

Pourquoi et quand exécuter cette tâche

Si vous souhaitez indiquer des attributs supplémentaires, exécutez les étapes ci-après. La valeur entrée pour l'option remplacera %BCGOPTION*x*% lorsque le script FTP sera exécuté (*x* correspond au numéro de l'option).

1. Cliquez sur **Nouveau**.
2. Saisissez une valeur en regard de **Option 1**.
3. Si vous souhaitez spécifier d'autres attributs, cliquez de nouveau sur **Nouveau** et saisissez une valeur.
4. Répétez l'étape 3 aussi souvent que nécessaire pour définir tous les attributs.

Prenons un exemple de script FTP :

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

Dans ce cas, %BCGOPTION% est un nom de répertoire.

Planification

Indiquez si vous souhaitez procéder à une planification en fonction d'un intervalle ou du calendrier.

- Si vous avez sélectionné **Planification en fonction de l'intervalle**, sélectionnez le nombre de secondes qui doivent s'écouler avant que le serveur FTP ne soit interrogé (ou acceptez la valeur par défaut).
- Si vous sélectionnez **Planification en fonction du calendrier**, choisissez le type de planification (**Planification quotidienne**, **Planification hebdomadaire**, ou **Planification personnalisée**).
  - Si vous sélectionnez **Planification quotidienne**, choisissez l'heure de la journée à laquelle le serveur FTP doit être interrogé.
  - Si vous sélectionnez **Planification hebdomadaire**, choisissez un ou plusieurs jours de la semaine, en plus de l'heure.
  - Si vous sélectionnez **Planification personnalisée**, choisissez l'heure de la journée puis **Intervalle** ou **Sélection des jours** pour indiquer la semaine et le mois. Dans **Intervalle**, indiquez une date de début et de fin Par exemple, vous pouvez cliquer sur **Lun** et **Ven**, si vous souhaitez que le serveur soit interrogé à une certaine heure uniquement les jours ouvrés. L'option **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.

Gestionnaires

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le gestionnaire de fractionnement approprié dans le point de configuration Preprocess.

Pour modifier le point de configuration Preprocess, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Configuration d'un récepteur SFTP

Pourquoi et quand exécuter cette tâche

Cette section présente des détails pour utiliser SFTP (SSH-FTP) en tant que protocole de transfert des documents métier. It garantit confidentialité, authentification et intégrité des messages des données.

Le composant récepteur SFTP interroge le serveur SFTP, extrait les fichiers du serveur SFTP et les stocke dans le répertoire local. Le répertoire du serveur SFTP qui est interrogé est nommé répertoire d'événements distants. Le répertoire dans lequel les fichiers récupérés sont stockés est nommé répertoire d'événements locaux. La procédure suivante indique comment définir un récepteur SFTP.

La procédure suivante indique comment définir un récepteur SFTP.

1. Pour afficher la liste des récepteurs, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Dans la page Liste des récepteurs, cliquez sur **Créer le récepteur**.

Création d'un récepteur SFTP sur les systèmes sur lesquels la sécurité administrative WAS est activée

Pourquoi et quand exécuter cette tâche

WebSphere Partner Gateway 6.2.1 facilite la création de récepteurs SFTP sur les systèmes sur lesquels la sécurité administrative WAS est activée. Cette rubrique décrit une tâche permettant de créer le récepteur SFTP sur un système sur lequel la sécurité administrative WAS est activée :

1. Dans la console WebSphere Partner Gateway, accédez à **Administration du système** > **Administration de la console** > **Sécurité administrative WAS**.
2. Sur cet écran, définissez la valeur de l'attribut **bcg.RMIConnector.security.enabled** sur vrai (true). Remarquez que la valeur de cet attribut est "faux" (false) par défaut.
3. Définissez les autres attributs sur cet écran comme illustré dans la procédure suivante :
   a. **bcg.RMIConnector.security.enabled** : définissez cet attribut sur "true" (vrai) uniquement si la **Sécurité administrative WAS** est activée. Si vous ne définissez pas cette propriété sur "true" (vrai), vous ne pourrez pas créer de récepteur SFTP.
   b. **bcg.RMIConnector.security.enabled** : si cet attribut est défini sur "true" (vrai), les attributs suivants doivent être obligatoirement définis :
      - **bcg.RMIConnector.host.name** : entrez le nom d'hôte ou l'adresse IP du gestionnaire de déploiement.
      - **bcg.RMIConnector.portNumber** : indiquez le PORT D'AMORCE du gestionnaire de déploiement.
      - **bcg.RMIConnector.admin.userId** : définissez cet attribut sur l'ID utilisateur qui est utilisé pour la sécurité administrative WAS.
      - **bcg.RMIConnector.admin.password** : définissez cet attribut sur le mot de passe qui est utilisé pour la sécurité administrative WAS.
4. Cliquez sur **Sauvegarder**.

Caractéristiques du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

Procédure

1. Attribuez un nom au récepteur. Par exemple, vous pourriez le nommer SFTPReceiver1. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.
2. Indiquez éventuellement l'état du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
3. Entrez éventuellement une description du récepteur.
4. Sélectionnez **SFTP** dans la liste **Transport**.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Dans la section **Caractéristiques du récepteur**, procédez comme suit :

Procédure

1. Entrez le **Mode d'opération**. Sélectionnez-le dans la liste ou cliquez sur **Nouveau** pour en créer un.
2. Dans la zone **IP de l'hôte SFTP**, entrez l'adresse URL du serveur SFTP. Vous pouvez saisir 100 caractères maximum. Vous pouvez aussi entrer les adresses IP, IPv4 et IPv6.
3. Entrez le **Numéro de port**. La valeur par défaut est 22.
4. **Répertoire d'événements distant** est le répertoire à partir duquel l'adaptateur télécharge les fichiers d'événements à partir du site SFTP.
5. Dans la zone **Type d'authentification**, sélectionnez le **Nom utilisateur/ mot de passe** ou l'authentification de **Clé privée**.
6. Entrez l'**ID utilisateur** et le **Mot de passe** pour nom utilisateur/mot de passe. Si le type d'authentification est l'authentification de clé privée, entrez le nom d'utilisateur, le fichier de clé privée et la phrase de passe. Le fichier de clés privé doit être au format OpenSSH.
7. Dans l'**Intervalle d'interrogation SFTP**, entrez la durée en millisecondes. Il s'agit de la durée pendant laquelle l'adaptateur attend en interrogeant le répertoire d'événement local. Cette durée et la durée nécessaire pour traiter les documents dans le répertoire d'événement local s'appellent les cycles d'interrogation.
8. **Quantité d'interrogations** est le nombre d'événements (documents) que le récepteur traite au cours de chaque cycle d'interrogation.
9. **Intervalle entre les tentatives** est la durée d'attente de l'adaptateur, en millisecondes, entre les tentatives d'établir une nouvelle connexion après une erreur au cours d'opérations entrantes.
10. **Nombre maximum de relances** est le nombre de fois où l'adaptateur tente de rétablir une connexion entrante après une erreur.
11. **Codage EIS** est le codage du serveur FTP. Utilisez cette valeur pour définir le codage de la connexion de contrôle du serveur FTP.

12. L'option **Activer l'authentification du serveur** peut être activée pour authentifier le serveur auquel la connexion est établie. Si l'authentification du serveur est activée, entrez le chemin du fichier de clés hôte. Le fichier de clés hôte doit être au format OpenSSH.
13. Configurez les gestionnaires si nécessaire.
14. Cliquez sur **Sauvegarder** pour sauvegarder le configuration.

Gestionnaires

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le gestionnaire de fractionnement approprié dans le point de configuration Preprocess.

Pour modifier le point de configuration Preprocess, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Configuration d'un récepteur pour un transport défini par l'utilisateur

Pourquoi et quand exécuter cette tâche

Si vous paramétrez un récepteur pour un transport défini par l'utilisateur, les noms de fichiers et autres informations sont précisés dans le fichier décrivant le transport.

Procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteur**.
2. Cliquez sur **Gérer les types de transport**.
3. Entrez le nom d'un fichier XML définissant le mode de transport (ou naviguez jusqu'au fichier en cliquant sur le bouton **Parcourir**).
4. Cliquez sur **Télécharger**.

   Remarque : Dans la liste des récepteurs, vous pouvez également supprimer un type de transport défini par l'utilisateur. Vous ne pouvez pas supprimer un transport fourni par WebSphere Partner Gateway. Vous ne pouvez pas non plus supprimer un transport défini par l'utilisateur une fois qu'il a été utilisé pour la création d'un récepteur.
5. Cliquez sur **Créer le récepteur**.
6. Attribuez un nom au récepteur. Cette zone est obligatoire. Le nom que vous entrez ici s'affichera dans la liste des récepteurs.
7. Indiquez éventuellement l'état du récepteur. L'état par défaut est **Activé**. Un récepteur activé est prêt à accepter des documents. Un récepteur désactivé ne peut pas accepter de documents.
8. Entrez éventuellement une description du récepteur.
9. Sélectionnez dans la liste un transport défini par l'utilisateur.
10. Renseignez les zones (qui seront uniques pour chaque transport défini par l'utilisateur).
11. Pour modifier des points de configuration pour ce récepteur, consultez la section « Modification des points de configuration», à la page 80. Sinon, cliquez sur **Sauvegarder**.

Modification des points de configuration

Le nombre de points de configuration disponibles et de gestionnaires associés varie en fonction du type de récepteur défini. Par exemple, le point de configuration SyncCheck n'est disponible qu'avec les récepteurs HTTP/S et JMS.

Pour certains protocoles métiers (RosettaNet, cXML, SOAP et AS2) impliqués dans les échanges synchrones, vous devez spécifier un gestionnaire pour le point de configuration SyncCheck. Vous pouvez également modifier la façon dont les récepteurs traitent les documents, en appliquant un gestionnaire téléchargé défini par l'utilisateur (ou un processus fourni par le produit) aux autres points de Preprocess et Postprocess de la cible.

Pour appliquer un gestionnaire écrit par l'utilisateur à ces points de configuration, vous devez d'abord télécharger le gestionnaire, comme décrit dans la section « Téléchargement de gestionnaires définis par l'utilisateur», à la page 62. Vous pouvez également utiliser un gestionnaire fourni par le produit, déjà disponible et qu'il n'est pas nécessaire de télécharger.

Preprocess

Le gestionnaire de configuration Preprocess est disponible pour tous les types de récepteurs, mais n'est pas applicable aux récepteurs SMTP.

Attributs Preprocess

Le tableau 4 décrit les attributs que vous pouvez définir dans un gestionnaire Preprocess, ainsi que les gestionnaires de fractionnement auxquels s'appliquent ces attributs.

Les attributs ROD pris comme exemple dans ce tableau correspondent à ceux utilisés dans « Exemple ROD vers EDI», à la page 378. Dans cet exemple, les attributs ROD sont contenus dans la mappe S_DT_ROD_TO_EDI.eif, qui comprend les définitions de documents suivantes :

- Package : None (version N/A)
- Protocole : ROD_TO_EDI_DICT (version TOUTE)
- Flux de documents : DTROD-TO-EDI_ROD (version TOUTE)

Le métadictionnaire et le métadocument ROD associés à ce flux sont ROD_TO_EDI_DICT et DTROD-TO-EDI_ROD.

Tableau 4. Attributs de gestionnaire de fractionnement

Attribut	Description	Gestionnaire de fractionnement
Encoding	Le codage des caractères du document. La valeur par défaut est ASCII.	ROD Generic XML EDI

Tableau 4. Attributs de gestionnaire de fractionnement (suite)

Attribut	Description	Gestionnaire de fractionnement
BATCHDOCS	Lorsque l'attribut BCG_BATCHDOCS est activé (on), l'utilitaire de fractionnement ajoute des ID de traitement aux documents après les avoir séparés. Si les documents sont transformés en transactions EDI pour être enveloppées, l'enveloppeur utilise ces ID de traitement pour s'assurer que les transactions sont (si possible) mises dans le même EDI avant d'être livrées. Notez que pour cela, l'enveloppeur doit avoir l'attribut de traitement par lots (batching) défini sur **On** (la valeur par défaut). Voir «Mode de traitement par lot», à la page 198.	ROD Generic XML
Nom de l'empaquetage d'origine	L'empaquetage associé au document. La valeur doit correspondre au package indiqué dans la définition de documents. Par exemple, pour un document dont le package est None, la valeur doit être **None**.	ROD Generic
Version du package d'origine	La version du package indiquée dans le Nom du package d'origine. Par exemple, pour un document dont le package est None, la valeur doit être **N/A**.	ROD Generic
Nom du protocole d'origine	Le protocole associé au document. La valeur doit correspondre au protocole indiqué dans la définition de documents. Par exemple, pour un document ROD, cette valeur doit être **ROD-TO-EDI_DICT**.	ROD Generic
Version du protocole d'origine	La version du protocole indiquée dans le Nom du package d'origine. Par exemple, pour le protocole ROD-TO-EDI_DICT, la valeur doit être **TOUT**.	ROD Generic
Code du processus d'origine	Le processus (type de document) associé à ce document. La valeur doit correspondre au type de document indiqué dans la définition de documents. Par exemple, pour un document ROD, cette valeur doit être DTROD-TO-EDI_ROD.	ROD Generic
Version du processus d'origine	La version du processus indiquée dans le Code du processus d'origine. Par exemple, pour DTROD-TO-EDI_ROD, cette valeur doit être **TOUT**.	ROD Generic
Métadictionnaire	Le métadictionnaire donne des informations qui permettent à WebSphere Partner Gateway d'interpréter les données. Par exemple, pour un document ROD, cette valeur doit être **ROD-TO-EDI_DICT**.	ROD Generic
Métadocument	Le métadocument donne des informations qui permettent à WebSphere Partner Gateway d'interpréter les données. Par exemple, pour un document ROD, cette valeur doit être **DTROD-TO-EDI_ROD**.	ROD Generic

Tableau 4. Attributs de gestionnaire de fractionnement (suite)

Attribut	Description	Gestionnaire de fractionnement
Métasyntaxe	La métasyntaxe décrit le format du document en cours de fractionnement. La valeur par défaut est **rod**.	ROD Generic
SenderId	L'ID du partenaire expéditeur.	Generic
ReceiverId	L'ID du partenaire récepteur.	Generic

Remarques :

1. Une instance de récepteur n'accepte qu'un seul type de document ROD.
2. Si un récepteur dispose de plusieurs gestionnaires de fractionnement configurés (par exemple des gestionnaires de fractionnement ROD, XML et EDI), le gestionnaire de fractionnement ROD doit être le dernier dans la **Liste configurée**.

Modification du point de configuration preprocess

Pourquoi et quand exécuter cette tâche

Pour modifier le point de configuration Preprocess, procédez comme suit :

1. Sélectionnez **Preprocess** dans la liste **gestionnaires des points de configuration**.

   Cinq gestionnaires de prétraitement sont fournis (par défaut) et sont affichés dans **Liste 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

   Remarque : Les gestionnaires Preprocess ne s'appliquent pas aux récepteurs SMTP.
2. Si vous comptez recevoir plusieurs EDI ou documents XML ou ROD qui doivent être fractionnés, veillez à sélectionner le bon gestionnaire de fractionnement. Pour configurer l'étape Preprocess :
   a. Sélectionnez un gestionnaire dans la **Liste des gestionnaires disponibles** et cliquez sur **Ajouter**. Notez que le gestionnaire passe de la **Liste des gestionnaires disponibles** à la **Liste des gestionnaires configurés**, comme illustré dans la figure 17, à la page 83:

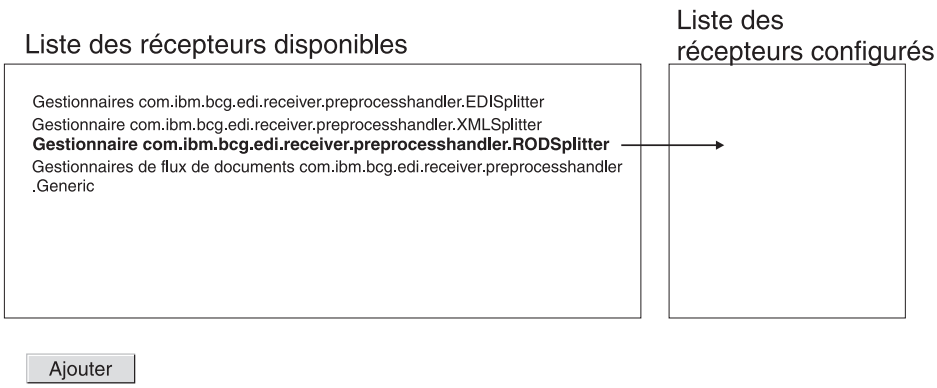


Figure 17. Configuration de l'étape de preprocess pour un récepteur

b. Répétez cette étape pour chaque gestionnaire que vous souhaitez ajouter à la liste des gestionnaires configurés.

   N'oubliez pas que pour les récepteurs, les gestionnaires sont appelés dans leur ordre d'apparition dans la liste des **gestionnaires configurés**. Le premier gestionnaire disponible traite la requête et les gestionnaires suivants de la liste ne sont pas appelés.

c. Pour configurer le gestionnaire, sélectionnez-le et cliquez sur **Configurer**:
   - Si vous avez ajouté le gestionnaire EDISplitterHandler, vous pouvez modifier le codage de ses attributs. Le codage par défaut est ASCII.
   - Si vous avez ajouté le gestionnaire XMLSplitterHandler, vous pouvez modifier le codage de ses attributs (BCGBATCHDOCs). La valeur par défaut est **ON**. Voir «Attributs Preprocess», à la page 80 pour obtenir des informations sur cet attribut.
   - Si vous avez ajouté le gestionnaire RODSplitterHandler, vous pouvez préciser des valeurs pour 11 attributs. Les attributs Codage, BATCHDOCS et Métasyntaxe ont des valeurs par défaut. Vous devez saisir une valeur pour les autres attributs, à savoir Nom du package d'origine, Version du package d'origine, Nom du protocole d'origine, Version du protocole d'origine, Code du processus d'origine, Version du processus d'origine, Métadictionnaire et Métadocument. Voir «Attributs Preprocess», à la page 80 pour obtenir des informations sur ces attributs.
   - Si vous avez ajouté GenericDocumentFlowHandler, vous pouvez spécifier des valeurs pour 13 attributs. Le codage et BATCHDOCS ont des valeurs par défaut. Les attributs SenderId et ReceiverId sont préconfigurés GenericDocumentFlowHandler sans valeur par défaut. Vous devez saisir une valeur pour les autres attributs, à savoir Nom du package d'origine, Version du package d'origine, Nom du protocole d'origine, Version du protocole d'origine, Code du processus d'origine, Version du processus d'origine, Métadictionnaire, Métadocument et Métasyntaxe. Voir «Attributs Preprocess», à la page 80 pour obtenir des informations sur ces attributs.
   - Si vous avez ajouté l'IDPartenaireNomFichier, cela ne prévoit aucun paramètre de configuration. Il prévoit que le fichier reçu suive cette convention d'appellation :

     ```
     <anystring>bcgrcv<Receiver ID>bcgsdr<Sender ID>bcgend<anystring>
     ```

     où

ID récepteur ,ID expéditeur
sont les ID entreprise des participants tels que configurés dans leur profil.

bcgrcv, bcgsdr
Sont les constantes de type chaîne qui signalent le démarrage des ID entreprise expéditeur et destinataire.

bcgend
Est une constante de type chaîne qui détermine la fin de la chaîne de convention d'appellation requise

anystring
est un caractère alphanumérique choisi par l'utilisateur

Ce gestionnaire peut être configuré uniquement pour le script FTP ou les récepteurs de répertoire FTP. Pour recevoir les fichiers binaires sur un Script FTP ou un Répertoire de fichier, vous pouvez configurer ce gestionnaire pour le récepteur.

SyncCheck

Pourquoi et quand exécuter cette tâche

Le point de configuration SyncCheck n'est disponible que pour les récepteurs HTTP/S et JMS.

Pour spécifier un gestionnaire pour un protocole métier impliqué dans un échange synchrone, procédez comme suit :

1. Sélectionnez **SyncCheck** dans la liste **gestionnaires des points de configuration**.

   Six gestionnaires SyncCheck sont fournis (par défaut) pour un récepteur HTTP/S. Ces gestionnaires figurent dans la **Liste des gestionnaires 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

   Par exemple, si vous configurez un récepteur HTTP/S, la Liste des gestionnaires disponibles se présente ainsi :

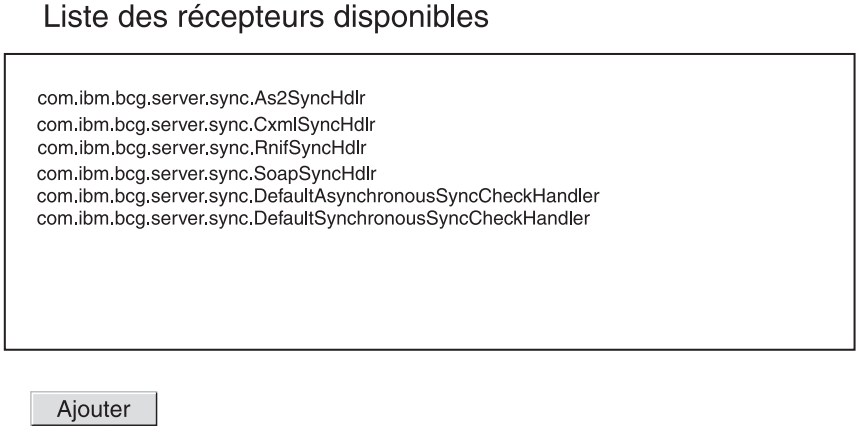


Figure 18. Liste des gestionnaires disponibles pour un point de configuration SyncCheck HTTP/S

Comme vous pouvez le constater à partir des conventions de dénomination, les quatre premiers gestionnaires s'appliquent de manière spécifique aux quatre types de documents qui peuvent être utilisés pour les transactions synchrones. Toute demande utilisant le gestionnaire DefaultAsynchronousSyncCheckHandler sera traitée comme une demande asynchrone. Toute demande utilisant le gestionnaire DefaultSynchronousSyncCheckHandler sera traitée comme une demande synchrone.

DefaultAsynchronousSyncCheckHandler et DefaultSynchronousSyncCheckHandler peuvent être utilisés avec d'autres récepteurs (telles qu'un récepteur JMS).

2. Si vous envisagez de recevoir des documents synchrones sur ce récepteur, procédez comme suit :
   a. Sélectionnez un ou plusieurs gestionnaires dans la **Liste des gestionnaires disponibles** et cliquez sur **Ajouter**.
   b. Répétez cette étape si vous voulez ajouter d'autres gestionnaires à la liste. N'oubliez pas que pour les récepteurs, les gestionnaires sont appelés dans leur ordre d'apparition dans la liste des **gestionnaires configurés**. Le premier gestionnaire disponible traite la requête et les gestionnaires suivants de la liste ne sont pas appelés.

   Pour les récepteurs HTTP et HTTPS, il est très judicieux d'indiquer le gestionnaire spécifique SyncCheck (par exemple, com.ibm.bcg.server.sync.As2SyncHdlr pour les transactions AS2), avant le gestionnaire par défaut SyncCheck.

Postprocess

Pourquoi et quand exécuter cette tâche

Aucun gestionnaire n'étant fourni par défaut pour le postprocess, aucun n'est indiqué par défaut dans la **Liste des gestionnaires disponibles**. Vous pouvez toutefois télécharger un gestionnaire pour ce point de configuration pour tous les types de récepteurs qui prennent en charge les communications synchrones. Les types de gestionnaires disponibles pour l'étape de postprocess sont :

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

Vous pouvez ajouter un gestionnaire de postprocess en en téléchargeant un qui soit conforme à l'un de ces types. Utilisez l'option **Importer** de la page Liste des gestionnaires pour télécharger un gestionnaire défini par l'utilisateur. Lorsque vous téléchargez un gestionnaire récepteur défini par l'utilisateur, le gestionnaire est ajouté à la liste des gestionnaires. Il apparaît également sur la liste des gestionnaires disponibles pour le type de point de configuration auquel il appartient.

Pour modifier le point de configuration Postprocess, procédez comme suit :

1. Sélectionnez **Postprocess** dans la liste **gestionnaires des points de configuration**.
2. Sélectionnez un gestionnaire défini par l'utilisateur dans la **Liste des gestionnaires disponibles** et cliquez sur **Ajouter**. Notez que le gestionnaire passe de la **Liste des gestionnaires disponibles** à la **Liste des gestionnaires configurés**.

Modification de la liste configurée

Pourquoi et quand exécuter cette tâche

Si vous souhaitez modifier l'ordre des gestionnaires, en supprimer un ou configurer des attributs, procédez comme suit :

- Supprimez un gestionnaire en le sélectionnant dans la **Liste des éléments configurés** et cliquez sur **Retrait**. Le gestionnaire est déplacé vers la **Liste des éléments disponibles**.
- Pour modifier l'ordre du gestionnaire dans la liste, sélectionnez-le dans la liste et cliquez sur le bouton de **déplacement vers le haut** ou **déplacement vers le bas**.

- Pour configurer le gestionnaire, sélectionnez-le dans la liste des **gestionnaires configurés** et cliquez sur **Configurer**. La liste des attributs pouvant être configurés s'affiche.

Chapitre 8. Configuration des procédures et actions portant sur les flux de travaux fixes

Ce chapitre décrit les tâches facultatives qui permettent de configurer des flux de travaux fixes de communications entrantes et sortantes ainsi que des actions. Si vous n'avez pas besoin de modifier le comportement des flux de travaux et actions tel que proposé par le système, passez au chapitre suivant.

Ce chapitre contient les rubriques suivantes :

Remarque : Pour effectuer des modifications de configurations sur WebSphere Partner Gateway, vous devez toujours utiliser la même instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Téléchargement de gestionnaires

Pourquoi et quand exécuter cette tâche

Si vous prévoyez de modifier des composants, vous devez télécharger les gestionnaires de ces composants avant de créer ou configurer ces composants. Il vous suffit de télécharger les gestionnaires définis par l'utilisateur pour les composants qui le nécessitent. Par exemple, si vous ajoutez votre propre étape de validation, vous devez télécharger ce gestionnaire depuis la page Actions des **Gestionnaires** (comme décrit par les étapes 1 à 4, à la page 90).

Remarque : Comme indiqué dans «Configuration des composants de traitement des documents à l'aide de gestionnaires», à la page 14, seuls les gestionnaires définis par l'utilisateur ont besoin d'être téléchargés. Les gestionnaires fournis par WebSphere Partner Gateway sont déjà disponibles.

Vous pouvez modifier les flux de travaux fixes et les actions et créer de nouvelles actions. Vous pouvez modifier ces composants via les gestionnaires avec lesquels vous les associez.

Remarque : Pour dresser la liste des types de gestionnaires valides pour les actions et les flux de travaux fixes, cliquez sur **Administrateur de concentrateur > Configuration du concentrateur > Gestionnaires > Action > Types de gestionnaires**, ou **Administrateur de concentrateur > Configuration du concentrateur > Gestionnaires > Flux de travaux fixes > Types de gestionnaires**. Utilisez cette liste pour confirmer que le type de votre gestionnaire est correct avant de le télécharger. Il doit s'agir de l'un des types admis, sinon son téléchargement n'aboutira pas.

Pour télécharger un gestionnaire, procédez comme suit :

1. Dans le menu principal, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Gestionnaires**.

2. Sélectionnez le type de gestionnaire (**Action** ou **Flux de travaux fixe**).

   La liste des gestionnaires actuellement définis pour le composant en question s'affiche à l'écran. Remarquez que les gestionnaires répertoriés sont ceux fournis par WebSphere Partner Gateway. Ils sont associés à l'ID fournisseur **Produit**.
3. Dans la page Liste des gestionnaires, cliquez sur **Importer**.
4. Sur la page d'importation de gestionnaire, indiquez le chemin d'accès au fichier XML qui décrit le gestionnaire, ou utilisez **Parcourir** pour rechercher ce fichier XML.
5. Cliquez sur **Télécharger**.

Une fois le gestionnaire téléchargé, vous pouvez l'utiliser pour créer de nouveaux flux de travaux et actions.

Remarque : Vous pouvez télécharger les gestionnaires définis par l'utilisateur en téléchargeant le fichier XML modifié. Par exemple, pour un gestionnaire d'action, vous pouvez cliquer sur **Administrateur du concentrateur > Configuration du concentrateur > Gestionnaires > Action**, puis cliquer sur **Importer**.

Vous ne pouvez ni modifier ni supprimer les gestionnaires fournis par WebSphere Partner Gateway.

Configuration des flux de travaux fixes

Pourquoi et quand exécuter cette tâche

Le Chapitre 2, «Introduction à la configuration du concentrateur», à la page 5 décrit les deux étapes de flux fixes de travaux de communication entrante que vous pouvez configurer, une pour le dégroupement d'un protocole et une autre pour son analyse syntaxique. Pour les flux de travaux de communication sortante, il n'existe qu'une seule étape, pour l'empaquetage de protocole.

Si vous prévoyez d'utiliser un gestionnaire défini par l'utilisateur pour configurer une étape de flux de travaux, téléchargez le gestionnaire comme décrit dans « Téléchargement de gestionnaires», à la page 89.

Pour configurer un flux de travaux fixe, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Flux de travaux fixe**.
2. Cliquez sur **Communication entrante** ou **Communication sortante**.
3. Cliquez sur l'icône **Afficher les détails** en regard du nom de l'étape que vous souhaitez configurer.

   L'étape, ainsi que la liste de gestionnaires configurés pour cette étape, est répertoriée. Pour la liste des gestionnaires par défaut, voir «Flux de travaux de communication entrante», à la page 91 et «Flux de travaux de communication sortante», à la page 92.
4. Cliquez sur l'icône **Edition** pour modifier la liste des gestionnaires.
5. Exécutez une ou plusieurs des tâches ci-après pour chaque étape que vous souhaitez modifier.
   a. Ajoutez un gestionnaire en le sélectionnant dans la liste des **gestionnaires disponibles** et en cliquant sur **Ajouter** (un gestionnaire apparaît dans la liste des **gestionnaires disponibles** si vous avez téléchargé un gestionnaire défini par l'utilisateur ou si vous avez précédemment supprimé un

gestionnaire de la liste des **gestionnaires configurés**). Le gestionnaire passe dans la liste des **gestionnaires configurés**.

b. Supprimez un gestionnaire en le sélectionnant dans la **Liste des éléments configurés** et cliquez sur **Retrait**. Le gestionnaire est déplacé vers la **Liste des éléments disponibles**.

c. Pour modifier l'ordre d'appel des gestionnaires, sélectionnez un gestionnaire dans la liste et cliquez sur le bouton de **déplacement vers le haut** ou **déplacement vers le bas**.

   Les gestionnaires sont appelés dans l'ordre de la liste des **gestionnaires configurés**. Le premier gestionnaire disponible se charge de la demande. Si vous prévoyez de recevoir un grand nombre de documents d'un certain type (par exemple, documents ROD), vous pouvez mettre en début de liste le gestionnaire associé à ce type de document (dans cet exemple, com.ibm.bcg.edi.business.process.RODScannerHandler).

6. Cliquez sur **Sauvegarder**.

Flux de travaux de communication entrante

Cette section dresse la liste des gestionnaires configurés pour les flux de travaux de communication entrante.

Gestionnaires de dégroupement de protocole

Par défaut, les gestionnaires ci-dessous sont configurés pour l'étape de dégroupement de Protocole :

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

Gestionnaires de traitement de protocole

Par défaut, les gestionnaires ci-dessous sont configurés pour l'étape de traitement de Protocole :

- 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

L'attribut "Content-Types" est associé à BinaryChannelParseHandler, XMLRouterBizHandler, EDIRouterBizProcessHandler et cXMLChannelParseHandler. Ces gestionnaires sont prédéfinis avec une liste par défaut de types de contenu. Si le document reçu a un en-tête de type de contenu configuré pour l'un des gestionnaires ci-dessus, le gestionnaire en question est appliqué.

Flux de travaux de communication sortante

Par défaut, les gestionnaires ci-dessous sont configurés pour l'étape d'empaquetage de Protocole :

- 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

Configuration des actions

Le Chapitre 2, «Introduction à la configuration du concentrateur», à la page 5 indiquait que les actions pouvaient être constituées d'une ou plusieurs étapes. WebSphere Partner Gateway fournit un ensemble d'actions par défaut. Vous pouvez effectuer des ajouts à la liste d'actions en téléchargeant un ou plusieurs gestionnaires (qui correspondent à des étapes dans les actions), que vous pouvez ensuite utiliser dans une action. Vous pouvez également créer des actions (voir «Création d'actions», à la page 109).

Remarque : Vous ne pouvez pas modifier les actions fournies par WebSphere Partner Gateway, bien que vous puissiez copier une ou plusieurs d'entre elles et les modifier ensuite (voir «Copie d'une action», à la page 110).

Si vous prévoyez d'utiliser un gestionnaire défini par l'utilisateur pour configurer une action, téléchargez-le comme décrit dans « Téléchargement de gestionnaires», à la page 89.

Actions fournies par le produit

Cette section présente l'objet des actions Websphere Partner Gateway fournies par le produit, ainsi que la configuration requise pour les utiliser. Le Chapitre 9, «Configuration des types de documents», à la page 111 explique dans quels cas utiliser certaines de ces actions.

Certaines actions comportent la mention Bidirectionnel dans leur nom. Dans ce cas, *Bidirectionnel* signifie qu'il est possible d'inverser le format de la source ou de la cible : l'action pourra toujours être utilisée. Par exemple, pour l'action “Translation bidirectionnelle de RosettaNet et XML avec Validation”, le document source peut être au format RosettaNet et le document cible au format XML, ou bien le document source peut être au format XML et le document cible au format RosettaNet.

Vous trouverez ci-dessous les différentes actions fournies avec Websphere Partner Gateway :

- «Passe-système», à la page 93
- «Annulation d'un processus RosettaNet par un partenaire interne», à la page 94
- «Passe-système RosettaNet avec consignation du processus», à la page 94
- «Translation bidirectionnelle de RosettaNet et de RosettaNet Service Content avec validation», à la page 95

- «Translation bidirectionnelle de RosettaNet et de RosettaNet Service Content sans validation du contenu», à la page 97
- «Translation bidirectionnelle de documents XML personnalisés issus du partenaire interne vers RosettaNet avec recherche de doublons et validation du contenu», à la page 97
- «Translation bidirectionnelle de RosettaNet et XML avec validation», à la page 96
- «Translation bidirectionnelle d'un document XML personnalisé avec validation», à la page 98
- «Translation bidirectionnelle d'un document XML personnalisé avec recherche de doublons et validation», à la page 99
- «Passe-système XML personnalisé avec recherche de doublons et validation», à la page 100
- «Passe-système XML personnalisé avec recherche de doublons», à la page 101
- «Passe-système XML personnalisé avec validation», à la page 101
- «Désenveloppement EDI», à la page 102
- «Validation et translation EDI», à la page 102
- «Translation ROD (fichier à plat) et validation EDI», à la page 104
- «Translation XML et validation EDI», à la page 103
- «Décomposition et analyse ebMS», à la page 104
- «Validation de l'élément SOAP Envelope», à la page 107
- «Validation de l'élément SOAP Body», à la page 107
- «Désenvelopper le protocole SOAP», à la page 107
- «Validation d'échange EDI», à la page 105
- «Transformation WTX», à la page 105
- «Réenveloppeur EDI», à la page 106

Passe-système

Cette action est utilisée lorsqu'aucun traitement spécifique (validation, transformation, etc.) n'est nécessaire pour le document. Le document source est envoyé vers la cible tel quel.

Configuration

Aucune configuration requise.

Modification

Cette action peut être copiée dans une nouvelle action. De nouvelles étapes peuvent être ajoutées avant les étapes existantes. Par exemple, une étape de validation personnalisée qui valide le document source, ou un autre traitement personnalisé.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.passthrough.No_op** – Permet d'indiquer que le type de contenu du document cible ne doit pas être déduit du contenu du document.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de

la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Annulation d'un processus RosettaNet par un partenaire interne Objet

Cette action permet au partenaire interne (dorsal) d'annuler un processus RNIF RosettaNet). Lorsque l'application dorsale (partenaire interne) envoie un document Evénement XML avec le code événement 800/801, un document 0A1 destiné au partenaire externe est créé dans le cadre de cette étape, puis le processus PIP correspondant est annulé.

Configuration

Le processus RNIF à annuler doit avoir été configuré dans WebSphere Partner Gateway et WebSphere Partner Gateway doit avoir reçu le document RosettaNet qui a démarré le processus à annuler.

Modification

Cette action ne peut pas être modifiée ni copiée car elle est spécifique à l'annulation du processus PIP RosettaNet.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Détermine la classe de dégroupement appropriée pour le package RNIF ou considère que le document n'est pas un package RNIF, auquel cas aucun dégroupement n'est effectué.
2. **com.ibm.bcg.validation.ValidationFactory** - Valide le document RN source pour vérifier le format RNIF Service Content.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Passe-système RosettaNet avec consignation du processus

Cette action est utilisée lorsque le document RNIF RosettaNet source est transmis directement à WebSphere Partner Gateway. Utilisez cette étape lorsque le document RNIF Service Content n'est ni extrait ni transformé. Même s'il s'agit d'une transmission directe, le traitement RNIF est exécuté malgré tout et des accusés de réception sont générés.

Configuration

Aucune configuration requises.

Modification

Cette action peut être copiée et modifiée. De nouvelles étapes peuvent être ajoutées avant les étapes existantes, afin de spécifier un traitement personnalisé.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.rosettanet.passthru.ProcessLoggingFactory** - Cette étape définit les métadonnées du document RosettaNet dans l'objet BDO (Business Document Object).
2. **com.ibm.bcg.passthrough.No_op** - Permet d'indiquer que le type de contenu du document cible ne doit pas être déduit du contenu du document.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation bidirectionnelle de RosettaNet et de RosettaNet Service Content avec validation

Cette action est utilisée pour les documents RNIF RosettaNet. Lors de la réception d'un document RNIF envoyé par un partenaire externe, les données utiles (RNSC - RosettaNet Service Content) sont extraites du document RNIF empaqueté, puis transmises à l'application dorsale (partenaire interne). La validation est effectuée sur le document RNIF, y compris le contenu RNSC. Lorsqu'il est transmis par l'application dorsale (partenaire interne), le contenu RNSC est validé.

Configuration

Le package PIP RosettaNet pour le document RosettaNet doit avoir été chargé.

Modification

Cette action ne peut pas être copiée ni modifiée.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Détermine la classe de dégroupement appropriée pour le package RNIF ou considère que le document n'est pas un package RNIF, auquel cas aucun dégroupement n'est effectué.
2. **com.ibm.bcg.validation.ValidationFactory** - Effectue la validation et utilise les processus métier suivants pour valider les documents RNIF 1.1, RNIF 2.0 et RNSC. - RNSignal0A1Validation (validation du message 0A1 ou des signaux RNIF générés par WebSphere Partner Gateway) - ValidationNoOp (ce processus renvoie le document de gestion sans aucun traitement ; il est appelé lorsque WBIC fait plusieurs tentatives pour les signaux RNIF ou le message 0A1) - RN11Validation (validation du message RNIF 1.1) - RN20Validation (validation du message RNIF 2.0) - RNSCValidation (validation de l'événement XML et du message RNSC).
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - Permet d'extraire le contenu RNSC du document RNIF ou de créer des informations RNIF pour le contenu RNSC.

4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Dans le cadre du traitement des documents 0A1 RosettaNet, permet de mettre à jour le moteur d'états RosettaNet.
5. **com.ibm.bcg.outbound.OutboundDocFactor** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation bidirectionnelle de RosettaNet et XML avec validation

Cette action est utilisée pour les documents RNIF RosettaNet qui doivent être transformés en documents XML personnalisés, ou vice versa. Lors de la réception d'un document RNIF envoyé par un partenaire externe, les données utiles (RNSC, RNIF Service Content) sont extraites du document RNIF, validées, transformées en document XML, puis transmises à l'application dorsale (partenaire interne) après validation des documents cible transformés. S'il est transmis par l'application dorsale (partenaire interne), le document XML est validé, transformé en document RNSC, puis revalidé.

Configuration

- Le package PIP RosettaNet pour le document RosettaNet doit avoir été chargé.
- Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document XML source ou cible.
- Nécessite la configuration d'une mappe de transformation XSLT.

Modification

Cette action ne peut pas être copiée ni modifiée.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Détermine la classe de dégroupement appropriée pour le package RNIF ou considère que le document n'est pas un package RNIF, auquel cas aucun dégroupement n'est effectué.
2. **com.ibm.bcg.validation.ValidationFactory** – Permet de valider le document RNIF ou XML source.
3. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – Transforme un document RNSC en XML, ou inversement.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - Valide le document XML transformé.
5. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Dans le cadre du traitement des documents 0A1 RosettaNet, permet de mettre à jour le moteur d'états RosettaNet.
6. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation bidirectionnelle de RosettaNet et de RosettaNet Service Content sans validation du contenu

Cette action est utilisée pour les documents RosettaNet (RNIF). Lors de la réception d'un document RNIF d'un partenaire externe, les données utiles (RNSC, RNIF Service Content) sont extraites du conditionnement RNIF. Les données utiles extraites sont validées et transformées en un document XML avant d'être envoyées à l'application dorsale (partenaire interne). Lorsqu'un document XML est émis par l'application dorsale (partenaire interne), les étapes suivantes sont effectuées :

1. Recherche d'ID en double
2. Validation
3. Transformation en RNSC
4. Validation de RNSC

Configuration

Le package PIP RosettaNet pour le document RosettaNet doit avoir été chargé.

Modification

Cette action ne peut pas être copiée ni modifiée.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Détermine la classe de dégroupement appropriée pour le package RNIF ou considère que le document n'est pas un package RNIF, auquel cas aucun dégroupement n'est effectué.
2. **com.ibm.bcg.validation.ValidationWithoutContentFactory** – Exécute la validation, mais pas sur le contenu RNSC.
3. **com.ibm.bcg.translation.protocol.StdRNandRNSCProtFactory** - Permet d'extraire le contenu RNSC du document RNIF ou de créer des informations RNIF pour le contenu RNSC.
4. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Dans le cadre du traitement des documents 0A1 RosettaNet, permet de mettre à jour le moteur d'états RosettaNet.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation bidirectionnelle de documents XML personnalisés issus du partenaire interne vers RosettaNet avec recherche de doublons et validation du contenu

Cette action est utilisée pour les documents RNIF RosettaNet qui doivent être transformés en documents XML personnalisés, ou vice versa. Lors de la réception d'un document RNIF envoyé par un partenaire externe, les données utiles (RNSC, RNIF Service Content) sont extraites du document RNIF, validées, transformées en document XML, puis transmises à l'application dorsale (partenaire interne). Si le document XML est transmis par l'application dorsale (partenaire interne), une recherche d'ID en double est effectuée, puis le document XML est validé,

transformé en RNSC, puis revalidé. Semblable à l'action "Translation bidirectionnelle de RosettaNet et XML avec validation", mais une recherche de doublons sur le document XML source est ajoutée.

Configuration

- Les clés de recherche de doublons doivent avoir été configurées pour le document source au format XML.
- Le package PIP RosettaNet pour le document RosettaNet doit avoir été chargé.
- Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document XML source ou cible.
- Nécessite la configuration d'une mappe de transformation XSLT.

Modification

Cette action ne peut pas être copiée ni modifiée, car elle est spécifique à un document RNIF.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Exécute une recherche d'ID en double sur le document XML personnalisé reçu.
2. **com.ibm.bcg.server.pkg.UnPackagingFactory** - Détermine la classe de dégroupement appropriée pour le package RNIF ou considère que le document n'est pas un package RNIF, auquel cas aucun dégroupement n'est effectué.
3. **com.ibm.bcg.validation.ValidationFactory** – Permet de valider le document RNIF ou XML source.
4. **com.ibm.bcg.translation.protocol.RNXsltProtFactory** – Transforme un document RNSC en XML, ou inversement.
5. **com.ibm.bcg.validation.OutboundValidationFactory** - Valide le document XML transformé.
6. **com.ibm.bcg.sponsor.SponsorBusProcessFactory** - Dans le cadre du traitement des documents 0A1 RosettaNet, permet de mettre à jour le moteur d'états RosettaNet.
7. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation bidirectionnelle d'un document XML personnalisé avec validation

Cette action est utilisée pour les documents XML personnalisés provenant de partenaires externes ou internes. Le document source est validé, transformé en document cible, puis ce dernier est à son tour validé.

Configuration

- Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document source.
- Nécessite la configuration d'une mappe de transformation XSLT.

- Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document cible.

Modification

Cette action peut être copiée et modifiée. Les étapes Transformation et Validation peuvent être remplacées par des étapes définies par l'utilisateur. Il est également possible d'ajouter des étapes définies par l'utilisateur.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.validation.ValidationFactory** – Valide le document XML personnalisé reçu.
2. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** – Exécute la transformation.
3. **com.ibm.bcg.validation.OutboundValidationFactory** - Valide le document XML transformé.
4. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation bidirectionnelle d'un document XML personnalisé avec recherche de doublons et validation

Cette action est utilisée pour les documents XML personnalisés. Elle est applicable aux documents provenant d'un partenaire externe ou interne. Une recherche d'ID en double est effectuée sur le document source, puis ce document est validé et transformé en document cible ; enfin, le document cible est à son tour validé. Semblable à l'action “Translation bidirectionnelle d'un document XML personnalisé avec validation”, avec une étape supplémentaire de recherche de doublons.

Configuration

- Les clés de recherche de doublons doivent avoir été configurées pour le document source au format XML.
- Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document source.
- Nécessite la configuration d'une mappe de transformation XSLT.
- Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document cible.

Modification

Cette action peut être copiée et modifiée. Les étapes ValidationFactory, XSLTTranslationFactory et OutboundValidationFactory peuvent être remplacées par des étapes définies par l'utilisateur. Il est également possible d'ajouter des étapes définies par l'utilisateur.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Recherche les éventuels documents en double, à partir de l'ID du document.
2. **com.ibm.bcg.validation.ValidationFactory** - Valide le document XML personnalisé reçu.
3. **com.ibm.bcg.translation.protocol.translators.xslt.XSLTranslationFactory** - Cette étape transforme le document XML personnalisé reçu en document XML cible.
4. **com.ibm.bcg.validation.OutboundValidationFactory** - Valide le document XML cible obtenu suite à l'étape de transformation précédente.
5. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Passe-système XML personnalisé avec recherche de doublons et validation

Objet

Cette action est utilisée pour les documents XML personnalisés. Elle est applicable aux documents provenant d'un partenaire externe ou interne. Une recherche des ID en double est effectuée sur le document source, puis ce dernier est validé. Semblable à l'action “Passe-système XML personnalisé avec recherche de doublons”, mais avec validation du document source.

Configuration

- Les clés de recherche de doublons doivent avoir été configurées pour le document source au format XML.
- Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document XML source.

Modification

Cette action peut être copiée et modifiée. L'étape ValidationFactory peut être remplacée par une étape définie par l'utilisateur. Il est également possible d'ajouter des étapes définies par l'utilisateur.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Recherche les éventuels documents en double, à partir de l'ID du document. Le document source au format XML doit être configuré pour la recherche d'ID en double.
2. **com.ibm.bcg.validation.ValidationFactor** - Valide le document XML personnalisé source.
3. **com.ibm.bcg.passthrough.No_op** - Permet d'indiquer que le type de contenu du document cible ne doit pas être déduit du contenu du document.
4. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de

la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Passe-système XML personnalisé avec recherche de doublons

Cette action est utilisée pour les documents XML personnalisés. Elle est applicable aux documents provenant d'un partenaire externe ou interne. Une recherche des ID en double est effectuée sur le document source.

Configuration

Les clés de recherche de doublons doivent avoir été configurées pour le document source au format XML.

Modification

Cette action ne peut pas être copiée dans une autre action, car une modification possible consiste à ajouter une étape de validation, définie dans l'action "Passe-système XML personnalisé avec recherche de doublons et validation".

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.duplicate.ContentDuplicateProcessFactory** - Recherche les éventuels documents en double, à partir de l'ID du document. Le document source au format XML doit être configuré pour la recherche d'ID en double.
2. **com.ibm.bcg.passthrough.No_op** - Permet d'indiquer que le type de contenu du document cible ne doit pas être déduit du contenu du document.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Passe-système XML personnalisé avec validation

Cette action est utilisée pour les documents XML personnalisés provenant d'un partenaire externe ou interne. Une validation est effectuée sur le document source.

Configuration

Nécessite la configuration de la mappe de validation (XML SCHEMA) sur le document XML source.

Modification

Cette action peut être copiée et modifiée. L'étape ValidationFactory peut être remplacée par une étape définie par l'utilisateur. Il est également possible d'ajouter des étapes définies par l'utilisateur.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.validation.ValidationFactory** - Valide le document XML personnalisé source.
2. **com.ibm.bcg.passthrough.No_op** - Permet d'indiquer que le type de contenu du document cible ne doit pas être déduit du contenu du document.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Désenveloppement EDI

Cette action est utilisée pour les échanges EDI provenant d'un partenaire externe. L'échange EDI est désenveloppé (extraction des transactions EDI), puis les transactions EDI sont réintroduites dans WebSphere Partner Gateway et traitées une par une. Le document d'échange EDI ne subit aucun autre traitement dans WebSphere Partner Gateway.

Configuration

Configuration facultative dans les définitions de documents.

Modification

Cette action ne peut pas être copiée ni modifiée.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.edi.business.process.EDIDenvFactory** – Désenveloppe l'échange EDI Interchange.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Validation et translation EDI

Cette action est utilisée pour les transactions EDI qui ont été extraites d'un échange EDI via l'action Désenveloppement EDI. Ces transactions proviennent d'un partenaire externe. Les documents de transaction EDI sont validés, puis transformés.

Configuration

- Configuration facultative dans les définitions de documents.
- Mappes de validation facultatives pour la transaction EDI source issue du client DIS ou Design Studio WTX.
- Mappes de transformation du client DIS ou WTX design studio.
- Connexion de participant de any package / EDI - Any / Any vers None / EDI - Any / Any doit être définie avec action définie en tant que désenvelopper EDI.

Modification

Cette action peut être copiée et modifiée pour ajouter des étapes d'exit utilisateur.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.edi.business.process.EDISourceValidationFactory** – Valide la transaction EDI. Cette étape émet également un accusé de réception (FA) une fois que toutes les transactions EDI de l'échange EDI ont été traitées.
2. **com.ibm.bcg.edi.business.process.EDITranslatorFactory** – Transforme la transaction EDI en un document cible.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation XML et validation EDI
Objet

Cette action est utilisée pour les documents XML personnalisés issus du partenaire interne. Le document XML source est transformé en transaction EDI, puis validé. Il est envoyé au système dorsal ou à un partenaire externe. Les formats XML sont utilisés pour l'identification des informations d'acheminement.

Configuration

- Configuration facultative dans les définitions de documents.
- Mappes de validation facultatives pour la transaction EDI cible issue du client DIS.
- Mappes de transformation depuis le client DIS ou WDI design studio.

Modification

Cette action peut être copiée et modifiée pour supprimer l'étape EDITargetValidationFactory ou pour ajouter des étapes d'exit utilisateur.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.edi.business.process.XMLTranslatorFactory** – Transforme le document XML source en transaction EDI cible.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – Valide la transaction EDI cible.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Translation ROD (fichier à plat) et validation EDI

Cette action est utilisée pour les documents Record Oriented Documents (ROD/fichiers à plat) issus du partenaire interne. Le document ROD source est transformé en transaction EDI, puis validé.

Configuration

- Configuration facultative dans les définitions de documents.
- Mappes de validation facultatives pour la transaction EDI cible issue du client DIS.
- Le standard ROD doit être défini dans le client DIS et compilé avec une mappe de transformation factice.
- L'Utilitaire de fractionnement/Processeur de document générique ROD doit être ajouté selon le gestionnaire de processus dans le récepteur. Cela permet de connaître le document et format du dictionnaire.

Modification

Cette action peut être copiée et modifiée pour supprimer l'étape EDITargetValidationFactory ou pour ajouter des étapes d'exit utilisateur.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.edi.business.process.RODTranslatorFactory** – Transforme le document ROD source en transaction EDI cible.
2. **com.ibm.bcg.edi.business.process.EDITargetValidationFactory** – Valide la transaction EDI cible.
3. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Décomposition et analyse ebMS

Cette action est utilisée pour les documents ebMS issus d'un partenaire externe. Les données utiles en pièce jointe sont extraites et réintroduites dans WebSphere Partner Gateway, où elles seront traitées une par une. Le document ebMS ne subit aucun autre traitement dans WebSphere Partner Gateway.

Configuration

Aucune configuration supplémentaire n'est requise.

Modification

Cette action ne peut pas être copiée ni modifiée.

Etapes

Cette action contient les étapes suivantes, qui sont effectuées dans leur ordre d'exécution :

1. **com.ibm.bcg.server.EBMSSplitAndParse** – Les données utiles en pièce jointe sont extraites dans des documents distincts.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - Obligatoire. Exécute le traitement WebSphere Partner Gateway requis sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Validation d'échange EDI

La validation d'échange EDI est utilisée pendant l'intégration asynchrone avec WTX. Les transactions individuelles sont extraites de l'échange en désenveloppant celui-ci. L'action de désenvelopper va extraire chaque transaction de l'échange. Chacune de ces transactions va produire un document qui sera directement transmis pour validation

Remarque : L'attribut "Annuler l'enveloppe en cas d'erreur" ne peut pas être utilisé dans le contexte de validation de l'échange de données informatisé. Si vous essayez de configurer la valeur pour utiliser cet attribut, cette valeur sera ignorée.

Configuration

- La connexion de participant de <any package> / EDI – xxxx / XXX à None / EDI – xxxx / XXX doit être définie avec action définie en tant que “Validation d'échange EDI”.
- Un utilisateur FA peut éventuellement configurer une FA.
- Un canal doit être défini pour l'accusé de réception fonctionnel par lequel le flux doit passer.

Transformation WTX

Les fichiers EDI, XML et ROD ou les fichiers à plat sont transformés avec WTX.

La transformation de EDI à l'aide de WTX peut être asynchrone ou synchrone. La transformation synchrone est principalement utilisée lorsqu'une transaction désenveloppée et validée est envoyé à WTX pour traitement, mais ici la transaction serait réenveloppée comme requis pour les traitements dans WTX. Une fois la transaction EDI validée, elle est transmise à l'action de transformation WTX de transaction EDI. En mode asynchrone, les transactions EDI sont transformées dans le système dorsal, où WTX est déployé sur le programme de lancement WESB/WMB ou WTX.

Les points suivants doivent être pris en compte lors de l'utilisation de l'échange des données informatisé comme entrée pour la transformation :

Important :

1. Utilisez toujours un seul délimiteur de caractères.
2. Si vous utilisez la combinaison de délimiteurs de caractères "/r/n" et que le délimiteur de caractères "/r" se trouve en position de délimiteur de segment de l'en-tête d'échange, le délimiteur de caractères "/n" sera ignoré.
3. Modifiez l'arborescence des types en conséquence.

Configuration pour transformation synchrone

- La connexion de participant de <any package> / EDI – xxxx / XXX à None / EDI – xxxx / XXX doit être définie avec action définie en tant que désenvelopper EDI.
- La connexion de participant de <N/A> / XXXXXXX/ YYYYY à None / ZZZZZZ / BBBBBBB doit être définie avec action définie en tant que “Validation EDI” & “Transformation WTX de transaction EDI”.
- Une mappe de transformation WTX doit aussi être associée à ce canal.

Configuration pour transformation asynchrone

- La connexion de participant de <any package> / EDI – xxxx / XXX à None / EDI – xxxx / XXX doit être définie avec action définie en tant que désenvelopper EDI.
- La connexion de participant de <N/A> / <edi version>/ transaction à <N/A> / <edi version> / transaction doit être définie avec une action définie en tant que Validation EDI.
- La connexion de participant de <N/A> / <edi version> / transaction à <BI> / <edi interchange> / <ISA> / <UNB> / <UCS> doit être définie avec une action définie en tant que Validation EDI & RE-ENVELOPPER EDI.

Configuration pour ROD et XML

- Transformation ROD - La connexion de participant de <any package> / <any protocol (fichier à plat) > / <any flat file> à <Any> / <ANY> / <Any> Format doit être définie avec action définie en tant que “Transformation WTX”.
- Transformation XML - La connexion de participant de <any package> / <any protocol> / <any XML> à <Any> / <ANY> / <Any> Format doit être définie avec une action définie en tant que “Transformation WTX”.

Enveloppe WTX
Objet

Lorsque WTX est utilisé en mode asynchrone, il transforme et produit des transactions EDI après la transformation WTX, et envoie cela à WebSphere Partner Gateway pour enveloppement.

Configuration

- Connexion de <Backend> / <EDI Dictionary> / <EDI document> {EDI Trx} à <N/A> / <EDI X12/EDIFACT> / <EDI ISA/UNB> avec l'action Passer Configurer le profil de l'enveloppeur dans la cible finale. (Canal-A).
- Connexion de <NA> / <EDI Interchange> / <EDI ISA/UNB> à <ANY PACKAGE> / <EDI X12/EDIFACT> / <EDI ISA/UNB> avec action en tant que passe-système. (Canal-B)
-

Réenveloppeur EDI

Un réenveloppeur est utilisé pour envelopper les transactions individuelles. Il utilise les en-têtes de l'enveloppeur de l'enveloppe source pour y encapsuler les transactions désenveloppées.

Configuration

- Une connexion entre la source (transaction) et la cible (échange EDI) avec le profil d'enveloppe défini

- Définissez l'action en tant que Réenveloppeur EDI

Validation de l'élément SOAP Envelope

La demande de service Web dans son ensemble sera validée par rapport au schéma SOAP1.1 selon les normes de l'industrie. L'action SOAP Envelope contient les étapes suivantes, dans leur ordre d'exécution :

1. **com.ibm.bcg.validation.WebserviceFactory** – effectue la validation de requête de service Web et renvoie le gestionnaire de validation de service Web.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - obligatoire. Exécute le traitement requis pour WebSphere Partner Gateway sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Validation de l'élément SOAP Body

Cette fonction permet de valider l'élément SOAP Body ou la charge disponible sous l'élément SOAP Envelope. La validation de charge est uniquement prise en charge pour les charges XML dans SOAP Envelope. Le pointeur d'emplacement de schéma standard sous Payload XML est utilisé pour la validation reposant sur les schémas. Vous pouvez éventuellement associer votre schéma à la connexion de service Web concernée pour valider la charge. Ce schéma aura priorité sur le schéma placé sous l'élément payload XML. En l'absence de pointeur d'emplacement de schéma dans payload XML, associez un schéma sous la connexion de service Web. Les attributs d'objet de routage pour les demandes et les réponses du service Web sont les suivants :

- **ResponseValidation** – définissez la valeur de cet attribut sur “Non” du côté cible, si vous ne souhaitez pas valider de document réponse. La valeur par défaut de cet attribut est “Oui”.
- **ContentValidation** – cet attribut vous permet d'activer ou de désactiver la validation de contenu sur payload XML. Cette validation est activée par défaut. Si vous le paramétrez sur “Non”, une validation grammaticale sera effectuée.

L'action SOAP Body contient les étapes suivantes, dans leur ordre d'exécution :

1. **com.ibm.bcg.validation.ValidationFactory** – effectue la validation de requête de service Web.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - obligatoire. Exécute le traitement requis pour WebSphere Partner Gateway sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Pour mettre à niveau WebSphere Partner Gateway afin d'inclure la fonction de validation de charge sous SOAP envelope, voir le Guide d'administration.

Désenvelopper le protocole SOAP

L'élément SOAP Envelope doit être désenveloppé et l'élément SOAP Body doit être introduit pour être traité. Les attributs d'objet de routage pour désenvelopper SOAP Envelope sont les suivants :

- **De-Envelope SOAP Envelope** - prend uniquement en charge la communication asynchrone. Aucun incident ou réponse SOAP n'est renvoyé puisqu'il s'agit d'une prise en charge de profil basique de service Web à sens unique. Dans le cas de communication synchrone, l'attribut va générer une erreur de document et consigner l'erreur d'événement.

- **Re-route De-enveloped Document** - attribut d'objet de routage lié de l'action **Désenvelopper SOAP Envelope**. S'il est défini sur "Oui", l'action **Désenvelopper SOAP Envelope** doit introduire l'élément SOAP Body extrait de SOAP Envelope en tant que nouveau document dans WebSphere Partner Gateway. Par ailleurs, la pièce jointe doit également être introduite en tant que nouveau document. Tous les documents qui sont introduits arrivent dans le package N/A. Pour les router plus loin, vous devez configurer un canal basé sur ce package pour les charges extraites et les documents attachés.
- **ConsumePayload** - cet attribut est lié à l'attribut **Re-route De-enveloped Document**. Il sert à supprimer la charge après l'extraction. Si la valeur de cet attribut et la valeur de **Re-route De-enveloped Document** sont définies sur "Oui", la charge n'est pas extraite ni redirigée depuis SOAP envelope. Seules les pièces jointes sont redirigées. Si cet attribut est défini sur "Non" et **Re-route De-enveloped Document** sur "Oui", la charge et les pièces jointes sont redirigées séparément. La valeur par défaut de cet attribut est "Non".

L'action désenvelopper SOAP Envelope contient les étapes suivantes, dans leur ordre d'exécution :

1. **com.ibm.bcg.validation.SOAPDeEnveloperFactory** – effectue la validation de requête de service Web et renvoie le gestionnaire de désenveloppement de SOAP.
2. **com.ibm.bcg.outbound.OutboundDocFactory** - obligatoire. Exécute le traitement requis pour WebSphere Partner Gateway sur le document cible. Il s'agit de la dernière étape, ajoutée automatiquement par la console aux actions existantes ou nouvelles. Cette étape n'apparaît pas dans la liste des gestionnaires configurés.

Dans les instances où vous voulez désenvelopper SOAP avec les pièces jointes et router uniquement ces dernières sans la charge sous SOAP body, la configuration se présente comme suit :

- bcg.soap.ConsumePayload = Y (par défaut cette valeur est N)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (par défaut cette valeur est Y)

Lorsque vous voulez désenvelopper SOAP avec les pièces jointes et router celles-ci et la charge séparément, la configuration se présente comme suit :

- bcg.soap.ConsumePayload = N (par défaut cette valeur est N)
- bcg.soap.Re-RouteDe-EnvelopedDocument = Y (par défaut cette valeur est Y)

Pour mettre à niveau WebSphere Partner Gateway afin d'inclure la fonction de validation de charge sous SOAP Envelope, voir le *Guide d'administration de WebSphere Partner Gateway*.

Modification d'une action définie par l'utilisateur

Pourquoi et quand exécuter cette tâche

Pour configurer une action définie par l'utilisateur, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Actions**.
2. Cliquez sur l'icône **Afficher les détails** en regard du nom de l'action définie par l'utilisateur que vous souhaitez configurer.

   L'action, ainsi que la liste de gestionnaires (étapes d'action) déjà configurés pour cette étape, est répertoriée.

3. Exécutez une ou plusieurs des étapes ci-après pour chaque action que vous souhaitez modifier.
   a. Ajoutez une étape en sélectionnant le gestionnaire associé dans la liste des **gestionnaires disponibles** et en cliquant sur **Ajouter**. Le gestionnaire passe dans la liste des **gestionnaires configurés**.
   b. Supprimez un gestionnaire en le sélectionnant dans la **Liste des éléments configurés** et cliquez sur **Retrait**. Le gestionnaire est déplacé vers la **Liste des éléments disponibles**.
   c. Pour modifier l'ordre d'appel des gestionnaires, sélectionnez un gestionnaire dans la liste et cliquez sur le bouton de **déplacement vers le haut** ou **déplacement vers le bas**.
   d. Pour exécuter un gestionnaire plusieurs fois, sélectionnez-le, puis cliquez sur **Répéter**.

      N'oubliez pas que tous les gestionnaires configurés pour une action sont appelés et que les étapes que les gestionnaires représentent sont exécutées en fonction de leur ordre dans la liste des **gestionnaires configurés**.
   e. Pour configurer le gestionnaire, sélectionnez-le dans la liste des **gestionnaires configurés** et cliquez sur **Configurer**. La liste des attributs pouvant être configurés s'affiche.
4. Cliquez sur **Sauvegarder**.

Création d'actions

Vous pouvez créer une action de l'une des manières suivantes :

- Créez une action et associez les gestionnaires à cette action.
- Copiez une action fournie par le produit et, si nécessaire, modifiez les gestionnaires qui lui sont associés.

Création d'une action

Pourquoi et quand exécuter cette tâche

Pour créer une action, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Actions**.
2. Cliquez sur **Créer**.
3. Attribuez un nom à l'action. Cette zone est obligatoire.
4. Entrez éventuellement une description de l'action.
5. Indiquez si l'action est activée pour l'utilisation.
6. Pour chaque étape qui sera appelée comme faisant partie de cette action, ajoutez le gestionnaire associé en le sélectionnant dans la liste des **gestionnaires disponibles** et en cliquant sur **Ajouter**. Le gestionnaire passe dans la liste des **gestionnaires configurés**.

   N'oubliez pas que les gestionnaires sont appelés par l'action dans l'ordre de la liste des **gestionnaires configurés**. Veillez à placer les gestionnaires dans l'ordre adéquat. Vous pouvez utiliser les boutons **Déplacement vers le haut** ou **Déplacement vers le bas** pour modifier l'ordre des gestionnaires, ou **Répéter** pour qu'un gestionnaire puisse être traité plusieurs fois.
7. Pour configurer un gestionnaire, sélectionnez-le dans la liste des **gestionnaires configurés** et cliquez sur **Configurer**. La liste des attributs pouvant être configurés s'affiche.
8. Cliquez sur **Sauvegarder**.

Copie d'une action
Pourquoi et quand exécuter cette tâche

Pour créer une action en copiant une action existante, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Actions**.
2. Dans la liste Actions, cliquez sur l'icône **Copie** en regard de l'action que vous souhaitez copier.
3. Attribuez un nom à l'action. Cette zone est obligatoire.
4. Entrez éventuellement une description de l'action.
5. Indiquez si l'action est activée pour l'utilisation.
6. Notez qu'une ou plusieurs étapes figurent déjà dans la **Liste configurée**. Il s'agit des étapes associées à l'action que vous avez copiée. Par exemple, si vous avez cloné l'action Annulation d'un processus RosettaNet par un partenaire interne, fournie par le système, la liste suivante de gestionnaires disponibles et configurés s'affiche :

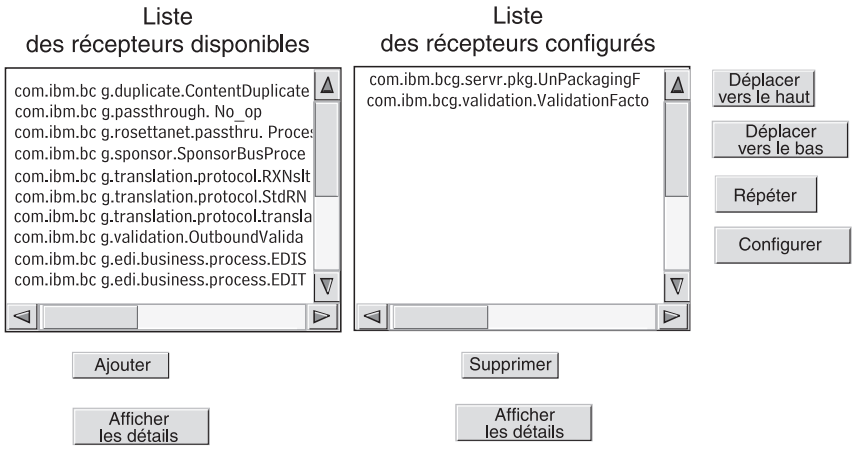


Figure 19. Clonage d'une action

Pour modifier la liste des **gestionnaires configurés**, effectuez une ou plusieurs des étapes suivantes :

a. Ajoutez une étape en sélectionnant le gestionnaire associé dans la liste des **gestionnaires disponibles** et en cliquant sur **Ajouter**. Le gestionnaire passe dans la liste des **gestionnaires configurés**.

b. Supprimez une étape en sélectionnant le gestionnaire associé dans la liste des **gestionnaires configurés** et en cliquant sur **Supprimer**. Le gestionnaire est déplacé vers la **Liste des éléments disponibles**.

c. Pour modifier l'ordre d'appel des gestionnaires, sélectionnez un gestionnaire dans la liste et cliquez sur le bouton de **déplacement vers le haut** ou **déplacement vers le bas**.

   N'oubliez pas que tous les gestionnaires configurés pour une action sont appelés et que les étapes associées à ces gestionnaires sont exécutées en fonction de leur ordre dans la liste des **gestionnaires configurés**.

d. Configurez l'étape en la sélectionnant dans la liste des **gestionnaires configurés** et en cliquant sur **Configurer**. La liste des attributs pouvant être configurés s'affiche.

7. Cliquez sur **Sauvegarder**.

Chapitre 9. Configuration des types de documents

Ce chapitre explique comment configurer les documents non EDI que vous échangerez avec les partenaires de la communauté et avec vos applications dorsales. La configuration des types de documents EDI et leurs interactions (à l'exception des documents EDI en transit) sont décrits au Chapitre 10, «Configuration des flux de documents EDI», à la page 179. Le Chapitre 10, «Configuration des flux de documents EDI», à la page 179 décrit également comment configurer les types de documents et les interactions pour les documents XML ou ROD (record-oriented-data).

Ce chapitre contient les rubriques suivantes :

Remarque : Pour effectuer des modifications de configurations sur WebSphere Partner Gateway, vous devez toujours utiliser la même instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Présentation des types de documents

Une définition de documents se compose, au minimum, d'un package, d'un protocole et d'un type de documents. Pour certains protocoles, il est possible de spécifier une activité, une action et un signal. Les définitions de documents précisent les types de documents qui seront traités par WebSphere Partner Gateway.

L'empaquetage est la logique requise pour empaqueter document en fonction d'une spécification, par exemple AS2. Un flux de protocole est la logique exigée pour traiter un document adhérant à un certain protocole, tel que EDI-X12. Un type de documents décrit l'aspect du document.

Les sections suivantes décrivent succinctement les étapes de définition d'un type de document entre le partenaire interne et un partenaire.

Etape 1 : Assurez-vous que la définition de documents est disponible

Pourquoi et quand exécuter cette tâche

Vérifiez qu'une définition de documents existe (parmi celles qui sont fournies prédéfinies avec le système). Si le flux n'existe pas encore, vous pouvez le créer en téléchargeant les fichiers nécessaires ou en créant manuellement une définition personnalisée.

Lors de la création d'une définition de documents, vous pouvez modifier certains attributs. Les attributs servent à diverses fonctions de traitement de document et de routage, comme la validation, la vérification pour chiffrement et le nombre de relances. Les attributs que vous définissez au niveau de la définition du document fournissent un paramétrage global du package, protocole ou type de documents associés. Les attributs disponibles varient selon la définition de documents. Les attributs des définitions de documents EDI sont différents de ceux des définitions de documents RosettaNet.

Par exemple, si vous indiquez une valeur pour l'attribut **Heure d'accusé de réception** du package AS, elle s'applique à tous les documents empaquetés avec AS (l'attribut **Heure d'accusé de réception** définit la durée d'attente d'un accusé de réception MDN avant de renvoyer la demande initiale). Si par la suite vous définissez l'attribut **Heure d'accusé de réception** au niveau des fonctions business-to-business, cette valeur supplante celle qui a été indiquée au niveau de la définition de documents.

Pour les attributs qui peuvent être définis à tous les niveaux de la définition de documents, les valeurs définies au niveau du type de document prévalent sur celles définies au niveau du protocole et ces dernières sont prioritaires sur celles paramétrées au niveau du package.

Le type de documents doit figurer sur la page Gérer des définitions de documents pour que vous puissiez créer des interactions. Pour la gestion des définitions de documents, voir le*Chapitre sur les tâches d'administration du concentrateur du Guide d'administration de WebSphere Partner Gateway.*

Etape 2 : Créez des interactions

Pourquoi et quand exécuter cette tâche

Créez des interactions pour les types de documents définis. L'interaction indique à WebSphere Partner Gateway les actions à effectuer sur un document. Pour certains échanges, deux flux suffisent : un pour décrire le document reçu dans le concentrateur (issu du partenaire ou du partenaire interne) et un qui décrit le document envoyé depuis le concentrateur (au partenaire externe ou au partenaire interne). Toutefois, si le concentrateur envoie ou reçoit un EDI qui sera fractionné en transactions individuelles, ou dans lequel des accusés de réception sont requis, vous créerez plusieurs interactions pour procéder à l'échange. Pour la gestion des interactions, voir le *Chapitre sur les tâches d'administration du concentrateur du Guide d'administration de WebSphere Partner Gateway.*

Etape 3 : Créez les profils, fonctions business-to-business et les destinations des partenaires

Pourquoi et quand exécuter cette tâche

Créez les profils de partenaire pour le partenaire interne et les partenaires externes. Définissez des destinations (qui déterminent à quel endroit les documents seront envoyés) et des fonctions business-to-business qui indiquent les documents que le partenaire interne et les partenaires externes peuvent envoyer et recevoir. La page Fonctions B2B répertorie tous les types de documents définis.

Vous pouvez définir des attributs au niveau des fonctions business-to-business. Tout attribut défini à ce niveau a la priorité sur ceux qui ont été définis au niveau de la définition de documents. Par exemple, si vous définissez **Heure d'accusé de réception** sur 30 au niveau de la définition de documents pour un package AS, puis la définissez sur 60 dans les fonctions business-to-business, la valeur 60 est utilisée. Le fait de définir un attribut au niveau business-to-business vous permet de le personnaliser en fonction d'un partenaire spécifique.

Etape 4 : Activez les connexions

Pourquoi et quand exécuter cette tâche

Activez les connexions entre les partenaires internes et externes. Les connexions disponibles dépendent des interactions qui sont créées. Les interactions reposent sur les fonctions business-to-business. Ces dernières dépendent de la disponibilité des définitions de documents.

Pour certains échanges, une seule connexion est requise. Par exemple, si un partenaire envoie un document binaire à une application dorsale du partenaire interne, une seule connexion est requise. Toutefois, dans le cadre des échanges EDI pour lesquels l'EDI est désenveloppé et les transactions individuelles transformées, plusieurs connexions sont définies.

Remarque : Les EDI transmis tels quels n'exigent qu'une seule connexion.

Vous pouvez définir des attributs au niveau de la connexion. Tout attribut défini à ce niveau remplace ceux qui ont été définis au niveau des fonctions business-to-business. Par exemple, si vous définissez **Heure d'accusé de réception** sur 60 au niveau des fonctionnalités business-to-business pour le package AS2, puis la définissez sur 120, c'est cette valeur qui est utilisée. Le fait de définir la valeur d'un attribut au niveau de la connexion permet de le personnaliser selon les besoins en routage des partenaires et applications impliqués.

Exemple de flux

Pourquoi et quand exécuter cette tâche

Par défaut, plusieurs méthodes d'empaquetage sont activées. Pour illustrer la procédure globale d'établissement des définitions de documents, prenons le cas d'un accord passé avec un partenaire externe, portant sur la réception d'un EDI conforme au standard EDI-X12. Le partenaire envoie le document dans un package AS2. Vous indiquez que l'EDI sera envoyé tel quel (sans transformation) à une application dorsale, sans empaquetage.

1. Sur la page Gérer les définitions de documents, vérifiez que la définition de documents (qui décrit le type de document envoyé dans le concentrateur par le partenaire externe) est activée.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
   b. Cliquez sur l'icône **Développer** en regard de **Package : AS**. Notez que **EDI-X12** figure déjà dans la liste.
   c. Cliquez sur l'icône **Développer** en regard de **Protocole : EDI-X12**. Notez que **Type de documents : ISA** figure déjà dans la liste.
2. Sur la page Gérer la définition de documents, vérifiez que la seconde définition de documents (qui décrit le type de document envoyé à l'application dorsale) est activée.
   a. Cliquez sur l'icône **Développer** en regard de **Package : None**. Notez que **EDI-X12** figure déjà dans la liste.
   b. Cliquez sur l'icône **Développer** en regard de **Protocole : EDI-X12**. Notez que **Type de documents : ISA** figure déjà dans la liste.
3. Créez une interaction indiquant si le type de documents sera un type source ou un type cible.
   a. La page Gérer la définition de documents étant toujours affichée, cliquez sur le lien **Gérer des interactions**.
   b. Dans la colonne Source, développez **Package : AS**, **Protocole : EDI-X12 (TOUT)**, puis cliquez sur **Type de documents : ISA**.
   c. Dans la colonne Cible, développez **Package : None**, **Protocole : EDI-X12 (TOUT)**, puis cliquez sur **Type de documents : ISA**.
   d. Dans cet exemple, aucune transformation n'a lieu. Par conséquent, ne sélectionnez aucun élément dans la liste **Mappe de transformation**.
   e. Dans la liste des **Actions**, sélectionnez **Passe-système**.
   f. Cliquez sur **Sauvegarder**.

A ce point, vous avez précisé si le concentrateur accepte les échanges EDI-X12 (standard ISA) empaquetés en tant que AS. Vous avez également indiqué qu'il est capable d'en envoyer sans empaquetage. Vous avez précisé que l'EDI ne doit faire l'objet d'aucune transformation. Il est simplement transmis à l'application dorsale (une fois les en-têtes AS supprimés).

Tableau 5. Interactions fournies par le produit pour Open PGP

Du côté expéditeur, définissez cette connexion	**Du côté récepteur, définissez cette connexion**
None/EDI-X12/ISA vers None/EDI-X12/ISA	None/EDI-X12/ISA vers None/EDI-X12/ISA
Backend integration/EDI-X12/ISA vers None/EDI-X12/ISA	None/EDI-X12/ISA vers None/EDI-X12/ISA

Remarque : EDI-X12 n'étant pas présent par défaut dans l'intégration dorsale, vous devez ajouter "EDI-X12" au contexte de l'intégration dorsale. Après avoir ajouté"EDI-X12" au contexte de l'intégration dorsale, ajoutez "ISA" au contexte de l'intégration dorsale - EDI-X12.

Vous n'avez pas encore précisé quel partenaire peut envoyer ce type d'EDI au concentrateur. Pour cela, vous devez définir le profil et les fonctions business-to-business du partenaire (mais aussi un profil et des fonctions business-to-business pour le système dorsal du partenaire interne). Une fois ces tâches effectuées, créez une connexion entre le partenaire et l'application dorsale. La figure 20 affiche la connexion entre le partenaire et l'application dorsale du partenaire interne pour cet exemple.

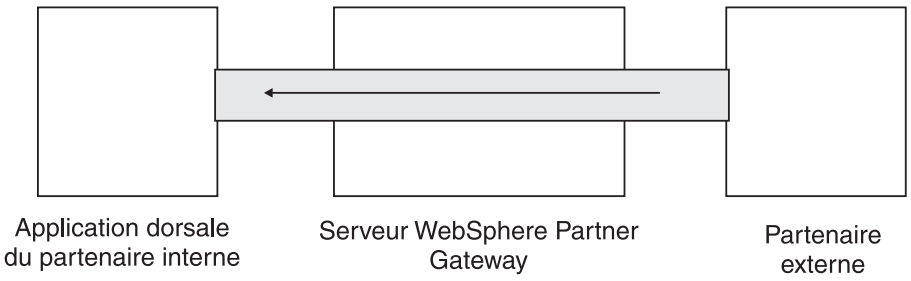


Figure 20. Une connexion unidirectionnelle depuis un partenaire vers des partenaires internes

Vous pouvez vérifier l'existence d'une connexion dans la page Gestion des connexions (**Administrateur du compte > Connexions > Connexions partenaire**). Dans la page Gestion des connexions, sélectionnez le partenaire dans la liste **Source**, le partenaire interne dans la liste **Cible**, puis cliquez sur **Rechercher**. La connexion disponible s'affiche. Si nécessaire, vous pouvez modifier les attributs et actions en appliquant les procédures décrites dans les sections suivantes.

Il existe trois types de définitions de documents : ceux qui sont fournis avec le système et peuvent être sélectionnés depuis la console, ceux qui sont déjà définis mais qui ne figurent pas encore sur la console de communauté (vous avez téléchargé ces définitions depuis le support d'installation WebSphere ou depuis un autre emplacement) et ceux que vous créez vous-même. Pour chaque type de définition de documents, vous pouvez (et parfois devez) préciser des attributs ou télécharger des mappes qui permettent de les configurer plus précisément.

Documents binaires

Les documents binaires sont les documents qui sont transmis à travers le concentrateur en l'état. Ces documents sont échangés entre un partenaire externe et un partenaire interne à l'aide d'une application dorsale. Vous devez définir les profils et fonctions business-to-business (B2B) des partenaires internes et externes avant de pouvoir créer des connexions entre eux. Si le partenaire interne par défaut n'est pas utilisé, l'ID récepteur du partenaire interne doit être défini explicitement. Lorsque le document binaire est routé via le protocole de transport HTTP à l'aide de l'authentification de base, l'ID récepteur peut transiter par l'attribut **X-aux-receiver-id**. Avec le protocole FTP, un partenaire externe peut envoyer des documents binaires au concentrateur. Le protocole binaire est déjà disponible pour les packages AS, None et Backend Integration. De ce fait, l'«Etape 1 : Assurez-vous que la définition de documents est disponible», à la page 112 est déjà effectuée.

Remarque : Vous pouvez ajouter des attributs au niveau Package, Protocole ou Type de documents pour modifier le traitement par défaut, en cliquant sur l'icône **Edition des valeurs d'attribut**. Par défaut, aucun attribut n'est associé au protocole binaire ou au type de documents.

Par défaut, quatre interactions impliquant des documents binaires sont déjà fournies pour WebSphere Partner Gateway et trois interactions sont nouvellement fournies pour Open PGP. Pour ces interactions, vous n'avez pas besoin d'exécuter «Etape 2 : Créez des interactions», à la page 112. Des interactions sont fournies pour les échanges suivants :

Tableau 6. Interactions fournies par le produit

Package/protocole/type de documents source	**Package/protocole/type de documents cible**
AS/binaire/binaire	Backend Integration/binaire/binaire
Backend Integration/binaire/binaire	AS/binaire/binaire
AS/binaire/binaire	None/binaire/binaire
None/binaire/binaire	AS/binaire/binaire

Pour OpenPGP, activez manuellement les interactions prises en charge suivantes depuis la console de WebSphere Partner Gateway :

Tableau 7. Interactions OpenPGP prises en charge

Package/protocole/type de documents source	**Package/protocole/type de documents cible**
None/binaire/binaire	None/binaire/binaire
Backend Integration/binaire/binaire	None/binaire/binaire

Pour échanger des documents binaires, vous devez toujours appliquer les étapes suivantes :

- «Etape 3 : Créez les profils, fonctions business-to-business et les destinations des partenaires», à la page 113, qui est décrit dans Chapitre 3, «Création et configuration de partenaires», à la page 25, et Chapitre 11, «Création de destinations», à la page 229.
- «Etape 4 : Activez les connexions», à la page 113, dans le Chapitre 12, «Gestion des connexions», à la page 253.

Documents EDI avec actions de passe-système

WebSphere Partner Gateway offre la possibilité de désenvelopper et de transformer des EDI. Cette procédure est décrite au Chapitre 10, «Configuration des flux de documents EDI», à la page 179.

figure 21, à la page 117 affiche le flux d'un échange EDI transmis depuis un partenaire au partenaire interne.

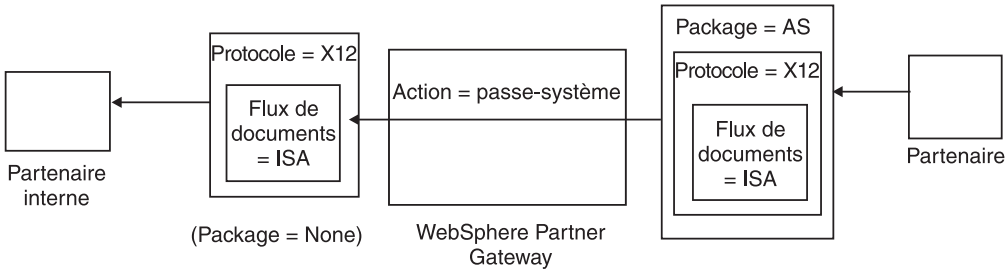


Figure 21. EDI entrant avec action passe-système

Dans cet exemple, les en-têtes AS2 sont supprimés, mais le reste de l'échange est laissé intact et traverse le système vers la destination du partenaire interne.

Dans la transformation synchrone de transaction EDI avec WTX (EDI vers Any), si la transformation a plus d'une sortie alors, reposant sur l'option de redirection, les enfants seront directement transmis au flux de travaux sortant ou redirigés dans le flux de travaux entrant fixe pour passer dans un nouveau canal. Dans les cas asynchrones, WTX envoie les transactions EDI vers WPG pour l'enveloppement. Vous devez définir les connexions des deux canaux - <none> / <EDI Dictionary> / <EDI document > {EDI Trx} avec passe-système et <NA> / <EDI interchange> / <,EDI ISA / UNB> to <Any Package> / <EDI X12 / <FACT> / <EDI ISA / UNB avec action en tant que passe-système.

Création de définitions de documents

Pourquoi et quand exécuter cette tâche

Le type de documents pour les échanges de passe-système EDI est déjà disponible (par défaut) sur la page Gérer des définitions de documents, décrite dans la section «Exemple de flux», à la page 113. Si vous souhaitez modifier l'un des attributs dotés de valeurs par défaut ou définir la valeur d'un attribut, vous pouvez utiliser la page Gérer les définitions de documents.

Supposons que vous souhaitiez modifier l'attribut **Heure d'accusé de réception** d'un document EDI empaqueté avec AS. Voici comment procéder :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur l'icône **Edition des valeurs d'attribut** en regard de **Package : AS**.
3. Faites défiler la page vers le bas, jusqu'à la section **Attributs de contexte de définition de documents**.
4. Sur la ligne **Heure d'accusé de réception**, tapez une valeur différente dans la colonne **Mettre à jour**.
5. Cliquez sur **Sauvegarder**.

Notez que, dans cet exemple, vous avez modifié un attribut d'empaquetage. Les attributs de protocole (par exemple, EDI-X12) et de type de documents (par exemple, ISA) ne conviennent pas à une action de passe-système. Cet attribut d'empaquetage s'applique à tous les documents compris dans le package AS.

Création d'interactions

Pourquoi et quand exécuter cette tâche

Pour créer l'interaction pour un EDI avec action passe-système, procédez comme suit :

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Sous **Source**, développez **Package : AS** et **Protocole : EDI-X12**, puis sélectionnez **Type de documents : ISA**.
4. Sous **Cible**, développez **Package : None** et **Protocole : EDI-X12**, puis sélectionnez **Type de documents : ISA**.
5. Sélectionnez éventuellement une **mappe de transformation**.
6. Dans la liste des **actions**, sélectionnez **Passe-système**.

Les étapes 1 à 4 ont permis à WebSphere Partner Gateway d'accepter un échange EDI-X12 empaqueté en tant que AS, à partir d'un partenaire source, pour envoyer un échange EDI-X12 sans empaquetage vers le partenaire cible et autoriser le transfert passe-système de la source vers la cible.

Si vous souhaitez définir une interaction avec un document source empaqueté en tant que None/EDI-X12/ISA et un document cible empaqueté en tant que AS/EDI-X12/ISA, développez **Package : None** à l'étape 3 (dans la colonne **Source**) puis développez **Package : AS** à l'étape 4 (dans la colonne **Cible**).

Documents RosettaNet

RosettaNet est une organisation qui fournit des normes ouvertes permettant de gérer l'échange de messages commerciaux entre des partenaires. Pour plus d'informations sur RosettaNet, voir http://www.rosettanet.org. Les normes comprennent les spécifications RNIF (RosettaNet Implementation Framework) et PIP (Partner Interface Process). RNIF définit l'échange de messages entre des partenaires commerciaux en fournissant une structure d'empaquetage de messages, de protocoles de transport et de sécurité. Deux versions ont été publiées : 1.1 et 2.0. Une processus PIP définit un processus métier public ainsi que les formats de message XML permettant la prise en charge de ce processus.

WebSphere Partner Gateway prend en charge l'échange de messages RosettaNet conformes aux spécifications RNIF 1.1 et 2.0. Lorsque le concentrateur reçoit un message PIP, il le valide et le transforme pour l'envoyer au système dorsal approprié. WebSphere Partner Gateway fournit un protocole permettant l'empaquetage du message transformé en un message RNSC (RosettaNet Service Content) que le système dorsal peut traiter. Pour plus d'informations sur l'empaquetage utilisé avec ces messages pour fournir des informations de routage, reportez-vous au *Guide d'intégration d'entreprise de WebSphere Partner Gateway*.

Le concentrateur peut également recevoir des messages RNSC à partir de systèmes dorsaux et créer le message PIP approprié puis l'envoyer au partenaire d'échanges qui convient (un partenaire). Vous fournissez les définitions de documents pour la version RNIF et les processus PIP que vous souhaitez utiliser.

En plus d'assurer l'acheminement des messages RosettaNet, WebSphere Partner Gateway maintient un état pour chaque message traité. Il peut ainsi renvoyer les messages qui échouent jusqu'à ce que le nombre de tentatives atteigne un seuil

spécifié. Le Mécanisme de notification d'événements alerte les systèmes dorsaux si un message PIP ne peut pas être remis. En outre, le concentrateur peut générer automatiquement des PIP 0A1 à envoyer aux partenaires appropriés s'il reçoit certains messages de notification d'événement provenant des systèmes dorsaux. Pour plus d'informations sur la notification d'événement, reportez-vous au *Guide d'intégration d'entreprise de WebSphere Partner Gateway*.

Packages RNIF et PIP

Pour prendre en charge l'échange de messages RosettaNet, WebSphere Partner Gateway fournit deux jeux de fichiers compressés appelés packages. Le *packages RNIF* comportent les définitions de documents nécessaires pour prendre en charge le protocole RNIF. Ces packages se trouvent dans le répertoire B2BIntegrate.

Pour RNIF V1.1, les packages sont :

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

Pour RNIF V02.00, les packages sont :

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

Le premier package de chaque paire fournit les définitions de documents requises pour la prise en charge des communications RosettaNet avec les partenaires, tandis que le second fournit les définitions nécessaires pour la prise en charge des communications RosettaNet avec les systèmes dorsaux.

Le second jeu de packages se compose de packages de types de documents PIP. Chaque package de type de documents PIP comporte un répertoire Packages contenant un fichier XML et un répertoire GuidelineMaps contenant des fichiers XSD. Le fichier XML spécifie les définitions de documents qui déterminent le mode de traitement du processus PIP par WebSphere Partner Gateway et définissent les messages et signaux échangés. Les fichiers XSD spécifient le format des messages du processus PIP et précisent les valeurs acceptées pour les éléments XML de ces messages. Les fichiers compressés des processus PIP 0A1 contiennent également un fichier XML que le concentrateur utilise comme modèle pour créer des documents 0A1.

Le processus PIP pour lesquels WebSphere Partner Gateway fournit des packages de type de documents PIP sont les suivants :

- PIP 0A1 Notification of Failure v1.0
- PIP 0A1 Notification of Failure V02.00.00
- PIP 2A1 Distribute New Product Information V02.00.00
- PIP 2A12 Distribute Product Master V01.03.00
- PIP 3A1 Request Quote V02.00.00
- PIP 3A2 Request Price and Availability R02.01.00
- PIP 3A4 Request Purchase Order V02.02.00
- PIP 3A4 Request Purchase Order V02.00
- PIP 3A5 Query Order Status R02.00.00
- PIP 3A6 Distribute Order Status V02.02.00
- PIP 3A7 Notify of Purchase OrderUpdate V02.02.00
- PIP 3A8 Request Purchase Order Change V01.02.00

- PIP 3A8 Request Purchase Order Change V01.03.00
- PIP 3A9 Request Purchase Order Cancellation V01.01.00
- PIP 3B2 Notify of Advance Shipment V01.01.00
- PIP 3B3 Distribute Shipment Status R01.00.00
- PIP 3B11 Notify of Shipping Order R01.00.00A
- PIP 3B12 Request Shipping Order V01.01.00
- PIP 3B13 Notify of Shipping Order Confirmation V01.01.00
- PIP 3B14 Request Shipping Order Cancellation V01.00.00
- PIP 3B18 Notify of Shipping Documentation V01.00.00
- PIP 3C1 Return Product V01.00.00
- PIP 3C3 Notify of Invoice V01.01.00
- PIP 3C4 Notify of Invoice Reject V01.00.00
- PIP 3C6 Notify of Remittance Advice V01.00.00
- PIP 3C7 Notify of Self-Billing Invoice V01.00.00
- PIP 3D8 Distribute Work in Process V01.00.00
- PIP 4A1 Notify of Strategic Forecast V02.00.00
- PIP 4A3 Notify of Threshold Release Forecast V02.00.00
- PIP 4A4 Notify of Planning Release Forecast R02.00.00A
- PIP 4A5 Notify of Forecast Reply V02.00.00
- PIP 4B2 Notify of Shipment Receipt V01.00.00
- PIP 4B3 Notify of Consumption V01.00.00
- PIP 4C1 Distribute Inventory Report V02.03.00
- PIP 4C1 Distribute Inventory Report V02.01
- PIP 5C1 Distribute Product List V01.00.00
- PIP 5C2 Request Design Registration V01.00.00
- PIP 5C4 Distribute Registration Status V01.02.00
- PIP 5D1 Request Ship From Stock And Debit Authorization V01.00.00
- PIP 6C1 Query Service Entitlement V01.00.00
- PIP 6C2 Request Warranty Claim V01.00.00
- PIP 7B1 Distribute Work in Process V01.00.00
- PIP 7B5 Notify of Manufacturing Work Order V01.00.00
- PIP 7B6 Notify of Manufacturing Work Order Reply V01.00.00

Pour chaque processus PIP, il existe quatre packages de type de documents PIP :

- Pour l'échange de messages RNIF 1.1 avec les partenaires
- Pour l'échange de messages RNIF 1.1 avec les systèmes dorsaux
- Pour l'échange de messages RNIF 2.0 avec les partenaires
- Pour l'échange de messages RNIF 2.0 avec les systèmes dorsaux

Chaque package de type de documents PIP respecte sa propre convention de dénomination, ce qui vous permet de déterminer s'il concerne les messages entre WebSphere Partner Gateway et les partenaires ou entre WebSphere Partner Gateway et les systèmes dorsaux. Cette convention identifie également la version RNIF, le processus PIP et la version PIP prise en charge par le package. Pour les packages de type de documents PIP destinés à l'échange de messages entre WebSphere Partner Gateway et les partenaires, le format est le suivant :

`BCG_Package_RNIF<version_RNIF>_<PIP><version_PIP>.zip`

Pour les packages de types de documents PIP destinés à l'échange de messages entre WebSphere Partner Gateway et les systèmes dorsaux, le format est le suivant :

`BCG_Package_RNSC<version_Backend_Integration>_RNIF<version_RNIF>_<PIP><version_PIP>.zip`

Par exemple, le fichier BCG_Package_RNIF1.1_3A4V02.02.zip sert à valider les documents pour la Version 02.02 du processus PIP 3A4 qui sont échangés entre les partenaires et WebSphere Partner Gateway à l'aide du protocole RNIF 1.1. Quant aux packages de type de documents PIP permettant la communication avec les systèmes dorsaux, leur nom doit également indiquer le protocole utilisé pour envoyer le contenu RosettaNet aux systèmes dorsaux. Pour plus d'informations sur l'empaquetage utilisé avec ces messages, reportez-vous au *Guide d'intégration d'entreprise de WebSphere Partner Gateway*.

Création de définitions de documents

Pourquoi et quand exécuter cette tâche

Pour l'échange de messages RosettaNet, WebSphere Partner Gateway exige les packages RNIF de la version utilisée pour envoyer les messages. Pour chaque processus PIP pris en charge par WebSphere Partner Gateway, il faut les deux packages de type de documents PIP pour la version RNIF. Par exemple, pour prendre en charge le processus PIP 3A4 sur RNIF 2.0, WebSphere Partner Gateway exige les packages suivants :

- 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

Le premier package prend en charge l'échange de messages RosettaNet avec les partenaires, le second l'échange de messages RosettaNet avec les systèmes dorsaux. Les troisième et quatrième packages permettent à WebSphere Partner Gateway de transmettre des messages 3A4 entre des partenaires et des systèmes dorsaux par le biais du protocole RNIF 2.0.

Pour télécharger des packages RosettaNet :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur **Téléchargement des packages**.
3. Sélectionnez **Non** pour **Package WSDL**.
4. Cliquez sur **Parcourir** et sélectionnez le package RNIF pour communiquer avec les partenaires.

   Par défaut, les packages RNIF sont situés dans le répertoire B2BIntegrate/Rosettanet du support d'installation. Par exemple, si vous téléchargez le package RNIF version 2.00, vous devez accéder au répertoire B2BIntegrate/Rosettanet et sélectionner : Package_RNIF_V0200.zip.
5. Assurez-vous que le paramètre **Validation dans la base de données** est sur **Oui**.
6. Cliquez sur **Télécharger**.
7. Cliquez de nouveau sur **Parcourir** et sélectionnez le package RNIF pour communiquer avec les applications dorsales.

Par exemple, si vous téléchargez le package RNIF version 2.00, vous devez accéder au répertoire B2BIntegrate/Rosettanet et sélectionner Package_RNSC_1.0_RNIF_V02.00.zip.

8. Cliquez sur **Télécharger**.

   Les packages nécessaires pour communiquer avec les partenaires ou le système dorsal sont à présent installés sur le système. Si vous consultez la page Gérer les définitions de documents, vous voyez une entrée pour **Package : RNIF/Protocole : RosettaNet**, qui représente l'empaquetage pour communiquer avec les partenaires, et **Package : Backend Integration/Protocole : RNSC**, qui est l'empaquetage pour communiquer avec les applications dorsales.

9. Pour chaque PIP que vous souhaitez prendre en charge, téléchargez l'empaquetage de flux de documents PIP pour le processus PIP et la version RNIF que vous prenez en charge. Par exemple, pour télécharger le PIP 3A6 (Notify of Remittance Advice) à envoyer à un partenaire, procédez comme suit :

   a. Cliquez sur **Parcourir** et sélectionnez BCG_Package_RNIFV02.00_3C6V02.02 dans le répertoire B2BIntegrate/Rosettanet.

   b. Assurez-vous que le paramètre **Validation dans la base de données** est sur **Oui**.

   c. Cliquez sur **Télécharger**.

   Le PIP 3C6V02.02 apparaît comme étant le type de documents sous **Package : RNIF/Protocole : RosettaNet** sur la page Gérer les définitions de documents. Une activité, une action et deux signaux sont également affichés. Ils sont inclus dans le téléchargement du PIP.

   Pour télécharger le PIP 3A6 à envoyer à l'application dorsale, procédez comme suit :

   a. Cliquez sur **Parcourir** et sélectionnez BCG_Package_RNSC1.0_RNIFV02.00_3C6V02.02.zip.

   b. Assurez-vous que le paramètre **Validation dans la base de données** est sur **Oui**.

   c. Cliquez sur **Télécharger**.

   Le PIP 3C6V02.02 apparaît désormais comme étant le type de documents sous **Package : Backend Integration/Protocole : RNSC** , sur la page Gérer les définitions de type de documents. Si WebSphere Partner Gateway ne fournit pas d'empaquetage pour le processus ou la version PIP que vous souhaitez utiliser, vous pouvez créer votre propre package et le télécharger. Pour plus d'informations, voir «Création de packages de définition de documents PIP», à la page 389.

Configuration des valeurs d'attribut

Pourquoi et quand exécuter cette tâche

Pour les définitions de documents PIP, la plupart des valeurs des attributs sont déjà définies et ne nécessitent pas de configuration. Toutefois, vous devez définir les attributs suivants :

Package RNIF (1.0)

- **GlobalSupplyChainCode** - Identifie le type de chaîne d'approvisionnement utilisée par le partenaire. Les différents types sont Composants électroniques, Technologie d'informations et Fabrication de semiconducteurs. Cet attribut n'a pas de valeur par défaut.

Package RNIF (V02.00)

- **Chiffrement** - Définit si les processus PIP doivent comporter des données utiles chiffrées, un conteneur et des données utiles chiffrés ou aucun chiffrement. La valeur par défaut est Aucun.
- **Accusé de réception de synchronisation requise** - Défini sur Oui si le partenaire souhaite recevoir l'accusé de réception. Défini sur Non si un 200 est demandé.
- **Synchronisation prise en charge** - Définit si le processus PIP prend en charge les échanges de message synchrones. La valeur par défaut est Non.

Notez que les processus PIP pour lesquels WebSphere Partner Gateway fournit des packages de types de documents PIP ne sont pas synchrones. En conséquence, il n'est pas nécessaire de modifier les attributs Accusé de réception de synchronisation requise et Synchronisation prise en charge pour ces processus PIP.

Remarque : Le comportement de l'attribut Accusé de réception de synchronisation requise est différent entre les processus PIP à sens unique et à double sens. Pour un processus PIP à double sens, lorsque l'attribut Accusé de réception de synchronisation requise a la valeur Non, ce paramètre prend le pas sur un paramètre Irréfutabilité de l'avis de réception ayant la valeur Oui. Par exemple, si vous envoyez un 3A7 avec les paramètres suivants :

- SiqReq=Y
- NonRepofRec=Y
- SyncSupported=Y
- SyncAckReq=N

Pour un processus PIP à double sens, vous recevez un message d'erreur sur le document entrant. Pour un processus PIP unidirectionnel, cependant, vous voyez le document entrant sur la console et un code 0KB 200 est renvoyé au partenaire.

Pour définir les attributs, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur les icônes **Développer** pour développer un noeud jusqu'au niveau Définition de documents approprié, ou sélectionnez **Tout** pour développer tous les noeuds de définition de documents de l'arborescence.
3. Dans la colonne **Actions**, cliquez sur l'icône **Edition des valeurs d'attribut** du package que vous souhaitez modifier (par exemple Package : RNIF (1.1) ou Package : RNIF (V02.00)).
4. Dans la section **Attributs de contexte de définition de documents**, allez dans la colonne **Mettre à jour** de l'attribut que vous souhaitez définir et sélectionnez ou entrez la nouvelle valeur. Répétez l'opération pour chaque attribut à définir.
5. Cliquez sur **Sauvegarder**.

Remarque : Vous pouvez également mettre à jour les attributs RosettaNet au niveau de la connexion en cliquant sur **Attributs** pour la source et la cible puis en entrant ou modifiant les valeurs de la colonne **Mettre à jour**. Voir «Spécification ou modification des attributs», à la page 255.

Création d'interactions

Pourquoi et quand exécuter cette tâche

La procédure suivante décrit la création d'une interaction entre un système dorsal et un partenaire. Notez que vous devez créer une interaction pour chaque processus PIP que vous souhaitez envoyer et une pour chaque processus PIP que vous souhaitez recevoir.

Avant de commencer, assurez-vous que les définitions appropriées de documents RNIF ont été téléchargées, ainsi que les packages du processus PIP que vous souhaitez utiliser. Si vous voulez pouvoir générer un PIP 0A1 (Notification of Failure), assurez-vous de l'avoir téléchargé, ainsi que décrit à l'étape 9, à la page 122.

Pour créer une interaction pour un PIP particulier, procédez comme suit :

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez l'arborescence **Source** jusqu'au niveau **Action** et l'arborescence **Cible** jusqu'au niveau **Action**.
4. Dans les arborescences, sélectionnez les définitions de documents à utiliser pour les contextes source et cible. Par exemple, si le partenaire est l'initiateur d'un processus PIP 3C6 (PIP à une action), sélectionnez les définitions de documents suivantes :

Tableau 8. Processus PIP 3C6 lancé par un partenaire

Source	Cible
Package : RNIF (V02.00)	Package : Backend Integration (1.0)
Protocole : RosettaNet (V02.00)	Protocole : RNSC (1.0)
Type de document : 3C6 (V01.00)	Type de document : 3C6 (V01.00)
Activité : Notification d'avis de paiement	Activité : Notification d'avis de paiement
Action : Action de notification d'avis de paiement	Action : Action de notification d'avis de paiement

Si le système dorsal est l'initiateur du processus PIP 3C6, sélectionnez les définitions de documents suivantes :

Tableau 9. Processus PIP 3C6 lancé par un système dorsal

Source	Cible
Package : Backend Integration (1.0)	Package : RNIF (V02.00)
Protocole : RNSC (1.0)	Protocole : RosettaNet (V02.00)
Type de document : 3C6 (V01.00)	Type de document : 3C6 (V01.00)
Activité : Notification d'avis de paiement	Activité : Notification d'avis de paiement
Action : Action de notification d'avis de paiement	Action : Action de notification d'avis de paiement

Pour un processus PIP à deux actions tel qu'un processus 3A4 lancé par un partenaire, sélectionnez les définitions de documents suivantes pour la première action :

Tableau 10. Processus PIP 3A4 lancé par un partenaire

Source	Cible
Package : RNIF (V02.00)	Package : Backend Integration (1.0)
Protocole : RosettaNet (V02.00)	Protocole : RNSC (1.0)
Type de documents : 3A4 (V02.02)	Type de documents : 3A4 (V02.02)
Activité : Demande de bon de commande	Activité : Demande de bon de commande
Action : Action de demande de bon de commande	Action : Action de demande de bon de commande

Si un système dorsal lance le processus PIP à deux actions 3A4, sélectionnez les définitions de documents suivantes pour la première action :

Tableau 11. Processus PIP 3A4 lancé par un système dorsal

Source	Cible
Package : Backend Integration (1.0)	Package : RNIF (V02.00)
Protocole : RNSC (1.0)	Protocole : RosettaNet (V02.00)
Type de documents : 3A4 (V02.02)	Type de documents : 3A4 (V02.02)
Activité : Demande de bon de commande	Activité : Demande de bon de commande
Action : Action de demande de bon de commande	Action : Action de demande de bon de commande

5. Dans la zone Action, sélectionnez **Translation bidirectionnelle de RosettaNet et de RosettaNet Service Content avec Validation**.
6. Cliquez sur **Sauvegarder**.
7. Si vous configurez un processus PIP à deux actions, répétez les étapes nécessaires pour créer l'interaction pour la seconde action. Par exemple, sélectionnez les définitions de documents suivantes pour la seconde action d'un processus PIP 3A4 lancé par un partenaire. Il s'agit de l'action par laquelle le système dorsal envoie la réponse.

Tableau 12. Processus PIP 3A4 lancé par un partenaire (seconde action)

Source	Cible
Package : Backend Integration (1.0)	Package : RNIF (V02.00)
Protocole : RNSC (1.0)	Protocole : RosettaNet (V02.00)
Type de documents : 3A4 (V02.02)	Type de documents : 3A4 (V02.02)
Activité : Demande de bon de commande	Activité : Demande de bon de commande
Action : Action de confirmation de bon de commande	Action : Action de confirmation de bon de commande

Pour la seconde action d'un processus PIP 3A4 lancé par un système dorsal, sélectionnez les définitions de documents suivantes :

Tableau 13. Processus PIP 3A4 lancé par un système dorsal (seconde action)

Source	Cible
Package : RNIF (V02.00)	Package : Backend Integration (1.0)
Protocole : RosettaNet (V02.00)	Protocole : RNSC (1.0)
Type de documents : 3A4 (V02.02)	Type de documents : 3A4 (V02.02)
Activité : Demande de bon de commande	Activité : Demande de bon de commande

Tableau 13. Processus PIP 3A4 lancé par un système dorsal (seconde action) (suite)

Source	Cible
Action : Action de confirmation de bon de commande	Action : Action de confirmation de bon de commande

8. Si vous voulez générer la Notification of Failure 0A1, créez une interaction pour XMLEvent.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Création d'une interaction**.
   c. Développez l'arborescence **Source** jusqu'au niveau **Type de documents** et l'arborescence **Cible** jusqu'au niveau **Type de documents**.
   d. Sélectionnez les définitions de documents suivants :

Tableau 14. Définition de documents d'événement XML

Source	Cible
Package : Backend Integration (1.0)	Package : Backend Integration (1.0)
Protocole : XMLEvent (1.0)	Protocole : XMLEvent (1.0)
Type de documents : XMLEvent (1.0)	Type de documents : XMLEvent (1.0)

   e. Dans la zone Action, sélectionnez **Passe-système**.
   f. Cliquez sur **Sauvegarder**.
9. Création d'une interaction pour XMLEvent vers 0A1 RNSC.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Développez l'arborescence **Source** jusqu'au niveau **Type de documents** et l'arborescence **Cible** jusqu'au niveau **Activité**.
   d. Sélectionnez les définitions de documents suivants :

Tableau 15. Définition de documents d'événement XML à 0A1

Source	Cible
Package : Backend Integration (1.0)	Package : Backend Integration (1.0)
Protocole : XMLEvent (1.0)	Protocole : RNSC (1.0)
Type de documents : XMLEvent (1.0)	Type de documents : 0A1 (V02.00)
	Activité : Distribution de notification d'échec.

   e. Dans la zone Action, sélectionnez **Translation bidirectionnelle de RosettaNet et XML avec Validation**.
   f. Cliquez sur **Sauvegarder**.

Remarque : Pour l'activation ou la désactivation des événements XML, voir *Activation ou désactivation des événements XML du guide d'intégration de l'entreprise*

Affichage des documents RosettaNet

Pourquoi et quand exécuter cette tâche

L'Afficheur RosettaNet affiche les informations sur les documents RosettaNet. Vous pouvez afficher des documents bruts ainsi que les détails des traitements et les événements associés, en précisant les critères de recherche. Ces informations sont intéressantes si vous essayez de savoir si un document a bien été livré ou de déterminer la cause d'un problème.

Affichez l'afficheur RosettaNet, en entrant ce qui suit :

1. Cliquez sur **Afficheurs> Afficheur RosettaNet**.
2. Sélectionnez les critères de recherche appropriés dans les listes, comme indiqué dans tableau 16.

Tableau 16. Critères de recherche RosettaNet

Valeur	Description
Date et heure de début	Date et heure auxquelles le processus a été initié.
Date et heure de fin	Date et heure auxquelles le processus s'est terminé.
Partenaire source et cible	Identifie les partenaires source (expéditeur) et cible (destinataire) (partenaire interne uniquement).
Partenaire	Indique si la recherche s'applique à tous les partenaires ou au partenaire interne uniquement.
Mon rôle est	Indique si la recherche s'applique aux documents pour lesquels le partenaire est la cible ou la source.
ID métier source	Numéro d'identification métier du partenaire expéditeur. Par exemple, DUNS.
Mode d'opération	Production ou test. Test est disponible uniquement sur les systèmes qui prennent en charge le mode d'opération test.
Protocole	Protocoles disponibles pour les partenaires.
Type de document	Processus métier spécifique.
ID Instance du processus	Numéro d'identification unique attribué au processus. Les critères de recherche peuvent inclure le caractère générique astérisque (*).
Trier par	Trier les résultats par : • Horodatage cible • Type de document La valeur par défaut est Horodatage cible.
Ordre décroissant ou Ordre croissant	Ordre décroissant affiche en premier l'horodatage le plus récent ou le début de l'alphabet. Ordre croissant affiche en premier l'horodatage le moins récent ou la fin de l'alphabet. La valeur par défaut est Ordre décroissant.
Résultats par page	Indique le nombre de résultats affichés par page.

3. Cliquez sur **Rechercher**.

Documents CIDX

CIDX est une association commerciale solide et un organisme de norme dont la mission est d'améliorer la facilité,la rapidité et le coût du commerce électronique entre les entreprises chimiques et leurs partenaires commerciaux. CIDX a eu plusieurs initiatives qui orientent les standards pour l'industrie chimique. L'initiation Chem eStandards de CIDX est abordée dans ce document. Chem eStandard sont les standards uniformes d'échange de données développés

spécifiquement pour l'achat, la vente et la livraison de produits chimiques. Chem eStandards se compose des éléments suivants :

- ChemXML ou les spécifications de message Chem eStandards : v2.0, v2.0.1, v2.0.2, v3.0 et v4.0
- Enveloppe et spécification de sécurité Chem eStandards : v2.0 and v3.0

Pour l'empaquetage, CIDX utilise toujours RNIF 1.1. Il est essentiel de noter que RNIF 1.1 est toujours asynchrone. Par conséquent, les échanges de documents CIDX sont toujours asynchrones.

CIDX consiste en packages et transactions tandis que RosettaNet consiste en packages et PIP (processus d'échange entre partenaires). CIDX utilise le package RNIF 1.1. Les transactions sont telles que définies par le standard ChemXML. Chaque version du standard ChemXML définit les transactions. Toutes les transactions de ChemXML sous une version du standard ChemXML donnée ont la même version que celle du standard ChemXML. Contrairement à RosettaNet, CIDX n'exige pas de conformité à la définition de processus. CIDX se préoccupe davantage de la structure de la transaction et de l'échange de messages de manière sécurisée.

Pour continuer la comparaison, RosettaNet est l'autorité d'administration du standard RosettaNet de même que CIDX est l'autorité d'administration du standard CIDX. RosettaNet définit le package RNIF et les PIP. Les messages RosettaNet peuvent utiliser RNIF 1.1 ou RNIF 2.0. Les PIP définis par RosettaNet donnent le jeu de message et la chorégraphie de processus. CIDX utilise toujours RNIF 1.1 tel que défini par RosettaNet. Dans la mesure où CIDX est le corps d'administration, l'enveloppe RNIF doit être construite telle que définie par l'enveloppe et la spécification de sécurité de Chem eStandards. Cette spécification se base sur l'implémentation de RosettaNet. CIDX n'utilise PAS les PIP définis par RosettaNet. A la place, CIDX utilise les spécifications de message Chem eStandards.

Pour plus d'informations sur CIDX, voir http://www.cidx.org. Les standards CIDX peuvent être téléchargés depuis : http://www.cidx.org. Enveloppe et sécurité Chem eStandards Version 3.0 se trouvent à l'adresse suivante : http://www.cidx.org/Portals/0/Publications/Envelope_and_Security_v3.0.pdf.

WebSphere Partner Gateway prend en charge les Chem eStandards suivants :

- Enveloppe et spécification de sécurité Chem eStandards v3.0
- ChemXML ou les spécifications de message Chem eStandards v4.0.

Packages de types de documents RNIF et PIP pour CIDX

CIDX utilise RNIF1.1 1.1. Pour prendre en charge CIDX, WebSphere Partner Gateway fournit deux jeux de fichiers compressés appelés packages. Le *packages RNIF* comportent les définitions de documents nécessaires pour prendre en charge le protocole RNIF. Ces packages se trouvent dans le répertoire B2BIntegrate.

Pour RNIF V1.1, les packages sont :

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

Le premier package de chaque paire fournit les définitions de documents requises pour la prise en charge des communications CIDX avec les partenaires, tandis que

le second fournit les définitions nécessaires pour la prise en charge des communications CIDX avec les systèmes dorsaux.

Le second jeu de packages se compose de packages de types de documents PIP. Chaque package de type de documents PIP comporte un répertoire Packages contenant un fichier XML et un répertoire GuidelineMaps contenant des fichiers XSD. Le fichier XML spécifie les définitions de documents qui déterminent le mode de traitement du processus PIP par WebSphere Partner Gateway et définissent les messages et signaux échangés. Les fichiers XSD spécifient le format des messages du processus PIP et précisent les valeurs acceptées pour les éléments XML de ces messages. Les fichiers compressés des processus PIP 0A1 contiennent également un fichier XML que le concentrateur utilise comme modèle pour créer des documents 0A1.

Pour CIDX, WebSphere Partner Gateway fournit des packages de types de documents pour E41 ChemXML version 4.0 Création de commandes et E42 ChemXML version 4.0 Réponse à une commande.

La convention de dénomination des packages fournis par CIDX est la même que celle des packages fournis pour RosettaNet. Par exemple, le package BCG_Package_RNIF1.1_E414.0.zip sert à valider les documents pour la version 02.02 du processus PIP 3A4 qui sont échangés entre les partenaires et WPG Partner Gateway à l'aide du protocole RNIF 1.1.

Création de définitions de documents

Pourquoi et quand exécuter cette tâche

Pour l'échange de messages CIDX, WebSphere Partner Gateway exige les packages RNIF de la version de RNIF utilisée pour envoyer les messages. Pour chaque processus PIP pris en charge par WebSphere Partner Gateway, il faut les deux packages de type de documents PIP pour la version RNIF. Par exemple, pour prendre en charge le processus E41 PIP sur RNIF1.1, WebSphere Partner Gateway exige les packages suivants :

- 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

Le premier package prend en charge l'échange de messages CIDX avec les partenaires, le second l'échange de messages CIDX avec les systèmes dorsaux. Les troisième et quatrième packages permettent à WebSphere Partner Gateway de transmettre des messages E41 entre des partenaires et des systèmes dorsaux par le biais du protocole RNIF 2.0.

Pour télécharger des packages CIDX :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur **Téléchargement des packages**.
3. Sélectionnez **Non** pour **Package WSDL**.
4. Cliquez sur **Parcourir** et sélectionnez le package RNIF pour communiquer avec les partenaires.

   Par défaut, les packages RNIF sont situés dans le répertoire B2BIntegrate/rosettanet du support d'installation. Par exemple, si vous

téléchargez le package RNIF version 2.00, vous devez accéder au répertoire B2BIntegrate/rosettanet et sélectionner : Package_RNIF_V0200.zip.

5. Assurez-vous que le paramètre **Validation dans la base de données** est sur **Oui**.
6. Cliquez sur **Télécharger**.
7. Cliquez de nouveau sur **Parcourir** et sélectionnez le package RNIF pour communiquer avec les applications dorsales.

   Par exemple, si vous téléchargez le package RNIF version 2.00, vous devez accéder au répertoire B2BIntegrate/rosettanet et sélectionnez Package_RNSC_1.0_RNIF_V02.00.zip.
8. Cliquez sur **Télécharger**.

   Les packages nécessaires pour communiquer avec les partenaires ou le système dorsal sont à présent installés sur le système. Si vous consultez la page Gérer les définitions de documents, vous voyez une entrée pour **Package : RNIF/Protocole : Rosettanet**, qui représente l'empaquetage pour communiquer avec les partenaires, et **Package : Backend Integration/Protocole : RNSC**, qui est l'empaquetage pour communiquer avec les applications dorsales.
9. Téléchargez le package de type de documents PIP pour le processus PIP et la version RNIF que vous prenez en charge.

   Par exemple, pour télécharger le PIP CIDX E41 (Order Create Remittance Advice) à envoyer à un partenaire, procédez comme suit :

   a. Cliquez sur **Parcourir** et sélectionnez **BCG_Package_RNIF1.1_E414.0.zip** dans le répertoire B2BIntegrate/Rosettanet.
   b. Assurez-vous que le paramètre **Validation dans la base de données** est sur **Oui**.
   c. Cliquez sur **Télécharger**.

   Le PIP E41 apparaît comme étant le type de documents sous Package : RNIF/Protocole : RosettaNet sur la page Gérer les définitions de documents. Une activité, une action et deux signaux sont également affichés. Ils sont inclus dans le téléchargement du PIP.

   Pour télécharger le PIP E41 à envoyer à l'application dorsale, procédez comme suit :

   a. Cliquez sur **Parcourir** et sélectionnez **BCG_Package_RNSC1.0RNIF1.1_E414.0.zip**.
   b. Assurez-vous que le paramètre **Validation dans la base de données** est sur **Oui**.
   c. Cliquez sur **Télécharger**.

   Le PIP E41 apparaît désormais comme étant le type de documents sous Package : Backend Integration/Protocole : RNSC, sur la page Gérer les définitions de documents.

Configuration des valeurs d'attribut

Pourquoi et quand exécuter cette tâche

Pour les définitions de documents RNIF, la plupart des valeurs des attributs sont déjà définies et ne nécessitent pas de configuration. Toutefois, vous devez définir les attributs suivants :

Package RNIF (1.1)

- **GlobalSupplyChainCode** - Identifie le type de chaîne d'approvisionnement utilisée par le partenaire. Les différents types sont Composants électroniques, Technologie d'informations et Fabrication de semiconducteurs. Cet attribut n'a pas de valeur par défaut.

Pour définir les attributs, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur les icônes **Développer** pour développer un noeud jusqu'au niveau Définition de documents approprié, ou sélectionnez **Tout** pour développer tous les noeuds de définition de documents de l'arborescence.
3. Dans la colonne **Actions**, cliquez sur l'icône **Edition des valeurs d'attribut** du package que vous souhaitez modifier (par exemple Package : RNIF (1.1) ou Package : RNIF (V02.00)).
4. Dans la section **Attributs de contexte de définition de documents**, allez dans la colonne **Mettre à jour** de l'attribut que vous souhaitez définir et sélectionnez ou entrez la nouvelle valeur. Répétez l'opération pour chaque attribut à définir.
5. Cliquez sur **Sauvegarder**.

Remarque : Vous pouvez également mettre à jour les attributs RosettaNet au niveau de la connexion en cliquant sur **Attributs** pour la source et la cible puis en entrant ou modifiant les valeurs de la colonne **Mettre à jour**. Voir «Spécification ou modification des attributs», à la page 255.

Création d'interactions

Pourquoi et quand exécuter cette tâche

La procédure suivante décrit la création d'une interaction entre un système dorsal et un partenaire. Notez que vous devez créer une interaction pour chaque processus PIP que vous souhaitez envoyer et une pour chaque processus PIP que vous souhaitez recevoir.

Avant de commencer, assurez-vous que les définitions appropriées de documents RNIF ont été téléchargées, ainsi que les packages du processus PIP que vous souhaitez utiliser.

Pour créer une interaction pour un PIP particulier, procédez comme suit :

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez l'arborescence **Source** jusqu'au niveau **Action** et l'arborescence **Cible** jusqu'au niveau **Action**.
4. Dans les arborescences, sélectionnez les définitions de documents à utiliser pour les contextes source et cible. Par exemple, si le partenaire est l'initiateur d'un processus PIP E41, sélectionnez les définitions de documents suivantes :

Tableau 17. Processus PIP 3C6 lancé par un partenaire

Source	Cible
Package : RNIF (1.1)	Package BackEnd Integration (1.1)
Protocole : RosettaNet(1.1)	Protocole : RNSC (1.0)
Type de documents : E41 (4.0)	Type de documents : E41 (4.0)
Activité : Création de commande	Activité : Création de commande

Tableau 17. Processus PIP 3C6 lancé par un partenaire (suite)

Source	Cible
Action : Création de commande	Action : Création de commande

Pour un processus PIP à deux actions tel qu'un processus 3A4 lancé par un partenaire, sélectionnez les définitions de documents suivantes pour la première action :

Tableau 18. Processus PIP 3A4 lancé par un partenaire

Source	Cible
Package : RNIF (V02.00)	Package : Backend Integration (1.0)
Protocole : RosettaNet (V02.00)	Protocole : RNSC (1.0)
Type de documents : 3A4 (V02.02)	Type de documents : 3A4 (V02.02)
Activité : Demande de bon de commande	Activité : Demande de bon de commande
Action : Action de demande de bon de commande	Action : Action de demande de bon de commande

5. Dans la zone Action, sélectionnez **Translation bidirectionnelle de RosettaNet et de RosettaNet Service Content avec Validation**.
6. Cliquez sur **Sauvegarder**.

Affichage des documents CIDX

Pourquoi et quand exécuter cette tâche

L'Afficheur RosettaNet affiche les informations sur les documents CIDX. Vous pouvez afficher des documents bruts ainsi que les détails des traitements et les événements associés, en précisant les critères de recherche. Ces informations sont intéressantes si vous essayez de savoir si un document a bien été livré ou de déterminer la cause d'un problème.

Affichez l'afficheur RosettaNet, en entrant ce qui suit :

1. Cliquez sur **Afficheurs> Afficheur RosettaNet**.
2. Sélectionnez les critères de recherche appropriés.
3. Cliquez sur **Rechercher**.

documents ebMS

ebMS offre un moyen standard d'échanger des messages commerciaux entre partenaires commerciaux ebXML. Le service de messagerie ebXML fournit un moyen fiable d'échanger des messages commerciaux sans dépendre de technologies et solutions propriétaires. Cette section indique comment définir des définitions de documents et d'interactions pour ces documents.

Création de définitions de documents

Pourquoi et quand exécuter cette tâche

La messagerie ebMS exige qu'un fichier XML de Collaboration Profile Agreement (CPA) soit téléchargé avant que les documents ne puissent être définis.

Pour télécharger un fichier XML CPA, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **ebMS**.
2. Cliquez sur **Télécharger CPA**.
3. Cliquez sur **Parcourir** et sélectionnez le package CPA approprié.
4. Veillez à ce que **ebMS version** 2.0 soit sélectionné.
5. Cliquez sur **Télécharger**.

Pendant le processus de téléchargement du CPA, il vous sera demandé de sélectionner le partenaire interne parmi les partenaires présents dans le CPA. Le partenaire interne est traité comme le gestionnaire du flux ebMS et toutes les cibles du flux ebMS du partenaire interne utiliseront le package Backend Integration ou N/A. Toutefois, sur la console le partenaire ne sera affiché qu'en tant que partenaire externe.

L'ebMS apparaît maintenant comme un package et comme un protocole sous ebMS et Package: Backend Integration sur la page Gestion des définitions de document.

le flux ebMS peut également être configuré dans WebSphere Partner Gateway sans CPA. Pour ce faire, créez des définitions de document ebMS, des fonctions business-to-business depuis la console WebSphere Partner Gateway comme décrit dans «Présentation des types de documents», à la page 111. En réalité, pendant le processus de téléchargement du CPA, toutes les configurations seront automatiquement effectuées. En l'absence du CPA, suivez la procédure indiquée dans cette section.

Configuration des valeurs d'attribut

Pourquoi et quand exécuter cette tâche

Pour les définitions de documents ebMS, la plupart des valeurs des attributs sont déjà définies et ne nécessitent pas de configuration. Toutefois, vous devez définir les attributs suivants :

Package ebMS

- **Heure d'accusé de réception en minutes**- Définissez la durée d'attente d'un accusé de réception avant de renvoyer la requête originale. Cet attribut est associé au Nombre de relances. Il est indiqué en minutes. La valeur par défaut est 30.
- **Nombre de relances** - Définit le nombre de fois qu'une demande sera envoyée si un accusé de réception n'est pas reçu. Cet attribut est associé à l'attribut Heure d'accusé de réception. La valeur par défaut est de 3.
- **Irréfutabilité obligatoire** - Définit si le document original doit être conservé dans le magasin d'irréfutabilité. La valeur par défaut est Oui.

  Remarque : Dans WebSphere Partner Gateway 6.2, les informations d'irréfutabilité sont obtenues dans les paramètres de connexion partenaire. Ces derniers sont obtenus suite à une recherche de connexion partenaire ayant réussie. Par défaut, l'irréfutabilité est définie sur "Oui", ce qui signifie que si les informations sont indisponibles dans la connexion partenaire pour quelque raison que ce soit, le document sera placé dans le magasin d'irréfutabilité.
- **Emplacement de stockage des messages requis** - Définit si le document doit être conservé dans l'emplacement de stockage des messages. La valeur par défaut est Oui.

  Remarque : Les informations de l'emplacement de stockage des messages sont obtenues dans les paramètres de connexion partenaire. Ces derniers sont obtenus suite à une recherche de connexion partenaire ayant réussie. Par défaut, l'emplacement de stockage des messages est défini sur "Oui" ce qui signifie que le document sera conservé dans l'emplacement de stockage des messages.
- **Irréfutabilité de réception** - Définit s'il faut enregistrer ou non la réception dans le magasin d'irréfutabilité. La valeur par défaut est Oui.
- **Intervalle de relance** - Définit le nombre de fois que le système attend et refait une tentative. Cet attribut est associé au Nombre de relances. La valeur par défaut est 5 minutes.

Pour définir les attributs, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur les icônes **Développer** pour développer un noeud jusqu'au niveau Définition de documents approprié, ou sélectionnez **Tout** pour développer tous les noeuds de définition de documents de l'arborescence.
3. Dans la colonne **Actions**, cliquez sur l'icône **Edition des valeurs d'attribut** du package que vous souhaitez modifier.
4. Dans la section **Attributs de contexte de définition de documents**, allez dans la colonne **Mettre à jour** de l'attribut que vous souhaitez définir et sélectionnez ou entrez la nouvelle valeur. Répétez l'opération pour chaque attribut à définir.
5. Cliquez sur **Sauvegarder**.

Remarque : Vous pouvez également mettre à jour les attributs ebMS au niveau de la connexion en cliquant sur **Attributs** pour la source ou la cible puis en entrant ou modifiant les valeurs de la colonne **Mettre à jour**. Voir «Spécification ou modification des attributs», à la page 255.

Création d'interactions

Pourquoi et quand exécuter cette tâche

La procédure suivante décrit la création d'une interaction entre un système dorsal et un partenaire.

Avant de commencer, assurez-vous que les définitions appropriées de documents ebMS ont été téléchargées.

Pour créer une interaction pour un partenaire particulier, procédez comme suit :

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez l'arborescence Source jusqu'au niveau Action et l'arborescence Cible jusqu'au niveau Action.
4. Dans les arborescences, sélectionnez les définitions de documents à utiliser pour les contextes source et cible. Par exemple, si le partenaire est l'initiateur d'un processus ebMS, sélectionnez les définitions de documents suivantes :

Tableau 19. ebMS lancé par un partenaire

Source	Cible
Package : ebMS	Package : Backend Integration (1.0)
Protocole : ebMS	Protocole : ebMS
Type de documents : ALMService	Type de documents : ALMService
Activité : ALMService	Activité : ALMService
Action : Remittance ALMBusiness	Action : ALMBusiness

Si le système dorsal est l'initiateur du processus ebMS, sélectionnez les définitions de documents suivantes :

Tableau 20. Processus ebMS lancé par un système dorsal

Source	Cible
Package : Backend Integration (1.0)	Package : ebMS
Protocole : ebMS	Protocole : ebMS
Type de documents : ALMService	Type de documents : ALMService
Activité : ALMService	Activité : ALMService
Action : ALMBusiness	Action : Remittance ALMBusiness

5. Eventuellement, dans la zone Action sélectionnez **Fractionnement et analyse ebMS**.

   La sélection de ce gestionnaire extraira les charges du message ebMS provenant du partenaire et réintroduira les charges dans le flux comme si elles provenaient du partenaire de manière séparée. Ce gestionnaire ne doit pas être sélectionné lorsque le système dorsal lance le message. Si vous ne sélectionnez pas ce gestionnaire, sélectionnez Pass Through pour la zone action
6. Cliquez sur **Sauvegarder**.

Remarque : Dans certains flux ebMS, par exemple dans les spécifications STAR, l'élément de service ebMS (la valeur de service ebMS est la même que la valeur de définition de flux de document du canal WPG) n'est pas un URI mais une chaîne. Dans ces cas, conformément à la spécification ebMS 2.0, un attribut de type doit être présent avec l'élément de service dans le Message SOAP ebMS. Par exemple, dans une spécification STAR, l'attribut type doit avoir une valeur "STARBOD." Vous pouvez configurer cet attribut sur le côté cible des attributs de définition de flux de document. (Voir tableau 22, à la page 151).

Mappage de CPA ebMS avec la configuration de WebSphere Partner Gateway

Pourquoi et quand exécuter cette tâche

Cette section traite du mappage entre CPA (Collaboration Profile Agreement) et la configuration d'IU WebSphere Partner Gateway. Les fonctions sont répertoriées avec la configuration d'IU WebSphere Partner Gateway correspondante.

1.

Fonction
Elément/Attribut

1.1 CPAId 1

Importé/Configuré manuellement : Importé

Configuration d'IU WebSphere Partner Gateway :

CPAID est configuré via les canaux associés entre deux partenaires. Vous pouvez afficher la valeur en allant dans **Administration concentrateur > ebMS** dans la console WebSphere Partner Gateway. Cliquez sur Rechercher puis sur l'icône Afficher les détails une fois les résultats de la recherche affichés.

2.

Fonction
Elément/Attribut

1.2. Status 1

Importé/Configuré manuellement : Importé mais non stocké dans WebSphere Partner Gateway. La configuration manuelle est également impossible.

Configuration d'IU WebSphere Partner Gateway :

Cet attribut ne peut pas être configuré dans WebSphere Partner Gateway. La valeur est vérifiée lors de l'importation de CPA. Un des statuts suivants s'affiche lors de l'importation :

- Accordé : le CPA peut être importé.
- Signé : le CPA peut être importé et la signature est vérifiée avant importation.
- Proposé : le CPA ne peut pas être importé.

3.

Fonction
Elément/Attribut

1.3 Start 1

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Cet attribut ne peut pas être configuré dans WebSphere Partner Gateway. Il ne peut être défini qu'à partir de l'importation de CPA. Vous pouvez afficher la valeur en allant dans **Administration concentrateur > ebMS** dans la console WebSphere Partner Gateway. Cliquez sur Rechercher puis sur l'icône Afficher les détails une fois les résultats de la recherche affichés.

4.

Fonction
Elément/Attribut

1.4 End 1

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Cet attribut ne peut pas être configuré dans WebSphere Partner Gateway. Il ne peut être défini qu'à partir de l'importation de CPA. Vous pouvez afficher la valeur en allant dans **Administration concentrateur > ebMS** dans la console WebSphere Partner Gateway. Cliquez sur Rechercher puis sur l'icône Afficher les détails une fois les résultats de la recherche affichés.

5.

Fonction
Elément/Attribut

1.5 Conversation Constraints 0, 1 (9.5) - invocationLimit 0,1 - concurrentConversations 0, 1

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Cet attribut ne peut pas être configuré dans WebSphere Partner Gateway. Il ne peut être défini qu'à partir de l'importation de CPA. Vous pouvez afficher la valeur en allant dans **Administration concentrateur > ebMS** dans la console WebSphere Partner Gateway. Cliquez sur Rechercher puis sur l'icône Afficher les détails une fois les résultats de la recherche affichés.

6.

Fonction
Elément/Attribut

1.6 PartyInfo 2
partyName 1

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Pour afficher les valeurs, naviguez jusqu'à **Administrateur de compte > Profils > Partenaire**. Cliquez sur Rechercher puis sur l'icône Afficher les détails une fois les résultats de la recherche affichés pour le partenaire dans CPA.

7.

Fonction
Elément/Attribut

1.6 PartyInfo 2
defaultMshChannelId 1

Importé/Configuré manuellement : Importé mais non stocké dans WebSphere Partner Gateway. La configuration manuelle est également impossible.

Configuration d'IU WebSphere Partner Gateway :

Les valeurs sont utilisées lors de l'importation de CPA pour définir les attributs de canal pour les éléments de signal **Activity- MSHService** comme Ping, Demande de statut, Erreur de message et Accusé de réception. Ces valeurs de canal sont écrasées s'il existe un élément "OverrideMshActionBinding" dans CPA pour tout élément d'action spécifique.

8.

Fonction
Elément/Attribut

1.6 PartyInfo 2
defautMshPackageId 1

Importé/Configuré manuellement : Importé mais non stocké dans WebSphere Partner Gateway. La configuration manuelle est également impossible.

Configuration d'IU WebSphere Partner Gateway :

Les valeurs sont utilisées lors de l'importation de CPA pour définir les attributs de canal pour les éléments de signal **Activity- MSHService** comme Ping, Demande de statut, Erreur de message et Accusé de réception. Ces valeurs de canal sont écrasées s'il existe un élément "OverrideMshActionBinding" dans CPA pour tout élément d'action spécifique.

9.

Fonction
Elément/Attribut

1.6 PartyInfo 2
PartyId 1, *

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Pour afficher les valeurs, naviguez jusqu'à **Administrateur de compte > Profils > Partenaire**. Cliquez sur Rechercher puis sur l'icône Afficher les détails une fois les résultats de la recherche affichés pour le partenaire dans CPA.

10.

Fonction
Elément/Attribut

1.6 PartyInfo 2
type

Importé/Configuré manuellement: Non importé et impossible à configurer.

11.

Fonction
Elément/Attribut

1.6 PartyInfo 2

```
PartyRef 1,*= (8.4.2)
- xlink:type F
- xlink:href 1
- type Fixed
- schemaLocation Implied
```

Importé/Configuré manuellement: Non importé et impossible à configurer.

12.

Fonction
Elément/Attribut

1.6 PartyInfo 2
1.6.3 CollaborationRole 1,*

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

WebSphere Partner Gateway prend en charge plusieurs éléments de rôle de collaboration.

13.

Fonction
Elément/Attribut

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
```

Importé/Configuré manuellement: Non importé.

Configuration d'IU WebSphere Partner Gateway :

Configuration impossible.

14.

Fonction
Elément/Attribut

1.6 PartyInfo 2

```
1.6.3.2 Role 1   (8.4.5)
- name 1
- xlink:type Fixed
- xlink:href 1
```

Importé/Configuré manuellement: L'attribut **xlink:href** est importé, les autres attributs ne sont pas importés.

Configuration d'IU WebSphere Partner Gateway :

La valeur peur être configurée dans les attributs de canal **Administrateur de compte > Connexions > Connexions partenaire**. Recherchez les canaux et accédez à l'attribut de canal - **Rôle**.

15.

Fonction
Elément/Attribut

1.6 PartyInfo 2

```
1.6.3.3  ApplicationCertificateRef 0,1  (8.4.6)
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

La valeur ne peut pas être configurée. Le certificat spécifié pour l'attribut **certId** est chargé dans le système de fichiers mais pas dans WebSphere Partner Gateway.

16.

Fonction
Elément/Attribut

1.6 PartyInfo 2

```
1.6.3.4  ApplicationSecurityDetailsRef 0, 1 (8.4.7)
- securityId 1
```

Importé/Configuré manuellement: Non importé.

Configuration d'IU WebSphere Partner Gateway :

Configuration impossible.

17.

Fonction
Elément/Attribut

1.6.3.5 ServiceBinding 1

```
1.6.3.5.1 Service 1 (8.4.9)
- type  Implied
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

- **Service** : nom de la définition de document. Pour afficher la valeur, naviguez jusqu'à **Administrateur concentrateur > Définitions de document**. La valeur Service sera affichée en tant que Type de document et Activité sous Package ebMS et Package d'intégration dorsale.
- **Type** : Type est utilisé comme attribut de canal sous **Administrateur de compte > Connexions > Connexions partenaire**. Recherchez les canaux et accédez à l'attribut de canal **Type de service**.

18.

Fonction
Elément/Attribut

1.6.3.5 ServiceBinding 1

```
1.6.3.5.1 Service 1 (8.4.9)
- type  Implied
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

- **Service** : nom de la définition de document. Pour afficher la valeur, naviguez jusqu'à **Administrateur concentrateur > Définitions de document**. La valeur Service sera affichée en tant que Type de document et Activité sous Package ebMS et Package d'intégration dorsale.
- **Type** : Type est utilisé comme attribut de canal sous **Administrateur de compte > Connexions > Connexions partenaire**. Recherchez les canaux et accédez à l'attribut de canal **Type de service**.

19.

Fonction
Elément/Attribut

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
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

- **CanSend** – Un canal est créé à partir de **Intégration dorsale > ebMS > Nom de service > Action du partenaire A** vers **ebMS > Nom de service > Action du partenaire B** (partenaire B ayant l'élément **CanReceive** lié via l'élément **OtherPartyActionBinding**).
- **Action** – Importé et créé en tant qu'élément Action sous **Activité** dans définition de document.
- **packageId** – Les attributs d'ID de package de référencement sont stockés en tant qu'attributs de canal.
- Xlink:href and xlink:type: Non importé et impossible à configurer.
- **isNonRepudiationRequired, isNonRepudiationReceiptRequired, isIntelligibleCheckRequired, timeToAcknowledgeReceipt, timeToPerform**: Ces attributs sont configurés en tant qu'attributs de canal.
- **isConfidential, isAuthenticated, isTamperProof, isAuthorizationRequired, timeToAcknowledgeAcceptance, retryCount** - non importés et non configurables.
- **ChannelId** 1, * : Une seule valeur est acceptée pour WebSphere Partner Gateway. Les attributs de référencement sont définis en tant qu'attributs de canal.
- **binaryCollaboration, businessTransactionActivity, requestOrResponseAction, CollaborationActivity** – non importés et non configurables.
- **OtherPartyActionBinding** - Importé. La référence est utilisée pour créer le canal.
- **CanReceive** - Importé et traité comme synchrone s'il existe tout autre canal pour la même connexion.

20.

Fonction
Elément/Attribut

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
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

- **CanReceive** – Un canal est créé à partir de **ebMS > Nom de service > Action du partenaire A** vers **Intégration dorsale > ebMS > Nom de service > Action du partenaire B** (partenaire B ayant l'élément **CanSend** lié via l'élément **OtherPartyActionBinding**).
- **OtherPartyActionBinding** - Importé. La référence est utilisée pour créer le canal.
- **CanSend** - Importé et traité comme synchrone s'il existe tout autre canal pour la même connexion.

21.

Fonction
Elément/Attribut

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.4 Certificate 1, * (8.4.18)
- certId  KeyInfo
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Les certificats sont stockés dans le système de fichiers et doivent être manuellement chargés dans WebSphere Partner Gateway sous **Administrateur de compte > Profils > Certificats**.

22.

Fonction
Elément/Attribut

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
```

Importé/Configuré manuellement: Non importé. Seuls les certificats de référence sont chargés dans le système de fichiers.

23.

Fonction
Elément/Attribut

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
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

- **channelId** : Les attributs de référencement sont définis en tant qu'attributs de canal.
- **transportId**: Les attributs de référencement sont utilisés pour créer la passerelle et définis comme passerelle par défaut pour le canal.
- **docExchangeId**: Les attributs de référencement sont définis en tant qu'attributs de canal.
- **syncReplyMode, ackRequested, ackSignatureRequested, duplicateElimination, actor** : Ces attributs sont importés et configurés comme attributs de canal.

24.

Fonction
Elément/Attribut

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
```

Importé/Configuré manuellement: Non importé.

25.

Fonction

Elément/Attribut

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
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

- **Protocole de transport** : Définit le protocole de passerelle
- **Version** : Définit la version du protocole de passerelle.
- **URL**: Définit l'URL de passerelle. Ces valeurs sont affichées sous **Administrateur de compte > Profils > Recherche de partenaire**. Pour tous les partenaires et pour le partenaire sélectionné, cliquez sur l'onglet **Destinations**. Les valeurs d'attribut restants ne sont pas importés.

26.

Fonction

Elément/Attribut

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
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm : Ces valeurs sont importées et stockées en tant qu'attributs de canal, présents dans **Administrateur de compte > Connexions > Connexions partenaire**. Recherchez les canaux et accédez à **Attributs de canal**. Les valeurs restantes ne sont pas importées et ne peuvent pas être configurées.

27.

Fonction

Elément/Attribut

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
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Retries, RetryInterval, MessageOrderSemantics, PersistDuration, HashFunction, SignatureAlgorithm, DigitalEnvelopeProtocol, EncryptionAlgorithm : Ces valeurs sont importées et stockées en tant qu'attributs de canal, présents dans **Administrateur de compte > Connexions > Connexions partenaire**. Recherchez les canaux et accédez à **Attributs de canal**. Les valeurs restantes ne sont pas importées et ne peuvent pas être configurées.

28.

Fonction
Elément/Attribut

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.6.9  OverrideMshActionBinding 0, *  (8.4.58)
- action 1
- channelId
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Pour l'action spécifiée, les attributs de canal sont définis en utilisant l'ID de canal de référence.

29.

Fonction
Elément/Attribut

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, *
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Mimetype : Les valeurs sont importées et stockées en tant qu'attributs de canal. Les valeurs restantes ne sont pas importées et ne peuvent pas être configurées.

30.

Fonction
Elément/Attribut

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, *
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Composite : mimetype, mimeparameters, Constituent-idref, Constituent-excludeFromSignature, signatureTransform, encryptionTransform, Algorithm: Ces valeurs sont importées et stockées en tant qu'attributs de canal dans **Administrateur de compte > Connexions > Connexions partenaire**. Recherchez les canaux et accédez à **Attributs de canal**. Les valeurs restantes ne sont pas importées et ne peuvent pas être configurées.

31.

Fonction

Elément/Attribut

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, *
```

Importé/Configuré manuellement : Importé.

Configuration d'IU WebSphere Partner Gateway :

Encapsulation : mimetype, mimeparameters, Constituent-idref, Constituent-excludeFromSignature, signatureTransform, encryptionTransform, Algorithm : Ces valeurs sont importées et stockées en tant qu'attributs de canal dans **Administrateur de compte > Connexions > Connexions partenaire**. Recherchez les canaux et accédez à **Attributs de canal**. Les valeurs restantes ne sont pas importées et ne peuvent pas être configurées.

32.

Fonction
Elément/Attribut

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
```

Importé/Configuré manuellement : Non importé.

Configuration d'IU WebSphere Partner Gateway :

Configuration impossible.

33.

Fonction
Elément/Attribut

1.6.3.5.2 CanSend 0, * (8.4.10)

```
1.10 Comments 0, * (8.8)
- xml:lang
```

Importé/Configuré manuellement : Non importé.

Configuration d'IU WebSphere Partner Gateway :

Configuration impossible.

Attributs de connexion

Le tableau suivant présente les attributs d'objet de routage disponibles dans les canaux métier du message sur le packagind ebMS.

Cliquez sur **Administrateur de compte > Connexions > Connexions partenaire** et sélectionnez Source et Cible. Si le canal est pour le message ebMS entrant, cliquez sur **Attributs** du côté source, et si le canal est pour le message ebMS sortant, cliquez sur **Attributs** du côté cible. Faites défiler l'écran qui s'affiche et cliquez sur le dossier **Action** .

Tableau 21. Attributs de connexion

Attributs XML CPA	Valeur par défaut	Valeurs possibles	Texte d'affichage dans WebSphere Partner Gateway
isNonRepudiationRequired	False	True/false - mapped as Yes/No	Irréfutabilité requise
isNonRepudiationReceiptRequired	False	True/false - mapped as Yes/No	Irréfutabilité de l'avis de réception
timeToAcknowledgeReceipt			Heure d'accusé de réception
Retries	3	Some Number	Nombre de relances
MessageOrderSemantics	Not Guaranteed	"Guaranteed" "NotGuaranteed"	Sémantique de commande de message
PersistDuration	P1D		Durée de conservation

Tableau 21. Attributs de connexion (suite)

Attributs XML CPA	Valeur par défaut	Valeurs possibles	Texte d'affichage dans WebSphere Partner Gateway
syncReplyMode	None	"mshSignalsOnly" "signalsOnly" "responseOnly" "signalsAndResponse" "none" (Moved to phase 2)	Mode de Réponse synchronisé
ackRequested	Per Message	"always" - implique que l'accusé de réception doit toujours être demandé. "never" - implique que l'accusé de réception ne doit jamais être demandé. “perMessage” - implique que l'accusé de réception peut ou peut ne pas être demandé en fonction de l'élément d'accusé de réception présent dans le document ebXML.	Accusé de réception demandé
ackSignatureRequested	Per Message	"always" "never" "perMessage"	Signature d'accusé de réception demandée
duplicateElimination	Per Message	"always" "never" "perMessage"	Elimination de doublon
Acteur	"urn:oasis:names:tc:ebxml-msg:actor:nextMSH"	"urn:oasis:names:tc:ebxml-msg:actor:nextMSH""urn:oasis:names:tc:ebxml-msg:actor:toPartyMSH"	Acteur
PartyRole	-	Rôle dans CPA	Rôle
Intervalle de relance	270	-	Intervalle de relance
NonRepudiationProtocol	-	http://www.w3.org/2000/09/xmldsig#	Protocole de signature
SignatureAlgorithm	-	1. http://www.w3.org.2000/09/xmldsig#dsa-sha1 2. http://www.w3.org/2000/09/xmldsig#rsa-sha1 **Remarque :** Dans ebMS, hmac-sha1 n'est pas pris en charge.	Algorithme de signature
isEncryptionRequired	Non	True/false - mapped as Yes/no	Chiffrement obligatoire
isCompressionRequired	Non	True/false - mapped as Yes/no	Compression obligatoire
/Packaging/CompositeList/Encapsulation/Constituent:mimetype	-		Type Mime de compression
/tp:SenderDigitalEnvelope/tp:DigitalEnvelopeProtocol	-	SMIME XMLEncryption	Protocole de chiffrement

Tableau 21. Attributs de connexion (suite)

Attributs XML CPA	Valeur par défaut	Valeurs possibles	Texte d'affichage dans WebSphere Partner Gateway
/tp:SenderDigitalEnvelope /EncryptionAlgorithm	-	3des-cbc, aes128-cbc, aes-256-cbc	Algorithme de chiffrement
/tp:ReceiverDigitalEnvelope /tp:DigitalEnvelopeProtocol	-	SMIME XMLEncryption	Protocole de chiffrement
/tp:ReceiverDigitalEnvelope /EncryptionAlgorithm	-	3des-cbc, aes128-cbc, aes-256-cbc	Algorithme de chiffrement
/Packaging/CompositeList /Encapsulation tp:MimeType	-	text/xml application/pkcs7-mime	Type Mime de chiffrement
/Packaging/CompositeList /Encapsulation- tp:mimeparameters	-		Paramètre Mime de chiffrement
/Packaging/CompositeList /Encapsulation/Constituent: mimetype	-		Constituant de chiffrement
/Packaging/CompositeList / Composite/ tp:mimeparameters	-		Paramètre Mime d'empaquetage
/Packaging/CompositeList / Composite /Constituent: mimetype	-		PackagingConstituent
/Packaging/CompositeList /Composite/Contituent /excludeFromSignature: mimetype	-		Exclure de la Signature
/Packaging/CompositeList / Composite/Contituent/ SignatureTransform	-	1. BASE64 2. ENVELOPED 3. XPATH 4. XPATH2 5. XSLT	Algorithme de transformation de signature
/Packaging/CompositeList /Composite/Contituent/ EncryptionTransform	-	1. BASE64 2. ENVELOPED 3. XPATH 4. XPATH2 5. XSLT	Algorithme de transformation de chiffrement

Limitations

Les limitations du mappage de CPA vers WebSphere Partner Gateway sont les suivantes :

1. Les certificats provenant de CPA ne sont pas importés dans WebSphere Partner Gateway. Ils sont stockés dans le système de fichiers et l'administrateur doit les vérifier manuellement et les télécharger vers WebSphere Partner Gateway.
2. WebSphere Partner Gateway peut traiter les flux synchrones et asynchrones provenant de CPA, mais pas plusieurs liaisons ayant la même valeur d'action.
3. Seul l'ID DUNS numérique à 9 chiffres est pris en charge (la structure libre n'est pas prise en charge).

Mappage des en-têtes SOAP ebMS vers les en-têtes WebSphere Partner Gateway

Les spécifications ebMS 2.0 définissent un ensemble d'en-têtes obligatoires, qui doivent être présents dans les messages SOAP ebMS. La table ci-dessous indique le mappage entre certains de ces en-têtes obligatoires et les en-têtes WebSphere Partner Gateway d'où ces valeurs sont extraites.

Tableau 22. Les en-têtes SOAP ebMS et les en-têtes WebSphere Partner Gateway correspondants

N° de série	Nom d'en-tête dans le message SOAP ebMS	Nom d'en-tête correspondant dans WebSphere Partner Gateway
1	Depuis IDPartie	“x-aux-sender-id” défini par le système dorsal
2	A partir du rôle	Attribut Rôle du côté source des attributs de Définition de documents
3	Depuis le Type IDPartie	L'utilisateur ne peut pas le configurer. Si l'IDPartie est DUNS, la valeur “type” sera “urn:duns.” Autrement, ce sera “chaîne.”
4	Vers IDPartie	“x-aux-receiver-id” défini par le système dorsal
5	Vers le rôle	Attribut Rôle du côté cible des attributs de Définition de documents
6	Vers le Type IDPartie	L'utilisateur ne peut pas le configurer. Si l'IDPartie est duns, la valeur “type” sera “urn:duns.” Autrement, ce sera “chaîne.”
7	Id CPA	Si un CPA est présent dans la base de données, alors WebSphere Partner Gateway utilisera l'ID-CPA présent dans le CPA. Autrement, l'utilisateur peut configurer l'attribut ID CPA présent sur le côté cibles des attributs de définition de document. Si l'utilisateur n'a pas configuré cet attribut et qu'un CPA n'est pas présent, alors WebSphere Partner Gateway générera un ID CPA basé sur les ID du partenaire.
8	ID de Conversation	“x-aux-process-instance-id” défini par le système dorsal. Si le système dorsal ne le définit pas, alors WebSphere Partner Gateway générera son propre ID de conversation.
9	Service	La valeur Définition du document sur la connexion du partenaire cible. **Remarque :** La définition du document et l'activité seront identiques dans un flux ebMS.
10	Type de service	L'attribut TypedeService sur la côté cible des attributs Définition de document
11	Action	La valeur Action sur la connexion du partenaire cible
12	IDMessage	“x-aux-msg-id” défini par le système dorsal. Si le système dorsal ne le définit pas, alors WebSphere Partner Gateway générera son propre ID de message.

Si vous envoyez une réponse ebMS synchrone à un document de requête ebMS, le système dorsal doit définir l'en-tête “x-aux-request-msg-id” sur le document réponse. La valeur de cet en-tête sera l'ID message du message de demande De plus, le document réponse doit être dans la même conversation que le document de requête. Cela signifie que le “x-aux-process-instance-id” pour la réponse doit être identique à l'ID Conversation de la requête.

L'ID Conversation et l'ID Message du document de requête sont envoyés au système dorsal respectivement en tant que “x-aux-process-instance-id” et “x-aux-msg-id”.

Affichage des documents ebMS

Pourquoi et quand exécuter cette tâche

L'Afficheur ebMS affiche les informations sur les documents ebMS. Vous pouvez afficher des documents bruts ainsi que les détails des traitements et les événements associés, en précisant les critères de recherche. Ces informations sont intéressantes si vous essayez de savoir si un document a bien été livré ou de déterminer la cause d'un problème.

Démarrez l'Afficheur ebMS, en entrant ce qui suit :

1. Cliquez sur **Afficheurs> Afficheur ebMS**.
2. Sélectionnez les critères de recherche appropriés.
3. Cliquez sur **Rechercher**.

Dans l'afficheur ebMS, les documents sont organisés en fonction de l'ID de conversation. Cela signifie que tous les documents ayant le même ID de conversation seront regroupés et pourront être vus en cliquant sur l'icône Plus de détails sur la partie gauche de chaque ligne d'ID de conversation. Lorsque vous cliquez sur l'icône Plus de détails, une nouvelle page s'affiche présentant tous les messages de cette conversation. Si le haut de la page, se trouve un attribut intitulé "Statut de conversation." La valeur de cet attribut est le prochain message prévu dans cette conversation.

Demander le statut d'un message ebMS

Pourquoi et quand exécuter cette tâche

Pour demander le statut d'un message ebMS, procédez comme suit :

1. Une fois que vous avez trouvé le document ebMS qui vous intéresse, cliquez sur l'icône **Afficher les détails** à côté.
2. Cliquez sur Demander le statut. Le statut de ce document s'affiche alors.

Pour rafraîchir le statut, cliquez sur **Afficher le statut**.

Lorsque vous configurez des documents de requête de statut et de réponse de statut ebMS, vous devez prendre en compte les éléments suivants :

- Seule la connexion de requête de statut doit être créée. La connexion de réponse de statut utilisera la connexion existante de requête de statut.
- Pour une connexion de requête de statut depuis le partenaire interne vers un partenaire externe, la destination source de la connexion n'est pas utilisée.
- Pour une connexion de requête de statut depuis un partenaire externe vers un partenaire interne, la destination source de la connexion est utilisée pour renvoyer le document réponse Réponse de statut vers le partenaire externe.
- Si un utilisateur ne dispose pas d'un CPA, alors il ou elle doit activer les fonctions business-to-business et créer un canal pour le message Requête de statut ebMS comme suit :
  - Pour le message entrant de requête de statut ebMS,

    Le côté source de la fonction business-to-business doit être :

    Package : N/A (N/A)
    Protocole : ebMS (2.0)
    Type de document : MSHService (2.0)
    Activité : MSHService (2.0)
    Action : StatusRequest(N/A)

Le côté cible de la fonction business-to-business doit être :

Package : ebMS (2.0)
Protocole : ebMS (2.0)
Type de document : MSHService (2.0)
Activité : MSHService (2.0)
Action : StatusRequest(N/A)

– Pour le message sortant de requête de statut ebMS

Le côté source de la fonction business-to-business doit être :

Package : ebMS (2.0)
Protocole : ebMS (2.0)
Type de document : MSHService (2.0)
Activité : MSHService (2.0)
Action : StatusRequest(N/A)

Le côté cible de la fonction business-to-business doit être :

Package : N/A (N/A)
Protocole : ebMS (2.0)
Type de document : MSHService (2.0)
Activité : MSHService (2.0)
Action : StatusRequest(N/A)

L'utilisateur doit ensuite activer le canal et définir les destinations à partir de la page de connexion partenaire.

Remarque : Il en est de même pour les erreurs ebMS et les accusés de réception. L'action de ces canaux affichera respectivement ErreurMessage et Accusé de réception.

Envoyer un message PING aux partenaires ebMS

Pourquoi et quand exécuter cette tâche

A partir de la page de test des connexions partenaires, vous pouvez envoyer un message ping aux partenaires ebMS. Cela signifie que vous pouvez envoyer un message ping à un partenaire, et, si le partenaire est prêt à le recevoir, il répond avec un message pong. Dès que vous avez téléchargé le CPA, le canal de ping-pong sera créé.

Pour la commande Ping à utiliser, les connexions doivent être définies avec le partenaire impliqué. Pour plus d'informations, voir la section sur l'envoi de messages ping aux partenaires ebMS dans le *Guide configuration du concentrateur de WebSphere Partner Gateway*.

Pour envoyer un message ping à un partenaire ebMS, procédez comme suit :

1. Cliquez sur **Outils** > **Test de la connexion du partenaire**.
2. Pour **Commande**, sélectionnez **PING ebMS**.
3. Sélectionnez **Du partenaire** et **Au partenaire**.
4. Indiquez éventuellement une **Destination** ou saisissez une **URL**.
5. Cliquez sur **Test** pour envoyer un message ping.

Pour détermine le statut du message ping, cliquez sur **Statut Ping**. Le statut de la dernière requête ping s'affiche alors sous les résultats.

Remarque : La dernière requête ping peut avoir été lancée depuis la connexion partenaire test ou depuis le renvoi d'un afficheur de documents d'un document ping existant.

services Web

Un partenaire peut appeler un service Web hébergé par le partenaire interne. De même, le partenaire interne peut appeler un service Web hébergé par un partenaire. Le partenaire ou le partenaire interne appelle le service Web via WebSphere Partner Gateway. WebSphere Partner Gateway agit comme un proxy en transférant la demande de Service Web au fournisseur d'accès du Service Web et en renvoyant la réponse de manière synchrone, du fournisseur au demandeur.

Cette section contient les informations suivantes pour configurer un service Web qu'un partenaire ou un partenaire interne pourra utiliser :

- Identification des partenaires pour un Service Web.
- Configuration d'une définition de documents pour un service Web.
- Ajout d'une définition de documents aux fonctions business-to-business d'un partenaire.
- Restrictions et limitations relatives à un support de service Web.

Identification des partenaires pour un Service Web

Lorsqu'un service Web est fourni par le partenaire interne pour être utilisé par des partenaires, WebSphere Partner Gateway requiert l'identification des partenaires internes et externes. WebSphere Partner Gateway prend en charge la création de plusieurs partenaires internes dont un est défini en tant que partenaire par défaut. Pour remplacer le partenaire interne par défaut et sélectionner un autre partenaire interne, vous devez envoyer d'autre paramètres au récepteur de WebSphere Partner Gateway, comme **FromPartnerBusinessId** ou **ToPartnerBusinessId** selon si le flux est sortant ou entrant respectivement. Un cas d'erreur se produirait si deux ID de partenaires externes différents sont fournis via l'authentification de base et une URL, l'authentification de base a priorité sur l'URL. Les différentes chaînes de requête possibles pour le flux sortant sont : `<Receiver-URL>?to=<business id>` et `<Receiver-URL?to=<business id>&from=<business id>`. Les différentes chaînes de requête possibles pour le flux entrant sont : `<Receiver-URL` et `Receiver-URL?to=business id`. Dans le cas de flux entrant, l'**authentification de base** est obligatoire.

Création de définitions de documents

Pour effectuer la définition de documents, téléchargez les fichiers WSDL (Web Service Definition Language) qui définissent le Service Web, ou entrez manuellement les définitions de documents équivalentes par la console de communauté.

Téléchargement de fichiers WSDL pour un Service Web

Pourquoi et quand exécuter cette tâche

La définition relative à un Service Web doit être comprise dans un fichier principal WSDL avec l'extension `.wsdl`, qui peut importer des fichiers WSDL supplémentaires via l'élément `import`. Les éventuels fichiers importés peuvent être téléchargés avec le fichier principal selon l'une des méthodes suivantes :

- Si le chemin d'accès au fichier ou l'URL (HTTP) de chaque attribut `location` de l'élément `import` est accessible à partir du serveur de la console de communauté

(et non pas de la machine de l'utilisateur), le fichier principal peut être téléchargé directement et les fichiers importes seront téléchargés automatiquement.

- Si tous les fichiers importés et le fichier principal sont compressés dans un fichier zip, chacun avec un chemin correspondant à celui (s'il existe) de l'attribut `location`, le téléchargement du fichier compressé entraînera celui de tous les fichiers principaux fichiers WSDL importés qui s'y trouvent.

Par exemple, si le fichier WSDL principal `helloworldRPC.wsdl` contient l'élément import suivant :

```
<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"/>
```

Et que le fichier WSDL `bindingRPC.wsdl` importé contient l'élément import suivant :

Le fichier doit contenir les informations suivantes :

```
Nom                   Chemin

helloworldRPC.wsdl

bindingRPC.wsdl

porttypeRPC.wsdl               port\
```

Lorsqu'un fichier de définition WSDL d'un Service Web est téléchargé, le fichier WSDL d'origine est enregistré sous forme de mappe de validation. (Les messages de Service Web ne sont pas réellement validés par rapport à WSDL par WebSphere Partner Gateway.) C'est ce qu'on appelle le WSDL *privé*.

De plus, un WSDL public est enregistré avec l'URL privé remplacé par l'URL cible indiqué par l'utilisateur dans la page Page Téléchargement des packages. Le WSDL public sera fourni aux utilisateurs du Service Web, qui appelleront le Service Web à l'URL de la cible (l'URL public). WebSphere Partner Gateway achemine ensuite la demande de Service Web à une destination qui est l'URL privé du fournisseur de Service Web d'origine. WebSphere Partner Gateway agit comme un proxy en transférant la demande de Service Web à un URL de fournisseur privé, inconnu de l'utilisateur de Service Web.

Les WSDL privé et public (y compris les fichiers importés) peuvent être téléchargés à partir de la console de communauté après le téléchargement du WSDL.

Téléchargement des fichiers WSDL à l'aide de la console de communauté : WebSphere Partner Gateway propose une méthode d' importation des fichiers WSDL. Si un Service Web est défini dans un fichier WSDL simple, vous pouvez télécharger directement ce fichier WSDL. Si le Service Web est défini à l'aide de plusieurs fichiers WSDL (ceci se produit lorsque vous avez importé des fichiers WSDL dans un fichier WSDL principal), ils seront téléchargés dans une archive compressée.

Important : Le fichiers WSDL se trouvant dans l'archive compressée doivent figurer dans un répertoire spécifié dans l'élément d'importation de WSDL. Supposons par exemple que vous ayez l'élément import suivant :

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
location="path1/bindingRPC.wsdl"/>
```

L'arborescence des répertoires de l'archive compressée zip sera : `path1/bindingRPC.wsdl` .

Pour l'exemple suivant :

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl"
 location="bindingRPC.wsdl"/>.
```

Le fichier `bindingRPC.wsdl` sera au niveau racine de l'archive.

Pour télécharger un fichier WSDL simple ou une archive compressée, procédez comme suit.

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **Définition de documents**.
2. Cliquez sur **Téléchargement des packages**.
3. Pour **Package WSDL**, cliquez sur **Oui**.
4. Pour **URL public du Service Web**, appliquez une des procédures suivantes :
   - Pour un service Web fourni par le partenaire interne (qui sera appelé par un partenaire), saisissez l'URL public du service Web. Par exemple :

     `https://<hôte_cible:port>/bcgreceiver/Receiver`

     L'URL correspond généralement à la cible HTTP de production définie dans les cibles.
   - Pour un service Web fourni par un partenaire (qui sera appelé par le partenaire interne), saisissez l'URL public du partenaire avec une chaîne de requête. Par exemple :

     `https://<target_host:port>/bcgreceiver/Receiver?to=<partner_business_ID>`
5. Cliquez sur **Parcourir** et sélectionnez le fichier WSDL ou l'archive compressée.
6. Pour la **validation dans la base de données**, sélectionnez **Non** si vous voulez télécharger le fichier en mode test. Lorsque vous sélectionnez **Non**, le fichier ne sera pas installé sur le système. Utilisez les messages générés par le système affichés dans la boîte de messages afin de résoudre les erreurs de téléchargement. Sélectionnez **Oui** pour télécharger le fichier dans la base de données du système.
7. Pour l'**écrasement des données**, sélectionnez **Oui** pour remplacer un fichier se trouvant actuellement dans la base de données. Sélectionnez **Non** pour ajouter le fichier à la base de données.
8. Cliquez sur **Télécharger**. Le fichier WSDL est installé dans le système.

Validation des packages à l'aide des fichiers schéma : Plusieurs schémas XML décrivant les fichiers XML qui peuvent être téléchargés via la console sont fournis sur le support d'installation WebSphere Partner Gateway. Les fichiers téléchargés sont validés pour ces schémas. Les fichiers schéma constituent une référence très utile pour la détermination des causes d'erreur lorsqu'un fichier ne peut pas être téléchargé en raison d'un XML non conforme. Les fichiers sont les suivants : `wsdl.xsd` , `wsdlhttp.xsd` et `wsdlsoap.xsd`, qui contiennent le schéma décrivant les fichiers WSDL (Web Service Definition Language)

Les fichiers se trouvent dans : `B2BIntegrate\packagingSchemas`

Création manuelle d'une définition de documents

Pour entrer manuellement les définitions équivalentes de documents, suivez les procédures indiquées dans cette section. Vous devez également créer individuellement le type de documents, l'activité et les entrées d'action sous

Protocole : Services Web, en tenant bien compte des conditions requises par l'action et de ses relations avec les messages SOAP reçus.

En ce qui concerne les définitions de documents en terme d'empaquetage, protocole, type de documents, activité et hiérarchie des actions, un Service Web pris en charge se présente comme suit :

- **Package : None**
- **Protocole : Service Web (1.0)**
- **Type de documents :** {*<espace-nom_du_Service_Web>*:*<nom_du_Service_Web>*} (nom et code), qui doit être unique parmi les types de documents pour le protocole de Service Web. Il s'agit normalement de l'espace-nom et du nom de WSDL.
- **Activité :** Une activité pour chaque opération de service Web avec le nom et le code :

  {*<espace_de_nom_opération>*}:*<nom_opération>*
- **Action :** Une action pour chaque message d'entrée, avec le nom et le code :

  {*<espacedenom_élément_xml_identifiant = espacedenom_premier_enfant_de_soap:body>*}:
  <nom_élément_xml_identifiant = nom_premier_enfant_de_soap:body>

Les définitions critiques sont les actions car WebSphere Partner Gateway va utiliser un espace-nom d'action et un nom pour reconnaître un message SOAP de demande de Service Web entrant et l'acheminer de manière appropriée en fonction d'une connexion donnée de partenaire. L'espace-nom et le nom du premier enfant de l'élément XML `soap:body` du message SOAP reçu doivent correspondre à un espace de nom et à un nom d'action dans les définitions de documents WebSphere Partner Gateway.

Par exemple, si un message SOAP de demande de Service Web se présente sous la forme suivante (pour une session de liaison SOAP de littéral-document) :

```
<?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>
```

Alors, WebSphere Partner Gateway cherchera une action de Service Web définie avec le code suivant :

```
{http://www.helloworld.com/xsd/helloDocLitSchema}:nameAndAddressElt
```

Par exemple, pour un message de demande SOAP de type session de liaison RPC :

```
<?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>
```

Alors, WebSphere Partner Gateway cherchera une action de Service Web définie avec le code suivant :

```
{http://www.helloworld.com/helloRPC}:helloWorldRPC
```

Pour une session de liaison RPC, l'espace-nom et le nom du premier élément enfant de `soap:body` d'un message de demande de SOAP doivent être l'espace-nom et le nom de l'opération du Service Web applicable.

Pour une session de liaison de littéral-document, l'espace-nom et le nom du premier élément enfant de `soap:body` d'un message de demande SOAP devraient correspondre à l'espace-nom de l'attribut `element` XML dans l'élément `part` de la définition de `message` entrant pour le Service Web.

Création d'interactions

Pourquoi et quand exécuter cette tâche

Pour créer une interaction pour un Service Web, utilisez la même action de type de documents de Service Web pour la source et la cible.

Pour créer des interactions, procédez comme suit :

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Sous **Source**, développez **Package : None > Protocole : Service Web > Type de documents : <** *type de documents*> > **Action :** <*action*>.
4. Répétez l'étape précédente dans la colonne **Cible**.
5. Sélectionnez **Passe-système** dans la liste des **Actions** figurant en bas de la page (**Passe-système** est la seule option prise en charge dans WebSphere Partner Gateway pour un Service Web).

Restrictions et limitations relatives à un support de service Web

WebSphere Partner Gateway prend en charge les standards suivants :

- WSDL 1.1
- SOAP 1.1
- WS-I Basic Profile v. 1.0 (qui contient des restrictions importantes sur la forme des messages SOAP pour la session de liaison de littéral document)

Remarque :

- WebSphere Partner Gateway dispose d'un support partiel pour Basic Profile 1.0.
- La session de liaison SOAP/HTTP est prise en charge.
- L'exécution d'une nouvelle session de liaison n'est pas prise en charge.
- Les styles de session de liaison codé RPC/littéral RPC et littéral document ne sont pas pris en charge (ils sont sujets aux restrictions dans WS-I Basic Profile).

Voir «Validation de l'élément SOAP Envelope», à la page 107 et «Désenvelopper le protocole SOAP», à la page 107.

Documents cXML

Le gestionnaire de documents de WebSphere Partner Gateway identifie un document cXML par le nom de l'élément racine du document XML, qui est `cXML` et la version par le cXML DOCTYPE (DTD) cXML. Par exemple, le DOCTYPE suivant correspond à cXML version 1.2.009 :

```
<!DOCTYPE cXML SYSTEM "http://xml.cXML.org/schemas/cXML/1.2.009/cXML.dtd">
```

Le gestionnaire de documents procède à la validation DTD des documents cXML ; toutefois, WebSphere Partner Gateway ne fournit pas de DTD cXML. Vous pouvez les télécharger à partir du site www.cxml.org puis les charger dans WebSphere Partner Gateway via le module de mappe de validation de console de communauté. Une fois que vous avez téléchargé le DTD, associez-le au type de documents cXML. Pour plus d'informations sur l'association du DTD avec le type de documents cXML, voir «Association de mappes à des définitions de documents», à la page 176.

Le gestionnaire de documents utilise deux attributs de l'élément racine du gestionnaire de documents : payloadID et timestamp. Les payloadID et timestamp cXML sont utilisés en tant que numéro d'ID document et horodatage du document. Ces deux informations peuvent être consultées sur la console de communauté pour le gestionnaire de documents.

Les éléments From (De) et To (A) de l'en-tête cXML contient l'élément Credential utilisé pour le routage et l'authentification du document. Le exemple ci-dessous affiche les éléments From (De) et To (A) comme source et cible du document cXML.

Remarque : Ici comme partout ailleurs dans ce document, les numéros DUNS ne sont que des exemples.

```
<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 plusieurs éléments credential sont utilisés, le gestionnaire de documents utilise le numéro DUNS comme identificateur entreprise pour le routage et l'authentification. Si aucun numéro DUNS n'a été indiqué, le premier Credential est utilisé.

WebSphere Partner Gateway n'utilise pas les informations se trouvant dans l'élément émetteur.

Dans le cadre d'une transaction synchrone, les en-têtes From (De) et To (A) ne sont pas utilisés dans le document réponse cXML. le document réponse est envoyé via la même connexion HTTP qui est établie par le document de la demande.

Types de document cXML

Un document cXML peut se présenter sous trois types : Demande, Réponse ou Message.

Demande

Il existe plusieurs types de demandes cXML. L'élément `Request` du Document cXML correspond au type de documents dans WebSphere Partner Gateway. Les éléments de demandes classiques sont les suivants :

- OrderRequest
- ProfileRequest
- PunchOutSetupRequest
- StatusUpdateRequest
- GetPendingRequest
- ConfirmationRequest
- ShipNoticeRequest

La table suivante illustre la relation entre les éléments d'un document de demande cXML et les définitions de documents dans WebSphere Partner Gateway :

Elément cXML
définition de document

DOCTYPE cXML
Protocole

Version DTD
Version de protocole

Demande (type) OrderRequest par exemple
Type de document

Réponse

Le partenaire cible envoie un réponse cXML pour indiquer au partenaire source les résultats de la demande cXML. Etant donné que les résultats de certaines demandes peuvent ne contenir aucune donnée, l'élément `Response` peut contenir uniquement un élément `Status`. Un élément `Response` peut également contenir toute donnée de niveau application. Par exemple, lors de la phase PunchOut, les données de niveau application sont contenues dans un élément `PunchOutSetupResponse`. Les éléments `Response` classiques sont les suivants :

- ProfileResponse
- PunchOutSetupResponse
- GetPendingResponse

La table suivante illustre la relation entre les éléments d'un document de réponse cXML et les définitions de documents de WebSphere Partner Gateway :

Elément cXML
définition de document

DOCTYPE cXML
Protocole

Version DTD
Version de protocole

Réponse (type) ProfileResponse, par exemple
type de document

Message

Une message cXML contient les informations type de documents de WebSphere Partner Gateway dans l'élément `Message` cXML. Il peut éventuellement contenir un élément `Status`, identique à celui d'un élément `Response`. Il serait utilisé dans des messages qui sont des réponses aux messages de demandes.

Le contenu de ce message est personnalisé en fonction des besoins métier de l'utilisateur. L'élément se trouvant directement sous l'élément `<Message>` correspond au type de documents créé dans WebSphere Partner Gateway. Dans l'exemple suivant, SubscriptionChangeMessage est le type de documents :

```
<Message>
<SubscriptionChangeMessage type="new">
           <Subscription>
                <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 table suivante illustre la relation entre les éléments d'un message cXML et les définitions de documents de WebSphere Partner Gateway :

Elément cXML
définition de document

DOCTYPE cXML
Protocole

Version DTD
Version de protocole

Message
Type de document

Le moyen le plus simple de distinguer un message unidirectionnel d'un document Demande-Réponse est la présence d'un élément `Message` au lieu d'un élément de demande ou de réponse.

Un message peut posséder les attributs suivants :

- `deploymentMode`, qui indique si le document est un document de test ou de production. Les valeurs admises sont production (par défaut) ou test.
- `inReplyTo`, qui indique le message auquel répond ce message. Le contenu de l'attribut `inReplyTo` est le payloadID d'un message précédemment reçu. Il serait utilisé pour construire une transaction bi-directionnelle avec plusieurs messages.

En-têtes Content-type et documents joints

Tous les documents cXML doivent contenir un en-tête Content-type. Pour les documents cXML ne contenant pas de pièces jointes, les en-têtes Content-type suivants sont utilisés :

- Content-Type: text/xml
- Content-Type: application/xml

Le protocole cXML prend en charge la connexion des fichiers externes via le format MIME. Par exemple, les clients ont souvent besoin de se remémorer les ordres d'achat à l'aide de mémos, dessins ou télécopies. L'un des en-têtes Content-type répertorié ci-dessous doit être utilisé dans les documents cXML contenant des pièces jointes :

- Content-Type: multipart/related; boundary=<*quelquechose_unique*>
- Content-Type: multipart/mixed; boundary=<*quelquechose_unique*>

L'élément `boundary` est un texte unique, utilisé pour séparer le corps du du message MIME de la partie données utiles. Pour plus d'information, consultez le guide d'utilisateur cXML à l'adresse www.cxml.org.

Interactions cXML correctes

WebSphere Partner Gateway prend en charge les interactions de définition de documents cXML :

- D'un partenaire externe vers un partenaire interne : None/cXML vers None/cXML avec Passe-système et validation
- D'un partenaire interne vers un partenaire externe :
  - None/cXML à None/cXML avec Passe-système et validation.
  - None/XML à None/cXML avec Passe-système, validation et transformation.

Création de définitions de documents

Pourquoi et quand exécuter cette tâche

Procédez comme suit pour créer une nouvelle définition de documents pour un document cXML.

Remarque : Vous devez vous assurer que la version correcte de cXML est définie avant de créer une définition de documents. La version par défaut est 1.2.009.

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **Définition de documents**.
2. Cliquez sur **Création d'une définition de documents**. La page Création d'une définition de documents s'affiche.
3. Sélectionnez **Type de documents** comme type de documents.
4. Selon le type de document, appliquez l'une des étapes suivantes :
   - Pour les demandes, entrez son type (par exemple `OrderRequest`) dans la zone **Nom**
   - Pour les réponses, si Response n'a aucune autre balise enfant que `<Status>`, entrez `Response`. Sinon, entrez le nom de balise qui suit `<Status>`. Dans cet exemple, vous entreriez `Response` pour le premier élément Response et `Profile Response` pour le second.

```
<cXML>
    <Response>
        <Status code="200" text="OK"/>
```

```
    </Response>
</cXML>
<cXML>
    <Response>
        <Status code="200" text="OK"/>
   </ProfileResponse>
    </Response>
</cXML>
```

5. Entrez **1.0** pour la **version**.

   Le numéro de version est indiqué uniquement à titre de référence. Le protocole réel de la version provient de la version DTD se trouvant dans le document cXML.
6. Entrez une **description** facultative.
7. Sélectionnez **Oui** pour **Niveau du document**.
8. Sélectionnez **Activé** pour **Etat**.
9. Sélectionnez **Oui** pour tous les attributs **Visibilité**.
10. Cliquez sur le dossier **Package : None** pour étendre les options de sélection d'empaquetage.
11. Sélectionnez **Protocole : cXML (1.2.009): cXML**.
12. Cliquez sur **Sauvegarder**.

Création d'interactions

Pourquoi et quand exécuter cette tâche

Après avoir créé la définition de documents, définissez une interaction pour le document cXML.

Pour créer des interactions, procédez comme suit :

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Si le document cXML est la source, sous **Source**, développez **Package : None** et **Protocole : cXML**, puis sélectionnez **Type de documents :**<*document _flow*>. Si le document cXML est la cible, développez **Package : None** et **Protocole : cXML**, puis sélectionnez **Type de documents :** <*document_flow*> dans la colonne **Cible**.
4. Développez la colonne source ou cible pour la seconde moitié de l'interaction (le document sera converti en cXML ou transformé à partir de cXML), développez le package et le protocole et sélectionnez son type de documents.
5. Sélectionnez **Passe-système** dans la liste des **Actions** figurant en bas de la page (**Pass-système** est la seule option prise en charge pour les documents cXML).

Traitement de documents XML personnalisés

Cette section décrit la configuration du concentrateur pour router les documents XML qui ne sont pas gérés par les autres protocoles de routage intégrés.

XML personnalisé est un terme de WebSphere Partner Gateway utilisé pour désigner les documents XML qui ne sont gérés par aucun des protocoles intégrés.

La manière dont les documents XML personnalisés sont identifiés est un processus d'élimination. En fonction de l'ordre des étapes d'analyse de protocole de flux de travaux entrants, le concentrateur tente de mettre en correspondance les documents

XML avec chacun des protocoles standard avant que ne soit appelée l'étape d'analyse standard qui gère le XML personnalisé. Le gestionnaire de XML personnalisé est appelé pour tout document XML que ne correspond pas à l'un des types de documents XML standard.

Pour traiter un document XML personnalisé, l'interpréteur de protocole doit extraire des informations du document. Votre collection de formats XML, définitions de protocole de documents et définitions de type de documents fournit à l'interpréteur de protocole XML personnalisé les informations dont il a besoin pour reconnaître et traiter un document à l'aide de votre configuration.

Depuis un niveau élevé, voici la manière dont fonctionne le protocole XML personnalisé :

1. Le document XML est analysé pour obtenir l'un de ces éléments qui existent : valeur du nom DTD du document; espace de nom de balise racine et nom de balise racine.
2. En fonction des identificateurs obtenus au cours de la première étape, un ensemble de familles de documents qui contiennent les formats XML est identifié comme correspondance possible pour le document. Vous apprendrez à créer des familles de documents et formats XML ultérieurement, dans «Création de formats XML», à la page 165.
3. Chaque mise en correspondance possible de format XML à partir des familles est appliquée au document pour voir s'il lui correspond. La mise en correspondance est évoquée plus loin dans cette section.
4. Lorsqu'un format XML correspondant est trouvé, il est utilisé pour extraire les données du document utilisé par le concentrateur pour traiter le document. La famille de documents dont le format XML est membre détermine le protocole de document utilisé pour le routage. La mise en correspondance du format XML est déterminée avec le type de document utilisé pour le routage.

Dans la page Gestion des protocoles XML, vous pouvez créer les familles de documents associées aux protocoles de documents. Vous renseignez ensuite les familles de format avec les formats XML associés aux types de documents.

une Le format XML comprend deux types d'informations :

- Les expressions XPath utilisées pour extraire les informations des documents XML.
- Les données littérales utilisées comme valeur constante.

Les formats XML sont utilisés par le gestionnaire de documents pour récupérer les valeurs qui identifient de façon unique un document entrant et d'accéder aux informations contenues dans le document qui s'avèrent nécessaires à un routage et à un traitement corrects.

La procédure de création d'un format XML personnalisé comporte plusieurs étapes. Pour ce faire, procédez comme suit :

1. Créez un protocole qui sera utilisé pour router un ensemble de documents connexes et associez-le à un ou plusieurs packages.
2. Créez un type de document pour le format et associez-le au protocole que vous venez de créer.
3. Créez une famille de documents pour contenir un ensemble de formats XML qui correspondent aux documents routés avec le protocole.
4. Ajoutez des formats XML à la famille, lesquels sont chacun associés à l'un des types de documents pour le protocole de la famille.

Vous créez ensuite des interactions entre les nouveaux types de documents, de sorte que des connexions puissent être effectuées.

Ces étapes sont décrites dans les sections qui suivent. Vous pouvez également trouver un exemple de ces étapes dans «Configuration du concentrateur pour les documents XML personnalisés», à la page 345.

Création de formats XML

Les formats XML sont utilisés pour identifier et extraire des données de documents XML personnalisés afin de pouvoir être traités. Les formats XML sont contenus dans des familles de documents. Une famille de documents est une collection de formats XMl associés qui partagent un nom DTD, une balise d'élément principal, ou un espace de nom d'élément principal communs. Il existe donc trois types de familles de documents : les familles DTD, les familles Balises principales et les familles Espace de nom.

Les familles de documents jouent deux rôles :

- Elles peuvent déterminer le mode de routage des documents. Pendant l'exécution, lorsqu'un document correspond à un format XML, le protocole et la version de routage associés à la famille du format sont utilisés pour router un document.
- Elles peuvent vous aider à organiser les formats XML dans le système. Lorsque vous configurez le système, vous pouvez organiser vos formats XML par familles. Par exemple, vous pouvez regrouper des messages d'achat dans une famille appelée messages d'achat et vous pouvez rechercher une famille de documents pour accéder aux formats se trouvant dans une famille particulière.

Création d'une famille de documents

Pourquoi et quand exécuter cette tâche

Pour regrouper des formats XML associés dans une famille, vous devez d'abord créer une famille. Pour créer une famille de documents, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **Formats XML**.
2. Cliquez sur **Création d'une famille de documents**.
3. Dans l'écran Nouvelle famille de documents, saisissez un **Nom de famille**.

   Remarque : Plusieurs familles peuvent avoir le même identificateur ou nom. Le type d'identificateur associé au nom forme une clé de famille unique. Par exemple, supposons que vous vouliez router des messages SOAP à l'aide du gestionnaire XML personnalisé. Si vous avez plusieurs types de messages SOAP, vous pouvez les classer dans des familles avec des noms différents ayant tous Enveloppe comme identificateur de balise racine.
4. Sélectionnez un **Protocole** dans la liste des protocoles disponibles dans le système. Vous devez définir un protocole personnalisé avant de définir la famille qui l'utilise. Vous ne pouvez pas modifier le protocole d'une famille une fois que la famille est créée, donc prévoyez bien à l'avance.
5. Sélectionnez une **Option grand fichier** : None, Utiliser un processeur de grand fichier ou Utiliser un processeur de grand fichier reconnaissant les espaces de nom.

   None signifie que les formats XML de la famille peuvent utiliser les expressions XPath version 1.0, mais que la taille des fichiers pouvant être traités sera limitée

par plusieurs facteurs, dont la configuration de mémoire du gestionnaire de documents, la charge de travail du gestionnaire de documents et la structure des documents qui sont traités.

Utiliser le processeur de grand fichier ou **Utiliser le processeur de grand fichier reconnaissant les espaces de nom** signifie que la taille du fichier n'est pas une limite mais que vous êtes limité pour utiliser des expressions de chemin d'accès à un élément simple dans les formats XML qui sont membres de la famille.

Utilisez une option grand fichier si vous écrivez des formats XML qui correspondront à de grands documents que ne peuvent être gérés à l'aide du processeur full XPath. Si vous sélectionnez l'option reconnaissance d'espace de nom, les chemins d'accès aux éléments comprendront les préfixes d'espace de nom lorsqu'ils apparaissent dans un document.

6. Sélectionnez un document **Type de famille** dans la liste : DTD, balise racine, ou espace de nom.
7. Saisissez un **Identificateur de famille** pour le type de famille que vous créez :

Tableau 23. Identificateurs des types de famille

Pour ce type de famille	Saisissez cela comme identificateur
DTD	Le nom DTD
Balise racine	La balise racine des messages qui sont dans cette famille **Remarque :** Omettez le préfixe d'espace de nom s'il en existe un.
Espace de nom	L'espace de nom de la balise racine

Cet identificateur est utilisé pendant l'exécution pour sélectionner une famille de formats XML, dont l'un peut être mis en correspondance avec le document et utilisé pour en extraire les informations de traitement. Notez que si plusieurs familles utilisent le même identificateur, les formats dans toutes les familles seront contrôlés par rapport au message, jusqu'à ce qu'une correspondance soit trouvée.

8. Cliquez sur **Sauvegarder** pour sauvegarder la nouvelle famille ou cliquez sur **Annuler** pour arrêter la création d'une famille de documents ou sur**Retour** pour revenir à la vue initiale.

Rechercher une famille de documents

Pourquoi et quand exécuter cette tâche

Pour afficher une famille de documents, vous devez d'abord la trouver. Pour trouver une famille de documents, procédez comme suit :

Procédure

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **Formats XML**.
2. Sélectionnez le protocole de la famille de documents que vous voulez afficher.
3. Saisissez le nom de famille si vous le connaissez. Vous pouvez utiliser un astérisque (*) pour effectuer une recherche générique
4. Sélectionnez le type de famille : Tout type, DTD, Espace de Nom ou Balise Racine.
5. Sélectionnez l'option Grand fichier : Aucun, Utiliser le processeur de grand fichier, Utiliser le processeur de grand fichier avec reconnaissance espace de nom

6. Cliquez sur **Rechercher**. Toutes les familles de documents correspondant à vos critères de recherche apparaîtront sous le bouton Rechercher.
7. Cliquez sur l'icône **Afficher les détails** à côté d'une famille de documents pour en voir les détails.

Edition d'une famille de documents

Pourquoi et quand exécuter cette tâche

Dans la fenêtre Caractéristiques de la famille de documents, vous pouvez éditer les propriétés d'une famille. Pour ce faire, procédez comme suit :

Procédure

1. Cliquez sur le bouton Stylo dans la vue Caractéristiques de la famille pour afficher une vue Edition d'une famille de documents. Notez que le protocole ne peut pas être modifié dans cette vue. C'est parce qu'il peut y avoir eu des messages routés à l'aide de formats dans la famille et que si le protocole associé à la famille était modifié, cela rendrait difficile le débogage.
2. Dans la vue Edition de la famille de documents, vous pouvez maintenant modifier le nom de famille, le type de famille et l'identificateur de famille.
3. Une fois vos modifications effectuées, cliquez sur **Sauvegarder** pour les sauvegarder. Cliquez sur **Annuler** ou sur le bouton du Stylo barré, pour revenir à la vue des détails de la famille sans sauvegarder les modifications.

Ajout d'un nouveau format XML à une famille

Pourquoi et quand exécuter cette tâche

Dès que vous avez créé une famille de documents, vous pouvez ajouter de nouveaux formats XML à cette famille. Pour ce faire, procédez comme suit :

Remarque : Dans cette section, le terme expression XPath est souvent utilisé. Lorsqu'un format XML utilise une option Grand fichier, ce terme doit être considéré comme désignant une expression Chemin d'élément, qui est un chemin d'accès simple depuis la racine d'un document vers un élément qui a une valeur.

1. A partie de la Caractéristiques d'une famille de documents, cliquez sur **Créer un format XML**. La vue définition de format XML s'affiche. Cette page se divise en quatre sections sous les en-têtes **définition du type de document**, **Critères de définition du type de document**, **Attributs Document** et **Attributs définis par l'utilisateur**.
2. Complétez la section **Définition du type de document**.

   Dans la section définition du type de document se trouve une liste de sélection avec les types de documents contenus dans le protocole associé à la famille du document. Dans cette liste, sélectionnez un **Type de Document type**. Lorsqu'un document correspond au format XML, le protocole associé à la famille de documents et le type de document associé au format sont utilisés pour router le document.
3. Complétez la section **Critères de définition du type de document**.

   La section **Critères de définition du type de document**et la section **Attributs du document** comprennent des zones dans lesquelles vous saisissez des valeurs et chemins d'accès à des éléments si vous utilisez l'option grand fichier ou saisissez des expressions XPath, espace de nom de préfixe et types de retour si tel n'est pas le cas.

   Valeur Dans cette zone, entrez une valeur pour l'identificateur de format. Cette zone est obligatoire.

Chemin d'accès à un élément

Dans cette zone, saisissez un chemin d'accès à un élément. Cette zone est obligatoire. Notez que ce chemin d'accès à un élément ne s'applique qu'aux formats qui utilisent l'option grand fichier.

Expression XPath

Dans cette zone, saisissez soit une expression XPath valide pour le document qui correspond au format soit une valeur de chaîne littérale qui est renvoyée comme constante pour tous les documents. Cette zone est obligatoire. Notez que les expressions XPath ne sont utilisées que dans les formats qui n'utilisent pas l'option grand fichier.

Zone Espace de nom de préfixe

Dans cette zone, saisissez la définition du dernier préfixe d'espace de nom, le cas échéant, utilisé dans votre expression XPath. Il a la forme du qualificatif prefix=namespace. Ainsi, si le dernier préfixe d'espace de nom de votre expression est SOAPENV et que son qualificatif est http://schemas.xmlsoap.org/soap/envelope/ vous saisiriez alors SOAPENV=http://schemas.xmlsoap.org/soap/envelope/ pour le préfixe d'espace de nom. Notez que les formats qui utilisent une option grand fichier n'ont pas de zone espace de nom de préfixe dans leur définition.

Type de retour

Dans cette zone, sélectionnez soit Constant, soit Texte, ou Nom de balise d'élément dans la liste de sélection. Utilisez Constant lorsque vous voulez interpréter la zone expression XPath comme chaîne littérale pour tous les documents. Utilisez Texte lorsque vous voulez utiliser le moteur d'évaluation XPath pour évaluer l'expression dans le contexte du document. Utilisez le Nom de balise d'élément lorsque vous voulez obtenir le nom d'élément pour le premier élément renvoyé par l'évaluation XPath de l'expression. Notez que les formats qui utilisent une option grand fichier n'ont pas de nom de balise d'élément comme type de retour.

Dans la section dans critères de définition du type de document, vous saisissez les valeurs et expressions XPath. Les valeurs et les résultats d'évaluation d'expression sont comparés lorsque les documents sont traités afin de déterminer si un format XML correspond à un document. Lorsqu'une correspondance est trouvée entre un document et un format et lorsque les identificateurs entreprise source et cible peuvent être trouvés à l'aide du format, le document est routé à l'aide du protocole et du type de document désigné dans la section définition du type de document. Voir le tableau 24, à la page 169 pour des détails sur les zones de cette section.

Tableau 24. Zones Critères de définition du type de document

Zone	Obligatoire/ facultatif	Action
Identificateur de format	Obligatoire	Saisissez l'expression XPath ou le chemin d'accès à l'élément qui définit le chemin d'accès au contenu dans les documents XML et qui identifie de manière unique le document. Par exemple, si la balise racine ressemble à <PurchasingMessage type="Purchase Order"> pour les bons de commande et ressemble à ça <PurchasingMessage type="Order Confirmation"> pour les confirmations, alors l'expression XPath /PurchasingMessage/@type renverrait le texte 'Bon de commande' pour certains messages et 'Confirmation de commande' pour d'autres. Deux formats XML, un pour les commandes et un autre pour les confirmations, seraient écrits et la zone 'Valeur' pour les commandes indiquerait 'Bon de commande' et la zone 'Valeur' pour les confirmations indiquerait 'Confirmation de commande'. Pendant l'exécution, le format adéquat peut être localisé par le système car il recherchera un format dans lequel l'évaluation d'expression renvoie un résultat correspondant à la valeur. Lorsque la correspondance est trouvée, le type de document de routage associé au format est utilisé par le système.
Version de format	Obligatoire	Saisissez l'expression XPath ou le chemin d'accès à l'élément qui définit la version de format. La version de format est évaluée de la même manière que pour l'identificateur de format. Lorsque l'expression pour la version correspond à la valeur de version d'un format, le format peut alors être utilisé si l'identificateur correspond également. Notez que s'il n'existe qu'une seule version d'un document, vous pouvez soit saisir '1' pour l'expression avec un type de retour Constant et '1' pour la valeur. Cela signifie que la version correspondra toujours et que l'identificateur seul est utilisé pour déterminer un format de correspondance.

4. Complétez la section **Attributs de document**.

   Dans la section **Attributs de Document**, saisissez les valeurs et expressions XPath, comme vous l'avez fait pour la section **Critères de définition du type de document**. Voir le tableau 25 pour plus de détails sur les zones de cette section.

Tableau 25. Zones Attributs du Document

Zone	Obligatoire/facultatif	Action
Identificateur d'entreprise source	Obligatoire	Saisissez l'expression XPath ou le chemin d'accès à l'élément qui définit le chemin d'accès de l'ID d'entreprise source dans le document XML. Elle est utilisée pour identifier le partenaire source à des fins de routage. Notez que ces données doivent être trouvées pour le format à utiliser.

Tableau 25. Zones Attributs du Document (suite)

Zone	Obligatoire/facultatif	Action
Identificateur d'entreprise cible	Obligatoire	Saisissez l'expression XPath ou le chemin d'accès à l'élément qui définit le chemin d'accès de l'ID d'entreprise cible dans le document XML. Elle est utilisée pour identifier le partenaire cible à des fins de routage. Notez que ces données doivent être trouvées pour le format à utiliser.
Identificateur de document	Facultatif	Saisissez l'expression XPath ou le chemin d'accès à l'élément qui définit le chemin d'accès pour le numéro d'ID de document dans le document XML. Cette valeur s'affichera dans l'afficheur de documents.
Horodatage de document	Facultatif	Saisissez l'expression XPath ou le chemin d'accès à l'élément qui définit le chemin d'accès à l'horodatage de création du document dans le document XML. Cette valeur s'affichera dans l'afficheur de documents.
Touches de vérification des doubles 1 - 5	Facultatif	Saisissez les expressions ou les chemins d'accès à un élément qui définissent les chemins d'accès utilisés pour identifier si un document est unique ou un double.
Indicateur synchrone	Facultatif	Saisissez une expression XPath ou un chemin d'accès à un élément qui évalue à *vrai* ou *faux* , en indiquant si ce type de document exige une réponse synchrone ou non. Vous pouvez saisir soit une expression XPath qui utilise le contenu de document pour définir la valeur, soit saisir la littéral chaîne vraie ou fausse avec un type de retour Constant. Si cette zone est définie sur vrai, l'attribut BCGDocumentConstants. BCG_GET_SYNC_RESPONSE sera défini dans BDO pendant le traitement d'analyse du canal.
Elément de racine de validation	Facultatif	Saisissez l'expression XPath qui définit le noeud racine du contenu (charge) d'un message enveloppé dans un document XML. WebSphere Partner Gateway validera un document commençant par cet élément. Vous devez spécifier une action qui effectue la validation pour effectuer ce travail. Cette zone n'existe que dans les formats qui utilisent l'option grand fichier.

Tableau 25. Zones Attributs du Document (suite)

Zone	Obligatoire/facultatif	Action
ID de document associé	Facultatif	Saisissez l'expression XPath ou le chemin d'accès à l'élément qui indique l'identificateur de document d'un document préalablement routé et auquel le document en cours est associé. Par exemple, une Confirmation de commande est généralement associée à un Bon de commande. La valeur de l'identificateur de document Bon de commande peut être obtenue à l'aide d'une expression XPath (voir ci-dessus). Si la Confirmation de commande contient l'identificateur de Bon de commande, alors elle peut être obtenue à l'aide de l'expression de l'ID de document associé. Cela liera les documents dans l'afficheur de documents.
Zones de recherche 1- 10	Facultatif	Saisissez les expressions ou les chemins d'accès à un élément qui définissent les chemins d'accès jusqu'à un contenu de document que vous voulez utiliser pour les recherches personnalisées dans le document XML. Dans l'afficheur de documents, vous pouvez rechercher des documents en fonction des valeurs de ces zones.

5. Complétez la section **Attributs définis par l'utilisateur**.

   Dans la section **Attributs définis par l'utilisateur**, vous pouvez ajouter des attributs personnalisés, définis par l'utilisateur. Vous ajoutez un attribut en saisissant son nom dans la zone de saisir et en cliquant sur **Ajouter**. Vous définissez ensuite ce nouvel attribut comme vous le feriez pour les autres attributs standard en saisissant, le cas échéant, l'expression XPath, le chemin d'accès à l'élément, l'espace de nom de préfixe et en sélectionnant un type de retour pour cet attribut

   Une fois que vous avez ajouté ces attributs, ils sont utilisés de la même manière que les attributs standard. Si vous souhaitez supprimer un attribut défini par l'utilisateur à partir d'un format, cliquez sur le X rouge qui apparaît à côté de son nom. Les attributs définis par l'utilisateur sont destinés à être utilisés par les gestionnaires écrits par l'utilisateur qui traitent le document. Les noms d'attribut ainsi que leurs valeurs sont ajoutés au document commercial lorsque celui-ci est traité. Votre code de gestionnaire peut y accéder en les obtenant auprès du document commercial à l'aide des noms que vous avez définis. Consultez *Le Guide du programmeur WebSphere Partner Gateway* pour plus d'informations.
6. Après avoir saisi les valeurs dans cette vue, accédez au bas de celle-ci et cliquez sur **Sauvegarder** pour enregistrer les modifications. Cliquez sur **Annuler** ou sur le bouton du stylo barré pour annuler les changements et revenir à la vue récapitulatif sur la famille.

Routage de messages XML avec différents préfixes d'espace de nom

Pourquoi et quand exécuter cette tâche

Lors du routage des messages XML, vous devez configurer une définition de format XML contenant l'espace de nom et le préfixe exacts définis dans le message XML. Lorsque vous utilisez différents préfixes d'espace de nom, configurez le

routage de messages XML dans la console de WebSphere Partner Gateway. Les trois méthodes permettant d'effectuer la configuration sont les suivantes :

- Création d'une famille de documents et d'un format XML pour tout message qui utilisera les différents préfixes d'espace de nom.
- Création d'une famille de documents et d'un format XML pour le nom local (balise racine de schéma).
- Création d'une famille de documents et d'un format XML, à l'aide d'une combinaison de nom local et d'espace de nom.

Création d'une famille de documents et d'un format XML pour tout message qui utilisera différents préfixes d'espace de nom :

1. Naviguez jusqu'à **Administrateur du concentrateur** > **Configuration du concentrateur** > **Formats XML**.
2. Cliquez sur le lien **Création d'une famille de documents**.
3. Dans la page **Nouvelle famille de documents**, créez une nouvelle famille de documents de type *espace de nom*.
4. Cliquez sur **Sauvegarder**.
5. Cliquez sur le lien **Création du format XML**. Ce format XML sera créé sous la famille de documents nouvellement créée.
6. Dans la page **Définition du format XML**, définissez le format XML pour l'espace de nom et le préfixe à utiliser par le message.
7. Répétez les étapes 2, 3, 4, 5 et 6 pour chaque format XML qui est défini pour le préfixe d'espace de nom. Cependant, créez une famille de documents différente pour chaque format XML.

Créez une famille de documents et un format XML pour le nom local (balise racine de schéma) :

1. Dans la page **Nouvelle famille de documents**, créez une **famille de documents** de type *balise racine*.
2. Créez le format XML sous la famille de documents nouvellement créée. Lors de la définition de l'**expression XPath**, utilisez le nom local (balise racine) pour l'identificateur de format (**identificateur entreprise source** et **identificateur entreprise cible**).
3. Cliquez sur **Sauvegarder**.
4. Envoyez le message XML qui contient les différents espaces de nom du préfixe XML.

   Remarque : Le nom local pour le schéma XML peut aussi être utilisé pour définir d'autres zones dans le format XML, par exemple des Zones de recherche. Les zones de recherche peuvent aussi être définies avec des commandes de mappage à l'aide du client Data Interchange Services ou à travers des exits utilisateur écrits et personnalisés.

Création d'une famille de documents et d'un format XML à l'aide d'une combinaison de nom local et d'espace de nom :

1. Dans la page **Nouvelle famille de documents**, créez une famille de documents de type *espace de nom*
2. Cliquez sur **Enregistrer** pour enregistrer la famille de documents nouvellement créée.
3. Créez le format XML sous la famille de documents nouvellement créée. Définissez le format XML à l'aide d'une combinaison de nom local (balise racine) et d'espace de nom. Par exemple, **expression XPath pour l'identificateur entreprise source :** *//*[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"]* **Expression XPath pour l'identificateur entreprise cible :** *//*[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. Envoyez le message XML qui contient les différents espaces de nom du préfixe XML.

Remarque : La combinaison de nom local et d'espace de nom pour le schéma XML peut aussi être utilisée pour définir d'autres zones au format XML, par exemple des zones de recherche. Les zones de recherche peuvent aussi être définies avec des commandes de mappage à l'aide du client Data Interchange Services ou à travers des exits utilisateur écrits et personnalisés.

Création d'une définition de protocole

Pourquoi et quand exécuter cette tâche

La procédure suivante explique comment créer un format de définition de protocole XML personnalisé :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définitions de documents > Création de définition de documents**.
2. Dans la liste déroulante **Type de définition de documents**, sélectionnez **Protocole**.
3. Dans la zone **Nom**, indiquez un identificateur pour la définition de documents. Par exemple, pour un protocole XML personnalisé, vous pouvez entrer XML_Personnalisé. Cette zone est obligatoire.
4. Pour**Version**, entrez une valeur pour la version de votre protocole. Les valeurs numériques ou valeurs de chaîne sont autorisées.
5. Entrez éventuellement une description du protocole.
6. Donnez au paramètre **Niveau du document** la valeur **Non**, car vous définissez un protocole et non un type de documents (que vous définirez dans la section suivante).
7. Réglez le paramètre **Etat** sur **Activé**.
8. Réglez le paramètre **Visibilité** pour ce protocole. Il est probable que vous souhaiterez le rendre visible à tous les partenaires.
9. Sélectionnez les packages dans lesquels ce nouveau protocole sera encapsulé. Par exemple, si vous souhaitez que ce protocole soit associé aux trois packages, sélectionnez **Package : AS**, **Package : None** et **Package : Backend Integration**.
10. Cliquez sur **Sauvegarder**.

Création d'une définition de type de documents

Pourquoi et quand exécuter cette tâche

Ensuite, utilisez de nouveau la page Création d'une définition de documents pour créer un type de documents.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définitions de documents > Création de définition de documents**.

2. Dans la liste déroulante **Définition de Type de documents**, sélectionnez **Type de documents**.
3. Dans la zone **Nom**, indiquez un identificateur pour la définition de documents. Par exemple, vous pouvez entrer `Bon de commande` comme nom de type de documents. Cette zone est obligatoire.
4. Pour**Version**, entrez une valeur pour la version de votre type de document. Les valeurs numériques ou valeurs de chaîne sont autorisées.
5. Entrez éventuellement une description du type de document.
6. Donnez au paramètre **Niveau du document** la valeur **Oui** (car vous définissez un objet de routage correspondant à un document réel).
7. Réglez le paramètre **Etat** sur **Activé**.
8. Réglez le paramètre **Visibilité** pour ce flux. Il est probable que vous souhaiterez le rendre visible à tous les partenaires.
9. Cliquez sur l'icône **Développer** pour développer chaque package sélectionné lors de l'étape 9, à la page 173. Développez le dossier, puis sélectionnez le nom du protocole créé à la section précédente (en l'occurrence, Protocole : XML_Personnalisé).
10. Cliquez sur **Sauvegarder**.

Si vous avez utilisé les valeurs d'exemple, la page Gérer des définitions de documents contient désormais un type de documents Bon de commande et un protocole XML personnalisé sous les packages AS, None et Backend Integration.

Parachèvement de la configuration

Une fois la définition de protocole effectuée, vous pourrez la choisir comme protocole de routage à utiliser pour une famille de documents XML. Après avoir ajouté des types de documents au protocole, vous pourrez les assigner aux définitions de format XML qui se trouvent dans la famille de documents. Les messages qui correspondront à un format de la famille seront routés via le protocole associé à la famille et au type de document associé au format correspondant.

Avant de pouvoir définir les canaux qui utiliseront les nouvelles définitions, vous devez activer les interactions entre vos nouveaux protocoles et les types de documents et autres protocoles et types de documents. Vous devrez peut-être également activer les fonctions business-to-business de vos partenaires pour envoyer et recevoir des documents à l'aide des nouveaux protocole et types de documents.

Validation d'un fichier XML personnalisé par rapport à un fichier XSD

Une fois effectuée la configuration basique du langage XML personnalisé (définition du type de document, création de la famille XML et du format XML, fonctions business-to-business et connexion) et lorsque le document XML est prêt à être acheminé vers l'action simple "Passe-système", procédez comme suit pour permettre la validation du document XML avant l'opération passe-système :

1. Dans la page **Connexions**, définissez *Passe-système XML personnalisé avec validation* en tant que nouvelle action.
2. Accédez à **Administrateur du concentrateur** > **Configuration du concentrateur** > **Définition de documents**.
3. Cliquez sur l'icône **Editer les valeurs des attributs** (flèche bleue) pour le type de document XML personnalisé.

4. Sélectionnez **Charger une mappe**.
5. Sélectionnez le fichier XSD correspondant et cliquez sur **Télécharger**.
6. Répétez les étapes 2-3.
7. Cliquez sur **Ajouter des attributs** pour ajouter des attributs de contexte de définition de document.
8. Sélectionnez **Mappe de validation** et cliquez sur **Sauvegarder**.
9. Dans **Administrateur du compte** > **Connexions**, recherchez la connexion.
10. Cliquez sur **Attributs** du côté **Source** de la connexion.
11. Développez l'icône de noeud réduite (dossier bleu) pour le type de document.
12. Dans la liste déroulante **Mappe de validation**, sélectionnez la mappe de validation XSD et cliquez sur **Sauvegarder**.

Si vous avez besoin de télécharger une version plus récente du fichier XSD, vous devez d'abord supprimer l'ancienne version. Pour cela, rendez-vous sur la page **Administrateur du concentrateur** > **Configuration du concentrateur** > **Mappes** > **Mappes de validation**. Après avoir téléchargé la nouvelle mappe, répétez l'étape 12, car la suppression d'une mappe réinitialise ses attributs de connexion.

Utilisation de mappes de validation

WebSphere Partner Gateway fait appel à des mappes de validation pour valider la structure de certains documents. Si vous souhaitez associer une mappe de validation à un document, assurez-vous que la mappe soit disponible pour WebSphere Partner Gateway, de la façon décrite dans la section «Ajout de mappes de validation». Pour la gestion des mappes de validation, voir le *Chapitre sur les tâches d'administration du concentrateur du Guide d'administration de WebSphere Partner Gateway.*

Ajout de mappes de validation

Pourquoi et quand exécuter cette tâche

Vous pouvez associer une action à une mappe de validation pour être certain que le partenaire de destination ou le système dorsal peut procéder à une analyse syntaxique du document. Sachez qu'une mappe de validation ne fait que valider la *structure* du document. Elle ne valide pas le contenu du message.

Remarque : Une fois que vous avez associé une mappe de validation à une définition de documents, vous ne pouvez plus les dissocier.

Pour ajouter une nouvelle mappe de validation au concentrateur, procédez comme suit :

1. Enregistrez le fichier de la mappe de validation dans le concentrateur ou un emplacement où WebSphere Partner Gateway peut lire les fichiers.
2. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de validation**.
3. Cliquez sur **Créer**.
4. Entrez une description de la mappe de validation.
5. Naviguez jusqu'au fichier schéma que vous voulez utiliser pour valider les documents et cliquez sur **Ouvrir**.
6. Cliquez sur **Sauvegarder**.

Association de mappes à des définitions de documents

Pourquoi et quand exécuter cette tâche

Pour associer une mappe de validation à une définition de documents, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de validation**.
2. Cliquez sur l'icône **Afficher les détails** en regard de la mappe de validation que vous voulez associer à la définition de documents.
3. Cliquez sur l'icône **Développer** en regard d'un package pour le développer jusqu'au niveau voulu (par exemple **Action** pour un document RosettaNet).
4. Sélectionnez la définition de documents que vous voulez associer à la mappe de validation.
5. Cliquez sur **Sauvegarder**.

Utilisation des mappes de transformation

Etapes pour utiliser les mappes de transformation, qui permettent de convertir un document d'un format en un autre.

Pourquoi et quand exécuter cette tâche

WebSphere Partner Gateway utilise des mappes de transformation pour convertir des documents d'une forme en une autre, par exemple, pour convertir un document XML en EDI.

Procédez comme suit pour utiliser les mappes de transformation :

1. Connectez-vous à la console d'administration de WebSphere Partner Gateway.
2. Cliquez sur **Assistants**.
3. Dans l'assistant d'importation EIF, **naviguez** et spécifiez l'emplacement du fichier .EIF.
4. Cliquez sur **Importer**.
5. Dans la page Récapitulatif d'importation, cliquez sur **Suivant**.
6. Dans l'écran Examiner les mappes de transformation et modifier les interactions à créer, sélectionnez la mappe de transformation, ajoutez une interaction et sélectionnez l'action pour l'interaction créée.
7. Cliquez sur **Terminer**.

Important : Si vous téléchargez une mappe de transformation depuis la console de WebSphere Partner Gateway, c'est un fichier d'une taille de 0 Ko qui est téléchargé ; c'est un problème connu. Comme solution palliative, utilisez le client Data Interchange Services pour télécharger ou extraire les mappes de transformation.

Affichage de documents

Pourquoi et quand exécuter cette tâche

L'Afficheur de documents présente des informations sur les documents qui constituent un type de document. Vous pouvez afficher des documents bruts ainsi que les détails des traitements et les événements associés, en précisant les critères de recherche. Ces informations sont intéressantes si vous essayez de savoir si un document a bien été livré ou de déterminer la cause d'un problème.

Démarrez l'Afficheur de documents, en entrant ce qui suit :

1. Cliquez sur **Afficheurs> Afficheur de documents**.
2. Sélectionnez les critères de recherche appropriés.
3. Cliquez sur **Rechercher**.

Consultez le *Guide d'administration de WebSphere Partner Gateway* pour obtenir plus d'informations sur l'utilisation de l'Afficheur de documents.

Configuration de la consignation d'irréfutabilité

Vous pouvez configurer la consignation d'irréfutabilité des messages en utilisant les attributs du package, du protocole ou du flux de documents utilisé pour le routage des documents. L'attribut est nommé Irréfutabilité requise (Non-Repudiation Required) et sa valeur peut être Oui ou Non. Sa définition s'effectue au niveau de l'objet de routage et elle peut être remplacée en la modifiant au niveau de la fonction business-to-business ou au niveau de la connexion.

Configuration de l'emplacement de stockage des messages

Vous pouvez configurer l'emplacement de stockage des messages en utilisant les attributs du package, du protocole ou du flux de documents utilisé pour le routage des documents. L'attribut est appelé Emplacement de stockage des messages requis et sa valeur peut être Oui ou Non. Sa définition s'effectue au niveau de l'objet de routage et elle peut être remplacée en la modifiant au niveau de la fonction business-to-business ou au niveau de la connexion.

Chapitre 10. Configuration des flux de documents EDI

Le présent chapitre décrit la méthode de configuration des définitions de documents et des interactions pour les EDI standard. Il décrit également la réception et la transformation de documents XML et ROD (record-oriented-data). Ce chapitre contient les rubriques suivantes.

Un EDI peut être transmis sans désenveloppement ni transformation. La procédure de création d'interactions pour ce type d'échanges est présentée à la section «Documents EDI avec actions de passe-système», à la page 116.

Remarque : Pour effectuer des modifications de configurations sur WebSphere Partner Gateway, vous devez toujours utiliser la même instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Présentation d'EDI

L'EDI est une méthode pour transmettre des informations métier par le réseau, entre des partenaires qui acceptent d'appliquer des standards industriels ou nationaux approuvés en matière de translation et d'échange d'informations. WebSphere Partner Gateway assure le désenveloppement, la transformation et l'enveloppement des standards EDI suivants :

- X12, un standard EDI commun approuvé par l'American National Standards Institute
- UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Support)
- UCS (Uniform Communication Standard)

Les sections qui suivent présentent rapidement les EDI conformes aux standards X12, EDIFACT et UCS, ainsi que les transactions et groupes contenus dans ces échanges. Sont également décrits les transformations des documents XML et ROD ainsi que les EDI.

Structure d'échange EDI

Un EDI contient une ou plusieurs transactions métier. Dans le standard X12 et les standards associés, une transaction métier est appelée *groupe de transactions*. Dans le contexte du standard EDIFACT et des standards associés, une transaction métier est appelée un *message*. Le présent document utilise généralement le terme *transaction* ou *transaction métier* pour désigner un groupe de transactions X12 ou UCS, ou un message EDIFACT.

Les EDI sont composés de *segments* qui contiennent des *éléments de données*. Ceux-ci sont constitués d'informations telles qu'un nom, une quantité, la date et l'heure. Un segment est un groupe d'éléments de données apparentés. Les segments sont identifiés par un nom ou un libellé qui s'affiche au début du segment (les éléments de données ne sont pas identifiés par leur nom mais sont délimités par des séparateurs spéciaux).

Dans certains cas, il est judicieux de faire la distinction entre les segments de données ou de détails contenus dans une transaction avec les autres segments utilisés à des fins administratives. Les segments administratifs sont appelés *segments de contrôle* dans X12 et *segments de service* dans EDIFACT. Les segments d'*enveloppe* qui délimitent un EDI sont un exemple de segment de contrôle ou de service.

Les EDI peuvent contenir trois niveaux de segments. Chaque niveau commence par un segment d'en-tête et se termine par un segment de fin.

Un EDI possède toujours un segment d'en-tête d'EDI et un segment de fin.

Un EDI peut contenir un ou plusieurs groupes. Un groupe contient une ou plusieurs transactions apparentées. Le niveau de groupe est facultatif dans EDIFACT, mais obligatoire dans le standard X12 et les standards associés. Chaque groupe présent commence par un segment d'en-tête et se termine par un segment de fin.

Un groupe (ou un EDI sans groupe) contient une ou plusieurs transactions. Chaque transaction a un en-tête de groupe de transactions et un élément de fin de groupe de transactions.

Une transaction représente un document métier tel qu'un ordre d'achat. Le contenu du document métier est représenté par les segments de détails placés entre le segment d'en-tête du groupe de transactions et le segment de fin.

Chaque standard EDI dispose de sa propre méthode d'affichage des données dans l'EDI. La table ci-dessous dresse la liste des trois standards EDI pris en charge.

Tableau 26. Segments des standards EDI pris en charge

Segment standard	X12	UCS	EDIFACT
Début de l'EDI	ISA	BG	UNB
Fin de l'EDI	IEA	EG	UNZ
Début du groupe	GS	GS	UNG
Fin du groupe	GE	GE	UNE
Début de la transaction	ST	ST	UNH
Fin de la transaction	SE	SE	UNT

La figure 22 illustre un exemple d'EDI X12, avec les segments qui le composent.

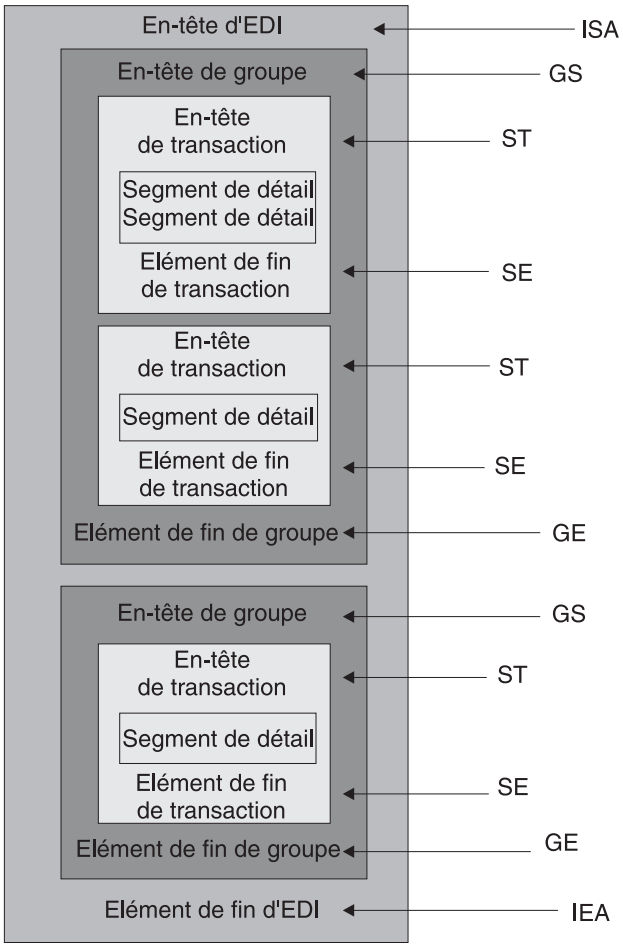


Figure 22. Une enveloppe d'EDI

Mappes

Le spécialiste de mappage du client Data Interchange Services crée des mappes de transformation qui indiquent comment changer le format d'un document. Par exemple, une mappe pour transformer une transaction X12 en message EDIFACT. Vous pouvez également transformer une transaction EDI en document XML ou ROD.

Les mappes peuvent être créées avec DIS ou WTX design studio. DIS permet de créer les mappes pour les transformations WDI et WTX design studio pour les transformations WTX. Les mappes crées à l'aide de DIS ne peuvent pas être migrées pour une transformation WTX et doivent être récrites. En fonction de votre action, le moteur de transformation sera sélectionné si les deux sont opérationnels pour vous.

Pour créer une mappe, la définition des documents source et cible est requise. La définition des documents source pour EDI est fournie par WDI, mais pour ROD et XML, vous devez la créer en utilisant le client DIS. Pour ce standard à utiliser par le code d'exécution, une compilation est nécessaire. Dans les versions précédentes, les mappes de transformation sont requises pour le standard, mais cette version permet d'effectuer une compilation sans mappe de transformation. La EIF standard

pour EDI est importée, mais pour ROD elle est créée avec le client DIS. Dans le cas de XML, DTD/XSD est importé dans la base de données de développement. Pour EDI, dans la console d'administration, accédez aux assistants EDI. Les formats/standards de données accessibles dans le fichier EIF s'affichent. Vous pouvez tout importer en même temps ou en sélectionner un, ou plusieurs, à importer. La chaîne de contrôle de standard sera importée dans la base de données d'exécution.

La mappe de transformation peut aussi créer plusieurs documents à partir d'un seul. Ce type de mappe utilise le *chaînage de mappe*, qui produit plusieurs sorties à partir d'une même transaction. Dans le chaînage de mappe, une fois qu'un document source a été converti en document cible, une autre mappe est utilisée pour convertir de nouveau le document source et produire un autre document cible. Cette opération peut être répétée autant de fois que nécessaire pour produire tous les documents requis.

En plus des mappes de transformation, vous pouvez utiliser des mappes d'accusé de réception fonctionnel et des mappes de validation. Les mappes d'accusé de réception fonctionnel fournissent des instructions sur la production d'un accusé de réception fonctionnel qui informe l'émetteur d'un document EDI que le document est arrivé. Plusieurs mappes d'accusé de réception fonctionnel de standard EDI sont installées en même temps que WebSphere Partner Gateway. Voir «Configuration des accusés de réception», à la page 224 pour obtenir une liste de ces mappes.

Lorsque le concentrateur d'expédition attend un accusé de réception fonctionnel et que celui-ci n'arrive pas dans les délais, le document original est renvoyé. Le nombre de tentatives et d'intervalles entre les nouvelles tentatives peut être configuré. Cette fonction n'est pas activée par défaut. Vous devez définir manuellement la valeur dans les propriétés EDI. Si le délai pour accusé de réception est défini sur Oui, vous devez alors définir des valeurs pour le nombre de tentatives et d'intervalles entre les tentatives. Les événements de relance sont consignés à des fins de contrôle. Si le nombre de tentatives est atteint sans accusé de réception fonctionnel, l'événement approprié sera consigné à des fins de contrôle.

Le spécialiste de mappage du client Data Interchange Services peut créer d'autres mappes d'accusé de réception fonctionnel. WebSphere Partner Gateway génère un accusé de réception fonctionnel lorsqu'une transaction EDI est validée et qu'une mappe d'accusé de réception fonctionnel lui est associée. Le document source doit être de type EDI.

WebSphere Partner Gateway fournit un niveau standard de validation des documents EDI. Si un accusé de réception fonctionnel va être généré, les résultats de la validation d'un document EDI sont sauvegardés. Des mappes de validation sont créées pour permettre des validations supplémentaires sur un document EDI. La génération d'un accusé de réception fonctionnel utilise la mappe d'accusé de réception fonctionnel et les résultats de la validation du document EDI. La mappe d'accusé de réception fonctionnel contient des commandes de mappage qui indiquent comment utiliser les résultats de validation pour créer un accusé de réception fonctionnel donné. Si la translation d'un document est acceptée par le processus de validation, la mappe de transformation des données adéquate est utilisée pour convertir le document source.

Vue d'ensemble des documents XML et ROD

Le spécialiste de mappage du client Data Interchange Services peut créer des définitions de documents XML et ROD ainsi que des mappes de transformation capables de changer le type du document.

Documents XML

Les documents XML sont définis par un DTD ou un schéma XML. Le spécialiste de mappage du client Data Interchange Services crée une mappe de transformation (basée sur le DTD ou le schéma) qui indique comment convertir le document XML dans un autre format. Un document XML peut être transformé en un document XML ou ROD, ou en une transaction EDI.

Documents ROD

L'acronyme ROD (record-oriented data) désigne des documents conformes à un format propriétaire. Le spécialiste de mappage du client Data Interchange Services procède à une définition du document ROD qui détermine la façon dont une application métier structure les données d'un document. Une fois la définition du document terminée, le spécialiste de mappage peut créer une mappe pour transformer le document ROD en un autre document ROD, en document XML ou en transaction EDI.

Utilitaires de fractionnement et documents multiples

Les documents XML ou ROD peuvent entrer dans le concentrateur en tant que documents individuels ou en tant que groupe de documents dans un même fichier. Plusieurs documents peuvent être placés dans le même fichier, par exemple lorsqu'un travail programmé au niveau du partenaire ou du partenaire interne télécharge régulièrement des documents à envoyer. Si plusieurs documents XML ou ROD arrivent dans un fichier, le récepteur appelle le gestionnaire de l'utilitaire de fractionnement (XMLSplitterHander ou RODSplitterHandler) pour fractionner le groupe de documents. (Les gestionnaires d'utilitaires de fractionnement sont configurés lors de la création d'une cible. Pour plus d'informations, voir « Preprocess», à la page 80.) Les documents sont ensuite réintroduits dans le gestionnaire de documents pour être traités individuellement.

Remarque : Les ID de l'émetteur et du récepteur doivent figurer dans la définition du document ROD associée à la mappe de transformation. Les informations nécessaires à l'identification du type du document et des valeurs du dictionnaire doivent également figurer dans la définition du document. Assurez-vous que le spécialiste de mappage client Data Interchange Services ait connaissance de ces exigences lors de la création de la mappe de transformation.

Plusieurs EDI peuvent également être envoyées dans un même fichier. Si plusieurs EDI arrivent dans un fichier, le récepteur appelle le gestionnaire EDISplitterHandler pour les séparer. Les EDI sont ensuite réintroduits dans le gestionnaire de documents pour être traités individuellement.

Remarque : Le fractionnement intervient sur l'EDI, pas sur les transactions qu'il contient. Les transactions de l'EDI sont désenveloppées.

Vue d'ensemble de la création de types de documents et de la définition des attributs

Une définition de documents se compose, au minimum, d'un package, d'un protocole et d'un type de documents. Les définitions de documents précisent les types de documents qui seront traités par WebSphere Partner Gateway.

L'empaquetage est la logique requise pour empaqueter document en fonction d'une spécification, par exemple AS2. Un flux de protocole est la logique exigée pour traiter un document adhérant à un certain protocole, tel que EDI-X12. Un type de documents décrit l'aspect du document.

Les sections suivantes décrivent succinctement les étapes de définition d'un flux de documents entre le partenaire interne et un partenaire externe. Elles décrivent également les points où vous pouvez définir des attributs.

Etape 1 : Assurez-vous que la définition de documents est disponible

Pourquoi et quand exécuter cette tâche

Avant de pouvoir envoyer ou recevoir un document, vous devez procéder à la définition de documents auquel il sera lié. WebSphere Partner Gateway propose plusieurs définitions de documents, dont une qui représente des accusés de réception fonctionnels. Lorsque vous importez des mappes de transformation pour des transactions EDI ou des documents XML ou ROD, les définitions de documents associées apparaissent sur la page des définitions de documents. De la même façon, si vous importez une mappe d'accusé de réception fonctionnel qui n'est pas encore définie, sa définition de documents s'affiche sur la page. Vous pouvez créer vos propres définitions de documents.

Lors de la création d'une définition de documents, vous pouvez modifier certains attributs. Les attributs servent à diverses fonctions de traitement de document et de routage, comme la validation, la vérification pour chiffrement et le nombre de relances. Les attributs que vous définissez au niveau de la définition du document fournissent un paramétrage global du package, protocole ou type de documents associés. Les attributs disponibles varient selon la définition de documents. Les attributs des définitions de documents EDI sont différents de ceux des définitions de documents RosettaNet.

Par exemple, si vous spécifiez une valeur pour **Autoriser une requête TA1** au niveau du type de documents ISA, elle s'applique à tous les documents ISA. Si par la suite vous définissez l'attribut **Autoriser une requête TA1** au niveau des fonctions business-to-business pour un partenaire ou le partenaire interne, cette valeur remplace celle qui était définie au niveau de la définition de documents.

Pour les attributs qui peuvent être définis à plusieurs niveaux de la définition de documents, les valeurs définies au niveau du type de document prévalent sur celles définies au niveau du protocole et ces dernières sont prioritaires sur celles paramétrées au niveau du package. Par exemple, si vous précisez un profil d'enveloppe au niveau du protocole &X44TA1 mais que vous précisez un profil d'enveloppe différent au niveau du type de documents TA1, c'est ce dernier qui est utilisé.

Le type de documents doit figurer sur la page Gérer des définitions de documents pour que vous puissiez créer des interactions.

Etape 2 : Créez des interactions

Pourquoi et quand exécuter cette tâche

Ensuite, vous définissez les interactions, qui sont des modèles pour créer les connexions des partenaires. Les interactions décrivent comment arrive le document, les traitements qu'il subit et comment il est envoyé depuis le concentrateur.

Pour certains protocoles, deux flux suffisent, un pour décrire le document qui est reçu dans le concentrateur (issu du partenaire ou du partenaire interne) et un qui décrit le document qui est envoyé depuis le concentrateur (au partenaire ou au partenaire interne). Toutefois, si le concentrateur envoie ou reçoit un EDI qui sera désenveloppé en transactions individuelles, ou pour lequel des accusés de réception sont requis, vous créerez plusieurs interactions. Par exemple, si vous recevez un EDI dans le le concentrateur, vous aurez une interaction qui décrira comment l'EDI est envoyé au concentrateur et comment il y est traité. Vous aurez également une interaction pour chaque transaction du concentrateur, qui décrit le traitement de la transaction. Pour les EDI qui quittent le concentrateur, vous aurez une interaction qui décrit comment l'enveloppe est envoyée au destinataire.

Etape 3 : Créez les profils, fonctions business-to-business et les destinations des partenaires

Pourquoi et quand exécuter cette tâche

Ensuite, créez les profils de partenaire pour le partenaire interne et les partenaires externes. Définissez les destinations (qui déterminent à quel emplacement les documents seront envoyés) et les fonctions business-to-business qui identifient les documents que le partenaire interne ou un partenaire peut envoyer et recevoir. La page Fonctions B2B répertorie tous les types de documents définis.

Vous pouvez définir des attributs au niveau des fonctions business-to-business. Tout attribut défini à ce niveau a la priorité sur ceux qui ont été définis au niveau de la définition de documents. Par exemple, si vous définissez **Autoriser une requête TA1** sur **Non** au niveau de la définition de documents pour les documents ISA, puis sur **Oui** au niveau des fonctions business-to-business, la valeur **Oui** est utilisée. Le fait de définir un attribut au niveau business-to-business vous permet de le personnaliser en fonction d'un partenaire spécifique.

Si vous définissez le profil d'enveloppe au niveau du protocole ou du type de documents (sur la page Gérer des définitions de documents) puis sur une valeur différente sur la page des fonctions business-to-business, c'est cette dernière valeur qui est utilisée.

Vous devez définir les profils et fonctions business-to-business du partenaire interne et des partenaires externes avant de pouvoir créer des connexions entre eux.

Etape 4 : Activez les connexions

Pourquoi et quand exécuter cette tâche

Enfin, activez les connexions entre le partenaire interne et les partenaires externes. Les connexions disponibles dépendent des fonctions business-to-business des partenaires et des interactions que vous avez créées. Ces dernières dépendent de la disponibilité des définitions de documents.

Pour certains échanges, une seule connexion est requise. Par exemple, si un partenaire envoie un document binaire à une application dorsale du partenaire interne, une seule connexion est requise. Toutefois, dans le cadre des échanges EDI pour lesquels l'EDI est désenveloppé et les transactions individuelles transformées, plusieurs connexions sont définies.

Remarque : Les EDI transmis tels quels n'exigent qu'une seule connexion.

Vous pouvez définir des attributs au niveau de la connexion. Tout attribut défini à ce niveau a le pas sur ceux qui ont été définis au niveau des attributs business-to-business. Par exemple, si vous définissez **Autoriser une requête TA1** sur **Oui** au niveau des fonction business-to-business, puis sur **Non** au niveau de la connexion, la valeur **Non** est utilisée. Le fait de définir la valeur d'un attribut au niveau de la connexion permet de le personnaliser selon les besoins en routage des partenaires et applications impliqués.

Vue d'ensemble des flux disponibles

Cette section présente rapidement les types de transformations réalisées par WebSphere Partner Gateway. Des informations détaillées sur ces transformations et les opérations nécessaires pour les configurer sont indiquées à la section «Définition des échanges de documents», à la page 210.

Flux EDI vers ED

WebSphere Partner Gateway peut accepter un échange EDI émis par un partenaire ou le partenaire interne, le transformer en un type d'échange EDI différent (par exemple, EDI-X12 vers EDIFACT), puis envoyer le document au partenaire interne ou au partenaire. Cette transformation se déroule comme suit :

1. L'EDI reçu au niveau du concentrateur est désenveloppé.
2. Les transactions individuelles comprises dans l'EDI sont transformées dans le format EDI du destinataire.
3. Les transactions EDI transformées sont enveloppées et envoyées au destinataire.

La figure 23 montre un EDI X12 composé de trois transactions désenveloppées. Les transactions sont transformées au format EDIFACT puis enveloppées et envoyées au partenaire.

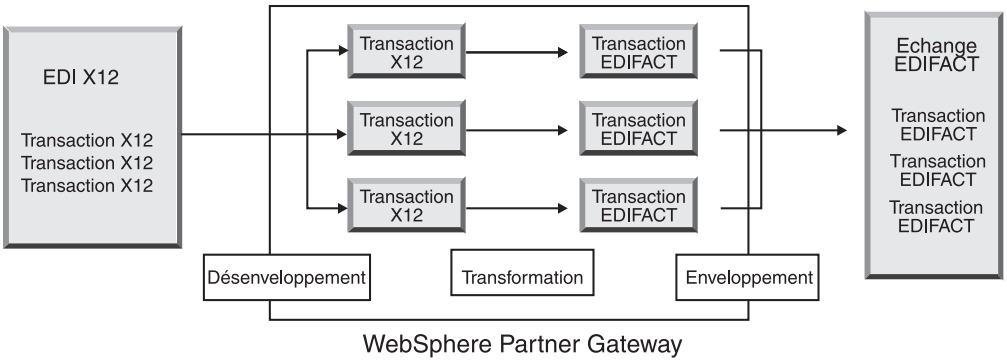


Figure 23. Flux EDI vers EDI

Chacune des transactions est associée à une mappe de transformation qui spécifie comment la transaction est convertie. La transaction peut être transformée en une seule transaction ou en plusieurs, si le chaînage de mappe a été utilisé pour créer la mappe. Si le mode par lots de l'enveloppeur est activé, les transactions qui arrivent au concentrateur dans une même enveloppe le quitteront également dans une même enveloppe. Cependant, s'il existe des points d'arrêt d'enveloppe (par exemple des valeurs différentes d'attribut EDI ou un profil d'enveloppe différent) ou si le traitement par lots est désactivé, les transactions repartiront dans plusieurs enveloppes. Voir «Enveloppeur», à la page 198 pour une description générale de l'enveloppeur (un composant qui rassemble plusieurs transactions destinées à un partenaire, les met dans une enveloppe et les envoie). Pour plus d'informations sur le traitement par lots, voir «Mode de traitement par lot», à la page 198.

Une mappe de validation peut également être associée à la transaction.

Flux EDI vers XML ou ROD

WebSphere Partner Gateway peut accepter un échange EDI émis par un partenaire ou le partenaire interne, le désenvelopper et transformer les transactions EDI obtenues en documents XML ou ROD.

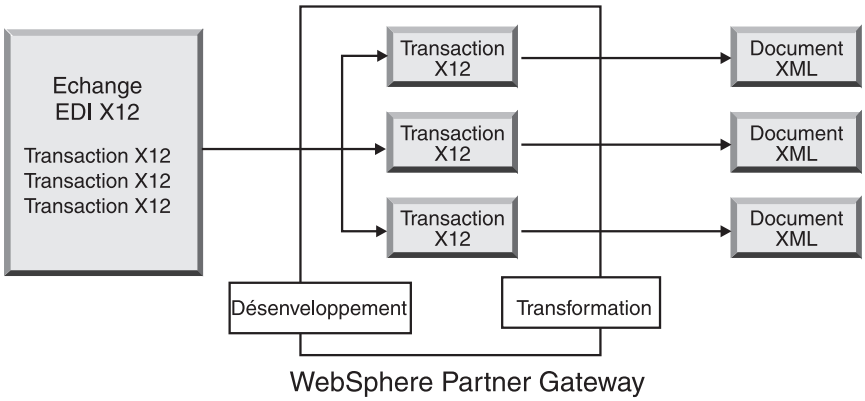


Figure 24. EDI vers un flux de documents XML

La transaction peut être convertie en un seul document ou, si le chaînage de mappes a été utilisé pour créer la mappe, en plusieurs documents.

Flux XML ou ROD vers EDI

WebSphere Partner Gateway peut recevoir des documents XML ou ROD émis par un partenaire ou le partenaire interne, les transformer en transactions EDI, envelopper les transactions et les envoyer au partenaire interne ou à un partenaire.

La figure 25, à la page 188 montre des documents XML transformés en transactions X12 puis enveloppés.

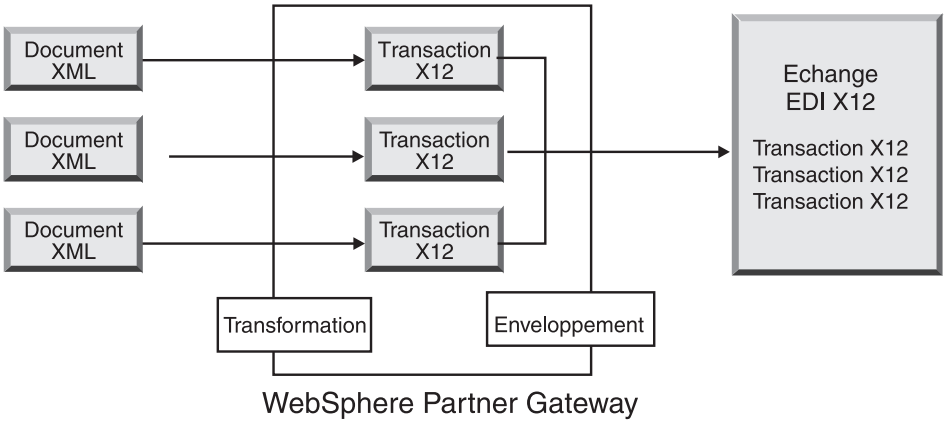


Figure 25. Flux de document XML en EDI

Un document peut être converti en plusieurs transactions (si le chaînage de mappes a été utilisé pour créer la mappe) et les transactions peuvent être enveloppées dans différents interchanges. La figure 26 montre un document XML transformé en trois transactions X12. Deux d'entre elles sont enveloppées ensemble. Celle restante est placée dans une enveloppe distincte.

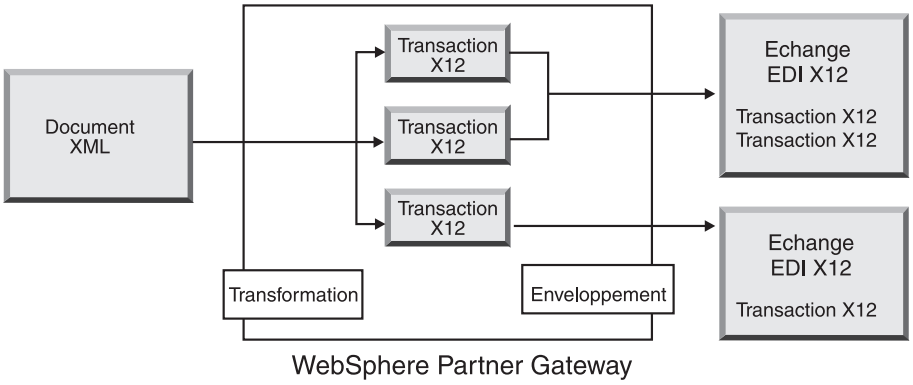


Figure 26. Flux de document XML vers plusieurs transactions EDI

Flux de plusieurs documents XML ou ROD vers EDI

WebSphere Partner Gateway peut recevoir un fichier composé d'un ou de plusieurs documents XML ou ROD de la part d'un partenaire ou du partenaire interne, le(s) transformer en transactions EDI, les placer dans plusieurs enveloppes et les envoyer au partenaire interne ou au partenaire.

Chaque document peut être transformé en une seule transaction ou en plusieurs, si le chaînage de mappe a été utilisé pour créer la mappe.

Remarques :

1. Les documents envoyés dans un fichier doivent être de même type (XML ou ROD) mais pas les deux à la fois.
2. Les documents ROD doivent être du même type.

La figure 27, à la page 189 montre le fractionnement d'un ensemble de documents XML pour obtenir des documents XML séparés. Les documents XML sont convertis en transactions X12 qui sont enveloppées.

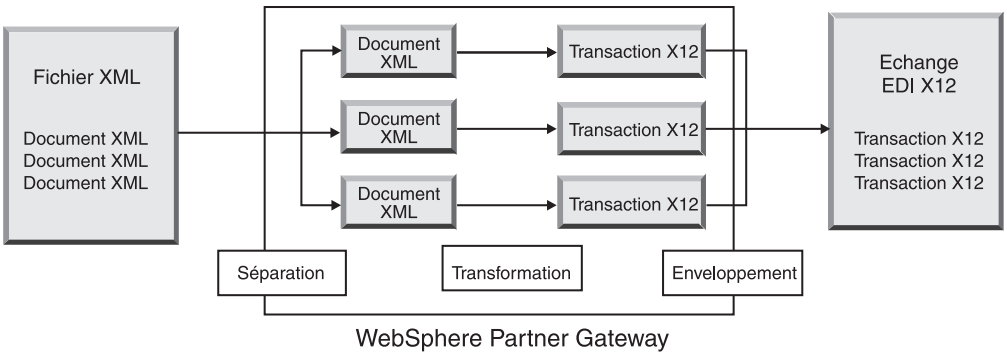


Figure 27. Flux de plusieurs documents XML vers un EDI

Dans la figure 27, les documents sont fractionnés (par le gestionnaire de fractionnement XML) et les transactions transformées sont enveloppées ensemble. Pour cela, le gestionnaire de l'utilitaire de fractionnement XML doit avoir l'option BCG_BATCHDOCS activée (la valeur on par défaut). Si BCG_BATCHDOCS est sur la valeur on et que le mode par lots de l'enveloppeur est également sur on, ces transactions pourront être enveloppées dans la même enveloppe d'EDI. L'attribut mode par lots de l'enveloppeur est décrit dans «Mode de traitement par lot», à la page 198.

Flux XML vers ROD ou ROD vers XML

WebSphere Partner Gateway peut recevoir un document XML ou ROD d'un partenaire ou du partenaire interne, le transformer en tout autre type de document (XML vers ROD ou ROD vers XML), puis l'envoyer au partenaire ou au partenaire interne.

La figure 28 montre plusieurs documents XML transformés en documents ROD.

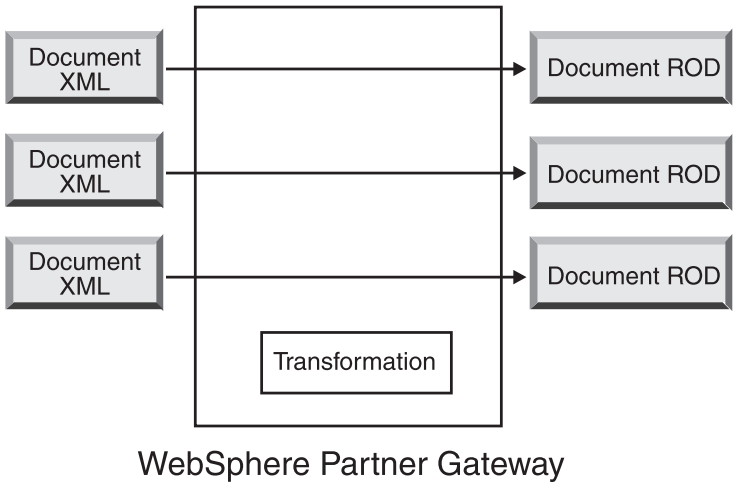


Figure 28. Flux de document XML en document ROD

Le document peut être transformé en un seul document ou en plusieurs si le chaînage de mappe a été utilisé pour créer la mappe.

Flux XML vers XML ou ROD vers ROD

WebSphere Partner Gateway peut recevoir un document XML ou ROD d'un partenaire ou du partenaire interne, le transformer en document de même type (XML vers XML ou ROD vers ROD), puis l'envoyer au partenaire ou au partenaire interne.

La figure 29 montre des documents XML transformés en documents XML de format différent.

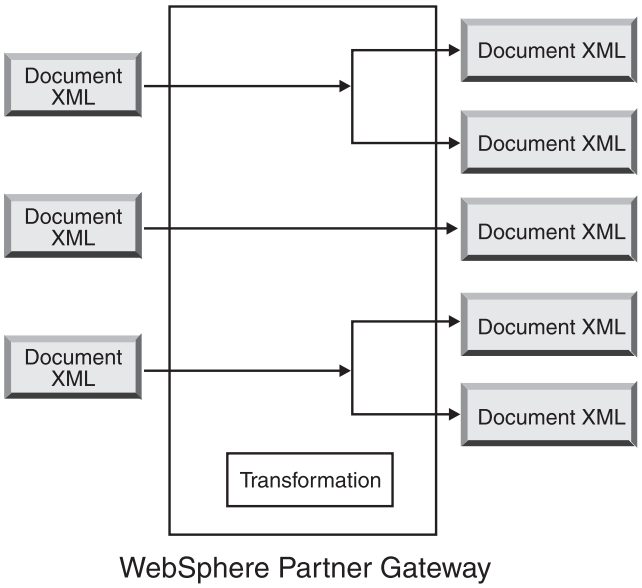


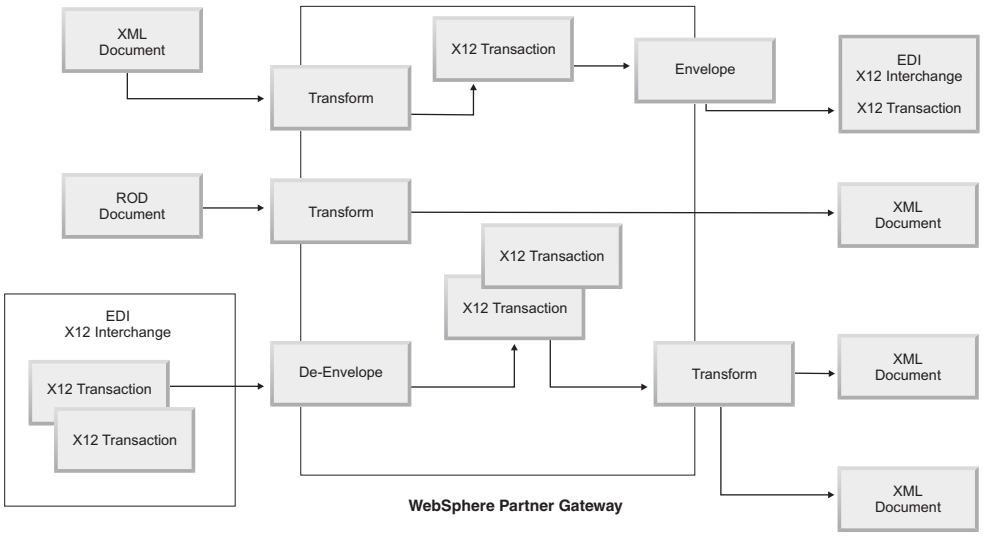
Figure 29. Flux de document XML en document XML

Le document peut être transformé en un seul document ou en plusieurs si le chaînage de mappe a été utilisé pour créer la mappe.

Flux Any vers Any

WTX vous permet de transformer un format Any vers Any. WTX design studio sert à créer des mappes. Les différents flux possibles sont ROD vers Any, XML vers Any et EDI vers Any. Quel que soit le flux requis, configurez l'utilitaire de fractionnement pour séparer les documents. Si ROD est le document source, les informations d'acheminement doivent également être définies. Si XML est le document source, ces dernières sont fournies. Les différentes actions possibles avec les différents flux sont les suivantes :

- ROD vers Any - transformation WTX
- XML vers Any - transformation WTX
- EDI vers Any - désenveloppement EDI si vous voulez désenvelopper l'échange de données dans les transactions. Les actions Réenveloppeur EDI et transformation WTX sont utilisées pour réenvelopper les transactions et les faire passer au format EDI - Any. L'action Validation EDI est utilisée si les transactions doivent être validées. Si vous voulez valider l'échange de données sans désenveloppement, utilisez Validation d'échange EDI.



Présentation des moteurs de transformation

WebSphere Partner Gateway prend en charge deux moteurs de transformation différents : WDI natif et WTX.

WDI natif- Des mappes de transformation sont créées dans le client DIS. Les différentes actions possibles fournies par WebSphere Partner Gateway pour l'intégration avec WDI sont Désenveloppement EDI, Translation EDI, Validation EDI, Réenveloppement EDI, Enveloppement EDI, Translation ROD et translation XML. Aucune configuration séparée n'est requise puisqu'il s'agit de WDI natif.

WTX - Des mappes de transformation sont créées à l'aide de WTX design studio. Les différentes actions possibles fournies par WebSphere Partner Gateway pour l'intégration avec WTX sont Transformation WTX, Validation d'échange EDI, Désenveloppement EDI, Validation EDI, Réenveloppement EDI et Enveloppement EDI. Deux approches sont possibles pour WTX : RMI et l'approche native. RMI est recommandée au cas où WTX n'est pas installé sur la même machine que WebSphere Partner Gateway. La procédure pour appeler WTX à distance est la suivante :

1. Dans le répertoire DTXHome, ouvrez le fichier rmiserver.properties et changer les propriétés. Vous pouvez par exemple définir le numéro de port.
2. A partir de ce même répertoire, exécutez startrmiserver.bat.
3. Dans les propriétés de la console, indiquez le nom d'hôte (où le serveur RMI est exécuté) et le numéro de port. Attribuez la valeur Oui à l'option de serveur RMI
4. Indiquez l'emplacement physique de la mappe.

Pour l'approche native, définissez le chemin du système en tant que répertoire de base WTX. Définissez également la propriété No pour rmiuseserver.

Transactions d'enveloppe depuis le système dorsal

Lorsque WTX est utilisé en mode asynchrone, l'application dorsale consomme les transactions EDI générées par WTX et les transfère à WebSphere Partner Gateway pour les envelopper selon le standard de conditionnement dorsal. Les en-têtes dorsaux par défaut sont utilisés pour indiquer les caractéristiques d'une transaction

(x-aux-senderid, x-aux-receiverid, x-aux-protocol, x-aux-protocol-version, x-aux-process-type, x-aux-process-version, et x-aux-docSyntax). Les en-têtes de package dorsaux contiendront les informations sur EDI-Dictionary/Protocol (par exemple X12v4R1), Docsyntax (EDI_transaction) et traiteront les informations de la transaction (par exemple 850) selon les en-têtes indiqués ci-dessus. Reportez-vous à la section sur l'action Enveloppe WTX.

Traitement des échanges EDI

Un EDI reçu au niveau du concentrateur est généralement désenveloppé avant que chaque transaction individuelle ne soit traitée. Souvent, des transactions EDI standard (telles que X12 850 ou EDIFACT ORDERS, qui représentent un ordre d'achat) sont transformées de façon à pouvoir être comprises par une application dorsale. De plus, un accusé de réception fonctionnel est souvent envoyé au partenaire pour indiquer que l'EDI a été reçu. Par conséquent, l'échange d'EDI exige plusieurs actions (désenveloppement, transformation, validation, enveloppement, échange de validation et réenveloppement EDI, transformation et enveloppe WTX). Par exemple, si l'EDI contient deux transactions et si aucun accusé de réception n'est requis, WebSphere Partner Gateway exécute les opérations suivantes :

1. Il désenveloppe l'EDI.

   WebSphere Partner Gateway extrait les informations relatives à l'EDI à partir des segments d'en-tête et de fin de l'enveloppe aux niveaux de l'EDI, du groupe et de la transaction. Ces informations peuvent comprendre :

   - Au niveau de l'EDI, les identificateurs entreprise des partenaires émetteurs et récepteurs, l'indicateur d'utilisation qui précise si l'EDI est destiné à un environnement de production ou de test et la date et l'heure auxquelles il a été préparé
   - Au niveau du groupe, les identificateurs d'application de l'émetteur et du récepteur et la date et l'heure de préparation du groupe
   - Au niveau de la transaction, le type de transaction (tel que X12 850 ou EDIFACT ORDERS)
   - Si une validation est requise pour les transactions individuelles, l'EDI est désenveloppé. Une fois la validation effectuée, les transactions validées sont enveloppées et envoyées au moteur de transformation (WDI ou WTX pour traitement) ou à la destination en fonction de l'action.
2. Il transforme la première transaction en fonction de la mappe qui lui est associée.
3. Il transforme la seconde transaction en fonction de la mappe qui lui est associée.
4. Il fournit les documents transformés à l'application dorsale.

De même, lorsque le concentrateur envoie un ou plusieurs documents émis par l'application dorsale du partenaire interne, les documents sont transformés en transactions EDI standard. Les transactions EDI obtenues sont enveloppées avant d'être envoyées au partenaire. Comme pour la réception, plusieurs actions sont nécessaires pour créer, envelopper et envoyer un EDI.

Les transactions individuelles, groupes et EDI sont identifiés par des numéros de contrôle. WebSphere Partner Gateway détermine ces numéros lorsqu'un échange a lieu. Toutefois, vous pouvez personnaliser les numéros de contrôle de la façon décrite dans la section «Numéros de contrôle», à la page 206.

L'illustration qui suit montre comment un échange EDI, empaqueté en tant que AS, est envoyé depuis un partenaire avec pour objectif de fournir deux documents XML transformés à deux destinations différentes sur le système dorsal du partenaire interne. Dans cet exemple, les transactions 850 sont transformées en ordres d'achat qu'une application dorsale peut traiter. Les transactions 890 sont transformées en ordres d'expédition d'entrepôt, que l'application dorsale peut traiter.

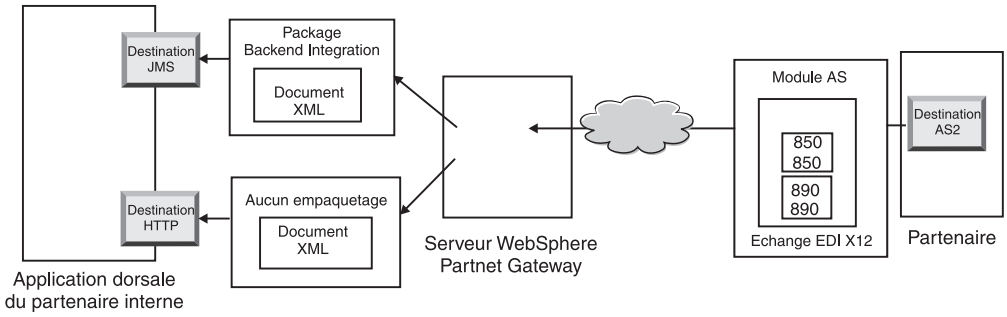


Figure 30. Flux général depuis un partenaire vers le partenaire interne

Au lieu d'une seule connexion entre le partenaire et le partenaire interne, cet échange demande trois connexions :

- Une du partenaire au concentrateur pour désenvelopper l'échange. Comme il s'agit d'une étape intermédiaire (l'échange est désenveloppé, mais n'est pas livré au partenaire), le côté cible de la connexion du partenaire est N/A (non applicable).

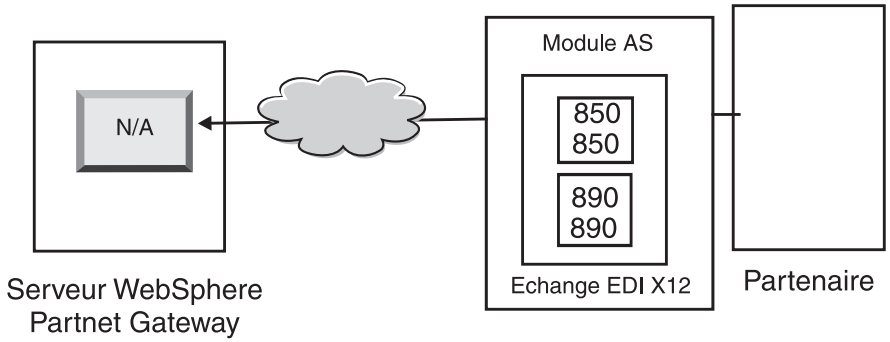


Figure 31. La connexion de désenveloppement

- Une pour la première transaction à transformer et à fournir à la destination JMS et au partenaire interne, et une pour la seconde transaction à transformer et à envoyer à la destination HTTP du partenaire interne.

  Pour les transactions, le package source est N/A, car elles sont arrivées par l'EDI original, qui a été désenveloppé par le système. Par conséquent, le côté source des transactions doit être indiqué **Package : N/A** dans la connexion du partenaire.

Pour la transaction qui est transformée en langage XML et qui va circuler vers l'application dorsale via le JMS, la destination cible sur la connexion du partenaire de cette transaction doit être définie comme la destination JMS du partenaire interne. Pour la transaction qui est transformée en langage XML et qui va circuler vers l'application dorsale via HTTP, la destination cible sur la connexion du partenaire de cette transaction doit être définie comme la destination HTTP.

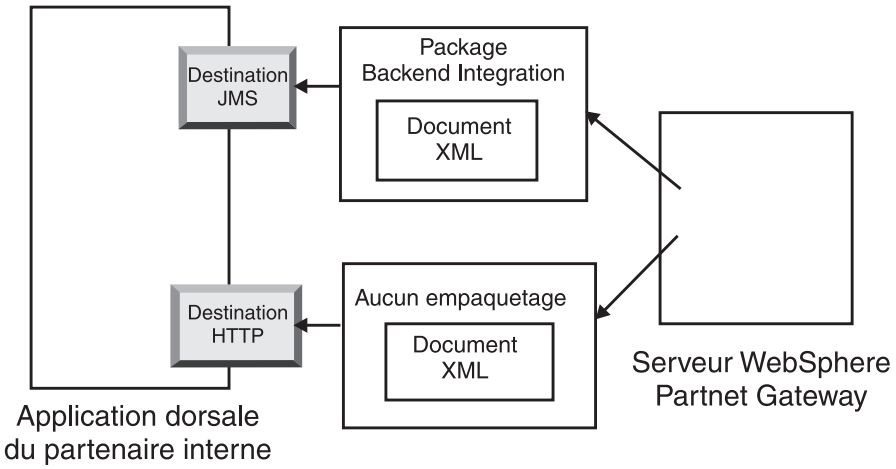


Figure 32. Connexions des transactions individuelles

Pour visualiser l'EDI et ses transactions, vous pouvez utiliser l'Afficheur de documents. Pour ce logiciel, les transactions sont les *enfants* de l'EDI. L'Afficheur de documents vos permet d'afficher les enfants d'un EDI source ou cible, ainsi que les événements associés. L'afficheur de documents est décrit dans la section "Affichage des événements et des documents" du *Guide d'administration de WebSphere Partner Gateway*.

Si l'émetteur exige des accusés de réception, vous devez mettre en place d'autres connexions :

- Une pour chaque accusé de réception renvoyé au partenaire. Les accusés de réception fonctionnels sont générés par le système. Par conséquent, le côté source de la connexion du partenaire doit être indiqué comme **Package : N/A**. Les accusés de réception fonctionnels sont enveloppés avant d'être livrés. Par conséquent, le côté cible de la connexion du partenaire doit également être indiqué comme **Package : N/A**. L'enveloppeur rassemble les accusés de réception votre définition. Voir «Enveloppeur», à la page 198 pour plus d'informations sur la configuration du programme.
- Une pour envelopper les accusés de réception avant qu'ils ne soient renvoyés au partenaire. L'enveloppe est générée par le système. Par conséquent, le côté source de la connexion du partenaire doit être indiqué comme **Package : N/A**. Le côté cible de la connexion du partenaire doit avoir la destination cible définie en tant que destination du partenaire et, dans ce cas, avec **Package : AS**. Vous pouvez soit utiliser une enveloppe par défaut pour le standard EDI, soit personnaliser des enveloppes. Voir « Profils d'enveloppe», à la page 199 pour plus d'informations sur la personnalisation des enveloppes.

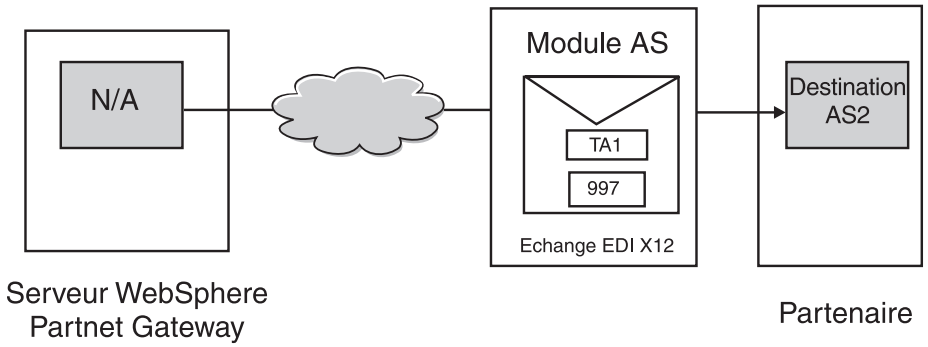


Figure 33. Enveloppement et envoi d'accusés de réception à l'émetteur

Transformation synchrone

WTX offre une fonction de transformation de format Any en format Any à l'aide d'une seule mappe. Une fonction d'appel est également fournie pour appeler directement l'API WTX pour la transformation. La transaction désenveloppée et validée est envoyée à WTX pour traitement après enveloppement.

Remarque : Voir «Présentation d'EDI», à la page 179 pour plus d'informations sur les différents formats EDI disponibles.

Une sortie - l'attribut de réacheminement détermine si le document de sortie doit être réintroduit dans le flux de travaux ou envoyé directement au flux de travaux sortant pour traitement.

Plusieurs sorties - reposant sur l'option de réacheminement, l'enfant sera directement transmis au flux de travaux sortant ou redirigé dans le flux de travaux entrant fixe pour passer dans un nouveau canal.

Transformation asynchrone

Lorsqu'un partenaire interne envoie un message à un partenaire externe de manière asynchrone, ce dernier peut utiliser WESB/WMB ou WTX pour la transformation. Aucune configuration n'est nécessaire car WTX est considéré comme une destination JMS. WTX envoie le document au système dorsal après le traitement et il n'y a aucun retour de flux d'informations vers WebSphere Partner Gateway. Le document EDI sera marqué comme Envoyé après livraison à la passerelle JMS.

Traitement des documents XML ou ROD

Un document XML ou ROD est reçu au niveau du concentrateur en tant que document individuel ou en tant que groupe de documents dans le même fichier. Dans ce dernier cas, WebSphere Partner Gateway procède comme suit :

1. Il fractionne l'ensemble de documents en documents individuels.
2. Il transforme chaque document en fonction de la mappe qui lui est associée.
3. Si les documents sont transformés en transactions EDI, il enveloppe les transactions et les transmet à l'application dorsale. Si les documents sont transformés en documents XML ou ROD, il les fournit à l'application dorsale.

Si le document XML ou ROD arrive en tant que document unique, WebSphere Partner Gateway procède comme suit :

1. Il transforme le document en fonction de la mappe qui lui est associée.
2. Si le document est transformé en transaction EDI, WebSphere Partner Gateway l'enveloppe et l'envoie à l'application dorsale. Si le document est transformé en un autre document XML ou ROD, il est livré à l'application dorsale.

De même, lorsque le concentrateur envoie un ou plusieurs documents émis par l'application dorsale du partenaire interne, ils sont transformés en documents XML ou ROD ou en transactions EDI. Ces dernières sont enveloppées avant d'être envoyées au partenaire. Comme pour la réception d'un EDI, plusieurs actions sont nécessaires pour transformer le ou les documents, envelopper les transactions obtenues et envoyer l'EDI.

Enveloppement d'intégration WTX et mappe polymorphe

Dans WebSphere Partner Gateway, une arborescence des types de métadonnées est définie. Vous pouvez configurer et donner des informations sur le type de données dans chacune des cartes. De manière générale, les propriétés sont sensées être configurées. Les noms et les valeurs des propriétés sont sensibles à la casse. Seules les valeurs booléennes ne le sont pas.

Tableau 27. Propriétés de l'arborescence des types de métadonnées

Nom de la propriété	Valeur	Description
BCG_DOCSYNTAX	EDI_INTERCHANGE EDI_TRANSACTION XML ROD	EDI_INTERCHANGE doit être définie si la sortie est un EDI enveloppé. EDI_TRANSACTION doit être définie si la sortie est une transaction EDI et n'est pas enveloppée. XML et ROD doivent être définie pour les sorties XML et ROD en conséquence.
BCG_REENVELOPE	vrai/faux	Si la valeur est vraie et que BCG_DOCSYNTAX a la valeur EDI_INTERCHANGE, l'enveloppe EDI sera désenveloppée. Après désenveloppement, chaque transaction produite sera considérée comme un document séparé au cours des étapes suivantes.
BCG_REROUTE	vrai/faux	Si la valeur est vrai, le document sera redirigé. Si la valeur est faux et que la sortie est unique, le BDO existant sera mis à jour avec le nouveau fichier et envoyé.
ProtocolName	Selon les besoins	Le nom du protocole du document de sortie. Il est obligatoire lorsque ReRoute a la valeur vrai. Vous l'utiliserez pour sélectionner le canal pour le document réacheminé.
ProtocolVersion	Selon les besoins	La version du protocole du document de sortie. Elle est obligatoire lorsque ReRoute a la valeur vrai. Vous l'utiliserez pour sélectionner le canal pour le document réacheminé.
ProcessCode	Selon les besoins	Le code de processus du document de sortie. Elle est obligatoire lorsque ReRoute a la valeur vrai. Vous l'utiliserez pour sélectionner le canal pour le document réacheminé.

Tableau 27. Propriétés de l'arborescence des types de métadonnées (suite)

Nom de la propriété	Valeur	Description
ProcessVersion	Selon les besoins	La version du processus du document de sortie. Elle est obligatoire lorsque ReRoute a la valeur vrai. Vous l'utiliserez pour sélectionner le canal pour le document réacheminé.
SegmentCountElementName	SE01/UNT01	Si la sortie est EDI_TRANSACTION, cet attribut doit être spécifié. Il doit être défini en fonction du type d'enveloppement souhaité.
SegmentCount	Selon les besoins	Si la sortie est EDI_TRANSACTION, cet attribut doit être spécifié. Il comportera les informations sur le nombre de segments dans la transaction.

Si la cible est EDI après transformation, il doit être enveloppé avant son envoi aux partenaires externes. Le document de sortie transformé peut avoir n'importe quelle combinaison de formats. Cela dépend des éléments codés dans le numéro de carte de la carte des métadonnées. Les propriétés des caractéristiques des autres cartes seront également contenues. Le créateur de la mappe devra coder la carte. Les différents attributs pris en compte sont ReRoute, ReEnvelope et DocSyntax. ReRoute et ReEnvelope peuvent avoir pour valeur Vrai ou Faux et DocSyntax peut avoir n'importe quelle valeur saisie par l'utilisateur. Si cette valeur est ediInchg, il sera pris en compte pour désenveloppement. Vous trouverez ci-dessous les résultats possibles des différentes combinaisons des valeurs de ReRoute et de ReEnvelope. On suppose que docSyntax est défini sur EDI_INTERCHANGE :

- ReRoute = Vrai, ReEnvelope = Faux : le document est traité comme tout autre document (XML ou ROD).
- ReRoute = Faux, ReEnvelope = Faux : le document est traité comme tout autre document (XML ou ROD).
- Reroute = Vrai, ReEnvelope = Vrai : le document est d'abord désenveloppé. Pour chaque transaction enfant, un bdo enfant est créé. Le dictionnaire et le document sont définis en tant que protocole et processus. Chaque BDO enfant (transaction) est réacheminé avec un conditionnement N/A. Un canal approprié doit être présent. Le profil de l'enveloppeur peut être configuré dans les attributs cibles de ce canal. Il faut également créer un canal pour l'enveloppe.
- Reroute = Faux, Reenvelope = Vrai : le document est d'abord désenveloppé. Si une transaction unique est produite, le document métier est mis à jour avec le fichier de transaction en tant qu'emplacement et envoyé. Si plusieurs transactions sont produites, des BDO enfant sont créés pour pour qu'il n'y ait pas de réacheminement et sont envoyés. L'attribut cible de ce canal doit être configuré en conséquence pour le profile de l'enveloppeur. Il doit y avoir un canal pour ce dernier.

Configuration de l'environnement EDI

Comme indiqué dans la précédente section, vous pouvez préciser de nombreux attributs portant sur l'échange d'EDI. Par exemple, vous pouvez modifier les profils d'enveloppe fournis par le produit, définir des enveloppes spécifiques à utiliser pour certaines connexions, déterminer les numéros de contrôle affectés aux diverses parties d'un EDI et configurer des profils de connexion pour que le même EDI puisse être livré de façons différentes. Ces tâches sont décrites dans la présente section.

Enveloppeur

L'enveloppeur est le composant qui rassemble un groupe de transactions à envoyer à un partenaire, les place dans une enveloppe et les envoie. Planifiez l'enveloppeur (ou acceptez la planification par défaut) pour indiquer à WebSphere Partner Gateway quand vous souhaitez que l'enveloppeur recherche les transactions qui attendent d'être envoyées. Vous pouvez également mettre à jour les valeurs par défaut de la durée de verrouillage, la durée de la file d'attente et du mode de traitement par lot.

Remarque : La configuration de l'enveloppeur est facultative. Si vous ne faites pas de modification, les valeurs par défaut fournies par le produit sont utilisées.

Verrouillage

Chaque instance du gestionnaire de documents possède son propre enveloppeur. Si deux gestionnaires de documents sont installés sur le système, vous disposez de deux enveloppeurs. Deux instances (ou plus) d'enveloppeurs peuvent donc tenter d'interroger des transactions qui attendent d'être enveloppées. Pour s'assurer qu'une transaction sera interrogée par un seul enveloppeur, il est fait usage de verrous. Ces verrous assurent que s'il existe plus d'un enveloppeur, un seul d'entre eux pourra interroger et traiter une transaction donnée. Les enveloppeurs interrogent simultanément, mais travaillent sur des transactions différentes.

Le verrou reçoit un limite de validité. La durée par défaut pendant laquelle un enveloppeur peut maintenir le verrou est de 240 secondes.

Si l'enveloppeur doit attendre le verrou, il est mis en file d'attente. La durée d'attente maximale dans la file (durée d'attente de l'enveloppeur) est de 740 secondes.

En règle générale, vous n'aurez pas besoin de modifier ces valeurs par défaut.

Mode de traitement par lot

Si plusieurs documents arrivent dans un même fichier, ils peuvent être fractionnés, selon la définition de l'utilitaire de fractionnement que vous avez faite pour ce type de document. (La configuration des gestionnaires de fractionnement fait partie de la définition des cibles. Elle est décrite dans « Modification des points de configuration», à la page 80.) BCG_BATCHDOCS est l'un des attributs du gestionnaire fractionnement. Lorsque BCG_BATCHDOCS est activé (on), l'utilitaire de fractionnement ajoute des ID de traitement aux documents après les avoir séparés.

L'enveloppeur dispose d'un attribut pour le mode de traitement par lots, qui est associé à l'attribut BCG_BATCHDOCS. Si des ID de traitement par lots ont été attribués aux documents individuels et si vous acceptez la valeur par défaut du mode de traitement par lots, l'enveloppeur s'assure que tous les documents qui arrivent ensemble dans le même fichier sont traités avant d'être enveloppés et envoyés. Vous êtes donc sûr que les transactions seront enveloppées ensemble. Par exemple, supposons que cinq documents XML arrivent dans le même fichier. Ils doivent être transformés en transactions EDI et livrés au même destinataire. Lorsque trois des documents ont été transformés, l'enveloppeur commence son interrogation planifiée des transactions. Si le mode de traitement par lot est sélectionné, l'enveloppeur ne traite (enveloppe) pas les trois transactions qui sont prêtes. Il attend que le traitement des cinq transactions soit terminé avant de les envelopper et de les envoyer. Elles sont placées dans la même enveloppe, à moins que le standard EDI applicable ne l'interdise.

Modification des valeurs par défaut
Pourquoi et quand exécuter cette tâche

Pour modifier les valeurs par défaut de l'enveloppeur, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Enveloppeur**.
2. Cliquez sur l'icône **Edition**.
3. Entrez de nouvelles valeurs pour **Délai maximal de verrouillage (secondes)** et **Délai maximal des files d'attente (secondes)** si vous souhaitez modifier la durée affectée à ces attributs.

   Remarque : En règle générale, vous n'aurez pas besoin de modifier ces valeurs par défaut.
4. Pour désactiver le mode de traitement par lot, décochez la case en regard de **Utiliser le mode de traitement par lot**
5. Pour modifier la fréquence à laquelle l'enveloppeur contrôle les transactions en attente d'envoi, effectuez l'une des procédures suivantes :
   - Pour utiliser la planification en fonction d'un intervalle (qui est la valeur par défaut) tout en modifiant la durée, entrez une nouvelle valeur en regard de **Intervalle**. Par exemple, si vous remplacez la valeur par 30 secondes, l'enveloppeur contrôlera les documents toutes les 30 secondes, les enveloppera et les enverra au destinataire.
   - Pour utiliser la planification en fonction du calendrier, procédez comme suit :
     a. Cliquez sur **Planification en fonction du calendrier**.
     b. Choisissez le type de planification (**Planification quotidienne**, **Planification hebdomadaire** ou **Planification personnalisée**).
        - Si vous sélectionnez **Planification quotidienne**, choisissez l'heure de la journée (heure et minutes) à laquelle l'enveloppeur doit vérifier la présence de documents.
        - Si vous sélectionnez **Planification hebdomadaire**, choisissez un ou plusieurs jours de la semaine, en plus de l'heure.
        - Si vous sélectionnez **Planification personnalisée**, choisissez l'heure de la journée puis **Intervalle** ou **Sélection des jours** pour indiquer la semaine et le mois. Dans **Intervalle**, indiquez une date de début et de fin (par exemple, vous pouvez cliquer sur **Lun** et **Ven** si vous souhaitez que l'enveloppeur contrôle la présence de documents à heure donnée, uniquement les jours ouvrés). L'option **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.
6. Cliquez sur **Sauvegarder**.

Profils d'enveloppe

Un profil d'enveloppe détermine les valeurs placées dans des éléments spécifiques de l'enveloppe. Vous affectez le profil d'enveloppe à des transactions EDI dans l'attribut **Profil d'enveloppe** de définition de documents. WebSphere Partner Gateway fournit un profil d'enveloppe prédéfini pour chaque standard pris en charge (X12, EDIFACT ou UCS). Vous pouvez utiliser ces enveloppes prédéfinies directement, les modifier ou les copier dans de nouveaux profils d'enveloppe. Les étapes pour créer ou modifier un profil d'enveloppe sont indiquées à la section «Modification des valeurs par défaut», à la page 200.

Les profils d'Enveloppe contiennent une zone pour chaque élément du standard d'enveloppe. Ils fournissent des données littérales ou des constantes pour concevoir des segments d'en-tête ou de fin adaptés aux ensembles de transactions, messages, groupes fonctionnels et EDI. Précisez uniquement les informations nécessaires et pour lesquelles aucune valeur n'est fournie par d'autres sources.

Les noms de zones sont conçus pour faciliter les références croisées. Par exemple, la zone UNB03 est le troisième élément de données du segment UNB.

Comme indiqué dans la section « attributs d'enveloppe», les attributs configurés dans d'autres éléments sont prioritaires sur ceux qui ont été définis dans le profil d'enveloppe. Certains attributs peuvent être supplantés par les attributs et mappes liés à la définition de documents.

attributs d'enveloppe

Des attributs d'enveloppe peuvent être définis à plusieurs moments de la configuration de l'échange, ainsi que dans la mappe de transformation associée aux documents. Par exemple, le spécialiste de mappage du client Data Interchange Services peut définir la propriété CtlNumFlag lorsqu'il définit une mappe. Cette propriété peut également être configurée dans le profil d'enveloppe (dans la zone **Numéros de contrôle par ID de transaction**). Tout attribut défini dans la mappe de transformation supplante les valeurs configurées sur la console de communauté. Par exemple, si CtlNumFlag est défini sur **N** (non) dans la mappe de transformation et sur **Y** (oui) dans la zone **Numéros de contrôle par ID de transaction**, c'est la valeur **N** qui est utilisée.

D'autres profils d'enveloppe peuvent être définis au niveau du protocole (à partir de la page Gérer des définitions de documents ou de la page Fonctions B2B associée au partenaire) ou en tant que partie de la connexion. La liste ci-dessous précise les priorités :

1. Les propriétés définies dans la mappe de transformation sont prioritaires sur les attributs associés définis sur la console de communauté.
2. Les attributs définis au niveau de la connexion sont prioritaires sur ceux qui ont été configurés au niveau des fonctions business-to-business.
3. Les attributs définis au niveau des fonctions business-to-business sont prioritaires sur ceux qui ont été configurés au niveau de la définition de documents.
4. Tous les attributs définis ailleurs (dans la mappe de transformation ou dans la définition de documents, dans les fonctions business-to-business ou au niveau de la connexion) sont prioritaires sur les valeurs définies dans le profil de l'enveloppe.

Pour consulter la liste des propriétés de mappe de transformation et les attributs de console de communauté associés, voir «Propriétés du client Data Interchange Services», à la page 457.

Modification des valeurs par défaut

Pourquoi et quand exécuter cette tâche

La section « attributs de profil d'enveloppe», à la page 445 présente un tableau indiquant les valeurs par défaut utilisées pour chaque attribut d'enveloppe de standard EDI, si vous n'entrez pas de valeur dans le profil ou si vous ne créez pas de profil. Assurez-vous que les profils d'enveloppe que vous utilisez fournissent tous les éléments obligatoires qui ne sont pas fournis par le système lors de l'exécution.

Pour définir un profil d'enveloppe, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Profil d'enveloppe**.
2. Appliquez l'une des procédures suivantes :
   - Création d'une enveloppe
     a. Cliquez sur **Créer**.
     b. Tapez un nom pour le profil d'enveloppe. Il s'agit du nom qui apparaîtra dans la liste des profils d'enveloppe.
     c. Indiquez éventuellement une **Description** du profil.
     d. Cliquez sur le **Standard EDI** auquel l'enveloppe appartient. Par exemple, si vous échangez des documents conformes au standard EDI-X12, sélectionnez **X12**.
   - Modification d'une enveloppe
     a. Sélectionnez un des profils d'enveloppe existants en cliquant sur l'icône **Afficher les détails** en regard du nom du profil.
     b. Cliquez sur l'icône **Edition**.
3. Le bouton **Général** est sélectionné par défaut. Vous pouvez indiquer une valeur dans toutes les zones sauf ENVTYPE, qui contient déjà le standard choisi à l'étape 2d.

   Vous pouvez ajouter des valeurs dans les zones suivantes :
   - **Longueur du numéro de contrôle EDI**, pour indiquer le nombre de caractères à utiliser lorsqu'un numéro de contrôle est affecté à un EDI contenu dans l'enveloppe.
   - **Longueur du numéro de contrôle de groupe**, pour indiquer le nombre de caractères à utiliser lorsqu'un numéro de contrôle est affecté à un groupe de l'enveloppe.
   - **Longueur du numéro de contrôle de la transaction**, pour indiquer le nombre de caractères à utiliser lorsqu'un numéro de contrôle est affecté à une transaction de l'enveloppe.
   - **Nombre maximum de transactions**, pour indiquer le nombre maximum de transactions autorisées dans cette enveloppe.
   - **Numéros de contrôle par ID de transaction**, pour indiquer si vous souhaitez utiliser l'ID de transaction (comme partie de la clé) lorsque les numéros définis sont recherchés dans la base de données. Si c'est le cas, des ensembles différents de numéros de contrôle sont utilisés pour chaque ID de transaction.

   Les zones du profil général d'enveloppe sont les mêmes pour les trois standards, sauf pour EDIFACT qui compte une zone supplémentaire : **Créer des groupes pour EDI**.

   Si vous avez apporté des modifications à la page Général, cliquez sur **Enregistrer**.
4. Pour préciser des valeurs de l'EDI, cliquez sur **EDI**. Un nouvel ensemble de zones s'affiche sur la page. Les zones dépendent du standard EDI. Notez que certaines valeurs sont déjà renseignées, ou le seront à l'exécution.
   - Pour le standard EDI-X12, vous pouvez modifier les zones suivantes :
     – **ISA01 : Qualificatif d'informations d'autorisation**, un code pour le type d'information dans ISA02.
     – **ISA02 : Informations d'autorisation**, les informations utilisées pour identifier plus avant ou autoriser l'expéditeur des données d'EDI.

- **ISA03 : Qualificatif d'informations de sécurité**, un code pour le type d'information dans ISA04. Les valeurs autorisées sont :

  00 ISA04 n'a pas de signification

  01 ISA04 contient un mot de passe
- **ISA04 : Information de sécurité**, les informations de sécurité concernant l'émetteur des données de l'EDI. Le code contenu par ISA03 définit le type de l'information.
- **ISA11 : ID des standards EDI**, un code pour l'agence qui contrôle l'EDI. Les valeurs autorisées sont : **U** (communauté EDI des US pour ASC X12), **TDCC** et **UCS**.

  Remarque : Cet attribut est utilisé jusqu'à la version 4010 de X12. Dans X12 4020, l'élément ISA11 sert de séparateur de répétition.
- **ISA12 : ID de version EDI**, qui est le numéro de version de la syntaxe utilisée dans les segments de contrôle de groupe fonctionnel et d'EDI.
- **ISA14 : Accusé de réception requis**, le code de l'émetteur pour demander un accusé de réception. Les valeurs autorisées sont :

  0 Pas de demande d'accusé de réception

  1 Demander la confirmation que les segments ISA et IEA ont été reçus et reconnus
- **ISA15 : Indicateur de test**, qui indique si l'EDI est destiné aux tests ou à la production. Les valeurs autorisées sont :

  T Pour données de test

  P Pour données de production

- Pour le standard UCS, vous pouvez modifier les zones suivantes :
  - **BG01 : ID de communications**, l'identification de la société émettrice.
  - **BG02 : Mot de passe de communications**, qui est le Mot de passe affecté par le récepteur, à utiliser de la façon convenue entre les partenaires.
- Pour le standard EDIFACT, vous pouvez modifier les zones suivantes :
  - **UNB0101 : ID de syntaxe**, qui est l'identification de l'agence chargée du contrôle de la syntaxe utilisée. Il s'agit de l'agence UNO. Le niveau est A ou B.
  - **UNB0102 : Version de la syntaxe**, le numéro de version de la syntaxe identifiée par l'ID de syntaxe.
  - **UNB0601 : Référence/mot de passe des destinataires**, qui est le Mot de passe affecté par le destinataire, à utiliser de la façon convenue entre les partenaires.
  - **UNB0602 : Référence des destinataires/qualificatif de mot de passe**, qui est un qualificatif du Mot de passe du destinataire, à utiliser de la façon convenue entre les partenaires.
  - **UNB07 : Référence de l'application**, qui est l'identification par l'émetteur de la zone fonctionnelle concernée par les messages EDI.
  - **UNB08 : Priorité**, qui est Le code de l'émetteur définissant la priorité de traitement, comme convenu avec le partenaire. Le Code A est la priorité la plus élevée.
  - **UNB09 : Demande d'accusé de réception**, qui est le code de l'émetteur pour demander un accusé de réception.
  - **UNB10 : ID d'accord de communications**, qui est le nom ou code du type d'accord utilisé pour cet échange, comme convenu avec le partenaire.

- **UNB11 : Indicateur de test (indicateur d'utilisation)**, qui indique si l'EDI est destinée aux tests. La valeur 1 indique un EDI de test.

Si vous avez apporté des modifications à la page EDI, cliquez sur **Enregistrer**.

5. Pour préciser des valeurs pour les groupes, cliquez sur **Groupe**. Un nouvel ensemble de zones s'affiche. Les zones dépendent du standard EDI.

   Les zones de cette page définissent généralement l'émetteur et le récepteur du groupe.

   - Pour les standards EDI-X12 et UCS, vous pouvez compléter les zones suivantes :
     - **GS01 : ID de groupe fonctionnel**, qui identifie le type d'ensembles de transactions dans le groupe.
     - **GS02 : Emetteur de l'application**, qui est le nom ou code pour un département donné de l'entreprise de l'émetteur.
     - **GS03 : Récepteur de l'application**, qui est le nom ou le code du département de l'entreprise qui doit recevoir le groupe.
     - **GS07 : Agence du groupe**, qui est un code utilisé avec GS08 pour identifier l'agence qui contrôle le standard.
     - **GS08 : version du groupe**, qui est un code pour la version, l'édition et le secteur d'activité du standard.
   - Pour le standard EDIFACT, vous pouvez compléter les zones suivantes :
     - **UNG01 : ID de groupe fonctionnel**, qui identifie le type de messages dans le groupe.
     - **UNG0201 : ID de l'émetteur de l'application**, qui est le nom ou code pour un département donné de l'entreprise de l'émetteur.
     - **UNG0202 : Qualificatif de l'ID de l'émetteur de l'application**, qui est le qualificatif du code d'ID de l'émetteur. Vous trouverez une liste des qualificatifs de code dans le répertoire de l'élément de données.
     - **UNG0301 : ID du récepteur de l'application**, qui est le nom ou le code du département de l'entreprise qui doit recevoir le groupe.
     - **UNG0302 : Qualificatif de l'ID de récepteur de l'application**, qui est le qualificatif du code d'ID de récepteur. Vous trouverez une liste des qualificatifs de code dans le répertoire de l'élément de données.
     - **UNG06 : Agence de contrôle**, le code qui identifie l'agence qui contrôle le type du message dans le groupe fonctionnel.
     - **UNG0701 : Version du message**, le numéro de version du type de message.
     - **UNG0702 : Edition du message**, le numéro d'édition dans le numéro de version pour le type de message.
     - **UNG0703 : Affecté par l'association**, le code attribué par l'association responsable, qui identifie le type de message.
     - **UNG08 : Mot de passe de l'application**, le mot de passe attribué au département concerné dans l'entreprise du récepteur.

   Si vous avez apporté des modifications à la page Groupe, cliquez sur **Enregistrer**.

6. Pour indiquer des valeurs pour les transactions d'un groupe, cliquez sur **Transaction**. Dans le cas d'EDIFACT, cliquez sur **Message**. Un nouvel ensemble de zones s'affiche. Les zones dépendent du standard EDI.

   - Pour le standard EDI-X12 ou USC, vous pouvez entrer une valeur pour **ST03 : Chaîne d'ID de convention d'implémentation**.
   - Pour le standard EDIFACT, vous pouvez compléter les zones suivantes :

- **UNH0201 : Type de message**, un code attribué par l'agence de contrôle pour identifier le type de message.
- **UNH0202 : Version du message**, le numéro de version du type de message.
- **UNH0203 : Edition du message**, le numéro d'édition dans le numéro de version pour le type de message.
- **UNH0204 : Agence de contrôle**, le code qui identifie l'agence qui contrôle le type du message.
- **UNH0205 : Code affecté par l'association**, un code attribué par l'association responsable et qui identifie davantage le type de message.
- **UNH03 : Référence d'accès commun**, la clé qui relie tous les transferts de données suivants à un fichier commun. Les partenaires peuvent accepter d'utiliser une clé constituée de composants, mais il est impossible d'utiliser des séparateurs d'élément secondaire.

Si vous avez apporté des modifications à la page Transaction, cliquez sur **Enregistrer**.

7. Cliquez sur **Sauvegarder**.
8. Répétez les étapes 2, à la page 201 à 7 pour tous les autres profils d'enveloppe que vous souhaitez définir ou modifier.

Lorsqu'un profil d'enveloppe est défini, il s'ajoute à la liste des profils d'enveloppe. Vous pouvez y sélectionner le profil et cliquer sur l'icône **Cas d'emploi** pour déterminer les connexions qui utilisent le profil.

Profils de connexion

Vous utilisez les profils de connexion avec des transactions désenveloppées et avec des échanges EDI créés par l'enveloppeur. Pour les transactions, le profil de connexion détermine comment la transaction est traitée après avoir été désenveloppé. Pour les échanges, le profil de connexion détermine comment l'échange est fourni.

Utilisez la fenêtre Profils de connexion pour créer un profil ou éditer les informations d'un profil existant. Le nom des profils définis et leur description, si elle a été définie, figurent dans la Liste des profils de connexion. Voir le *Guide de configuration du concentrateur de WebSphere Partner Gateway* pour plus d'informations sur les profils de connexion.

Transactions

Lorsqu'un EDI arrive dans WebSphere Partner Gateway, la première opération consiste généralement à le désenvelopper en transactions individuelles. Lorsque les transactions sont créées, l'action de désenveloppement définit l'**Indicateur d'utilisation de l'EDI** et les informations de groupe (l'**Identificateur de l'émetteur d'application de groupe**, l'**Identificateur du récepteur d'application de groupe** et le **Mot de passe d'application de groupe**) dans les métadonnées de la transaction. Chaque transaction est ensuite à nouveau traitée par WebSphere Partner Gateway, dans son propre flux de travaux.

Prenons deux transactions de même type (par exemple 850) qui doivent être traitées différemment en fonction du groupe auquel elles appartenaient et des valeurs de leurs indicateurs d'utilisation EDI. Si l'**Indicateur d'utilisation** est Production (**P**), vous souhaiterez peut-être utiliser une mappe (A) et si l'**Indicateur d'utilisation** est Test (**T**), vous utiliserez une autre mappe (B). Deux connexions identiques sont requises pour cette transaction 850, la seule différence étant que l'une des connexions utilise la mappe A et l'autre la mappe B.

Les transactions étant identiques (mêmes partenaires source et cible, package, protocole et type de document), le gestionnaire de documents doit pouvoir déterminer laquelle utiliser. Il utilise pour cela l'attribut de profil de connexion que vous avez indiqué dans les métadonnées de la transaction. Dans cet exemple, si vous créez deux profils de connexion, l'un (CPProduction) avec le **Type de syntaxe EDI** défini sur **P** et l'autre (CPTest) sur **T**, le gestionnaire de documents fait correspondre la transaction dont l'identificateur de syntaxe est P avec le profil CPProduction. Il sait ensuite utiliser la mappe A pour convertir la transaction.

L'exemple de cette section utilise un attribut **Identificateur de syntaxe EDI**, mais vous pouvez également utiliser les attributs **Identificateur d'application d'émetteur de groupe**, **Identificateur d'application de récepteur de groupe** et **Mot de passe d'application de groupe** pour différencier les transactions.

Echanges

Pour les EDI, utilisez l'attribut **Qualificatif 1 de profil de connexion**.

Par exemple, supposons que votre société soit en train de migrer depuis un VAN (package None) ou Internet (package AS2). Vous souhaitez que les transactions 840 (Demande de devis) utilisent le VAN et les transactions 850 (Bon de commande) utilisent Internet. Vous configurez deux connexions de partenaires pour le même échange source mais avec deux cibles différentes (l'une pour le package None, l'autre pour le package AS2). Les profils de connexion aident à faire la distinction entre les deux connexions.

La configuration du profil de connexion des EDI s'effectue en plusieurs étapes. Voici comment procéder pour créer les deux profils de connexion de l'exemple :

1. Créez deux connexions pour les transactions. Définissez l'attribut **Qualificatif 1 de profil de connexion** sur "To" (Vers) pour les deux connexions. La valeur doit être significative (par exemple ConNone et ConAS2).
2. Définissez deux profils de connexion (par exemple CPNone et CPAS2), chacun avec la valeur **Qualificatif1** correspondant à celle des attributs **Qualificatif1 du profil de connexion** définis à l'étape 1 (ConNone et ConAS2).
3. Créez deux connexions pour l'EDI. Chaque connexion a le même package source (N/A) mais un package cible différent (None ou AS2). La connexion du partenaire avec le profil CPNone aura sa destination cible définie sur la destination de script FTP qui peut se connecter au VAN. La connexion du partenaire avec le profil CPAS2 aura son package cible défini sur AS.
4. Associez le profil de connexion adapté à chacun.

L'enveloppeur utilise l'attribut **Qualificatif 1 de profil de connexion** du côté "Destination" de la connexion du partenaire comme point d'arrêt d'enveloppe. Ainsi, les transactions qui ont des valeurs différentes pour l'attribut **Qualificatif 1 de profil de connexion** iront dans des enveloppes différentes. Lorsque vous indiquez des valeurs différentes pour les transactions, l'enveloppeur ne placera jamais les transactions 840 et 850 dans le même EDI.

Lorsque le gestionnaire de document recherche la connexion, il trouve les deux connexions possibles mais utilise celle dont le profil de connexion est approprié.

Configuration des profils de connexion
Pourquoi et quand exécuter cette tâche

La configuration des profils de connexion est facultative. Si vous n'avez pas besoin de plus d'une connexion pour chaque type de document échangé pour un partenaire, passez à la section suivante.

Pour configurer un profil de connexion :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Profil de connexion**.
2. Cliquez sur **Créer un profil de connexion**.
3. Sur la page Détails du profil de connexion, indiquez un nom pour ce profil de connexion.
4. Entrez éventuellement une description du profil.

   Le nom et la description (le cas échéant) apparaîtront sur la page Liste des profils de connexion.
5. Eventuellement, précisez une valeur du **Qualificatif 1** pour indiquer la connexion qui sera utilisée par l'EDI. Voir « Echanges», à la page 205 pour un exemple d'utilisation du **Qualificatif 1**.
6. Eventuellement, précisez une valeur du **Type d'utilisation EDI** pour indiquer s'il s'agit d'un échange de test, de production ou d'information. Voir « Transactions», à la page 204 pour un exemple d'utilisation du **Type d'utilisation EDI**.
7. Eventuellement, précisez un **ID de l'émetteur de l'application** pour indiquer l'application ou la division de l'entreprise associée à l'émetteur du groupe.
8. Eventuellement, précisez un **ID du récepteur de l'application** pour indiquer l'application ou la division de l'entreprise associée au récepteur du groupe.
9. Eventuellement, précisez un **Mot de passe**, si vous avez besoin d'en définir un entre l'émetteur de l'application et le récepteur.
10. Cliquez sur **Sauvegarder**.

Pour les transactions que vous voulez insérer dans certaines enveloppes d'échange, pour pouvez donner à l'attribut **Qualificatif 1 de profil de connexion** la valeur qui correspond au profil de connexion avec la même valeur pour l'attribut **Qualificatif 1**. L'attribut **Qualificatif 1 de profil de connexion** peut être défini au niveau protocole d'une définition de documents (vous pouvez par exemple modifier les attributs du protocole X12V5R1 dans la fenêtre Gestion des définitions de documents pour indiquer le profil de connexion à utiliser, en cliquant sur la valeur de l'attribut **Qualificatif 1 de profil de connexion** correspondant). Ensuite, lorsque vous activez la connexion EDI, associez le profil de connexion en cliquant sur le bouton **Profil de connexion** et en sélectionnant le profil dans la liste.

Numéros de contrôle

L'enveloppeur utilise des numéros de contrôle pour assurer la numérotation unique des EDI, groupes et transactions d'une enveloppe. Ces numéros sont établis pour le partenaire interne et les partenaires externes. Lors de l'échange de documents, des numéros de contrôle sont générés pour la *paire* de partenaires.

Pour chaque partenaire bénéficiant de fonctions business-to-business d'EDI correspond un ensemble de valeurs d'initialisation des numéros de contrôle. Ces valeurs sont utilisées la première fois qu'un EDI est créé et échangé entre une paire de partenaires. Les valeurs d'initialisation s'appliquent au partenaire auquel l'EDI

est envoyé. Lorsqu'un document a été envoyé d'un partenaire à un autre, les derniers numéros utilisés s'affichent sur la page Numéros de contrôle actuels. Pour une paire donnée de partenaires, il peut exister plusieurs entrées, si **Numéros de contrôle par ID de transaction** a la valeur **O**. Une fois qu'une entrée existe, elle sert à générer les nouveaux numéros de contrôle.

Dans le cadre de l'initialisation des numéros de contrôle, vous pouvez utiliser des masques pour modifier la création normale de numéros de contrôle par l'enveloppeur. Les masques servent à baser le numéro de contrôle sur le numéro de contrôle du groupe ou sur le numéro de l'EDI. Les masques sont décrits ci-dessous. Remplacez le *n* qui figure dans le masque d'édition par le nombre d'octets que vous souhaitez utiliser pour créer la valeur du numéro de contrôle. Consultez le tableau 28 pour une description des codes disponibles :

Tableau 28. Masques des numéros de contrôle

Code	Numéro de contrôle	Description
G	Transaction	Le numéro de contrôle de transaction est identique au numéro de contrôle de groupe. Une seule transaction est autorisée par groupe.
G*n*	Transaction	*n* octets sont extraits du numéro de contrôle de groupe. Le reste du numéro de contrôle de transaction est complété par des zéros jusqu'à la taille maximale. Une seule transaction est autorisée par groupe.
C	Groupe, transaction	Les octets restants de la zone du numéro de contrôle de transaction ou de groupe sont utilisés pour maintenir un numéro de contrôle pour ce partenaire.
V	Groupe, transaction	Une valeur incrémentale est utilisée. Le premier groupe ou la première transaction a la valeur 1, le deuxième la valeur 2, etc.
V*n*	Transaction	Une valeur incrémentale de *n* octets de long est utilisée. La première transaction a la valeur 1, la deuxième la valeur 2, etc.
G*n*C	Transaction	*n* octets sont extraits du numéro de contrôle de groupe, les octets restants de la zone du numéro de contrôle de transaction sont utilisés pour maintenir un numéro de contrôle. Le nombre de positions laissées détermine la valeur maximale du numéro de contrôle. Par exemple, G5C laisse quatre positions et la valeur maximale est 9999. Le numéro de contrôle repasse ensuite à 1.
G*n*V	Transaction	*n* octets sont extraits du numéro de contrôle de groupe. Pour les octets restants de la zone de numéro de contrôle de transaction, une valeur incrémentale est utilisée, de sorte que la première transaction a la valeur 1, la deuxième la valeur 2, etc.
G*n*V*m*	Transaction	*n* octets sont extraits du numéro de contrôle de groupe. Pour les octets restants, jusqu'à *m* octets de la zone du numéro de contrôle de transaction, une valeur incrémentale est utilisée, de sorte que la première transaction a la valeur 1, la deuxième la valeur 2, etc.

Tableau 28. Masques des numéros de contrôle (suite)

Code	Numéro de contrôle	Description
I	Groupe, transaction	Le numéro de contrôle de groupe ou de transaction doit être identique au numéro de contrôle de l'EDI. Un seul groupe est autorisé pour l'EDI et une seule transaction est autorisée pour le groupe ou l'EDI.
I*n*	Groupe, transaction	*n* octets sont extraits du numéro de contrôle de l'EDI. Le restant de la zone du numéro de contrôle de transaction ou de groupe est complété par des zéros jusqu'à sa taille maximale. Un seul groupe est autorisé pour chaque EDI et une seule transaction est autorisée pour chaque groupe.
I*n*C	Groupe, transaction	*n* octets sont extraits du numéro de contrôle de l'EDI. Les octets restants de la zone du numéro de contrôle de transaction sont utilisés pour maintenir un numéro de contrôle. Le nombre de positions laissées détermine la valeur maximale du numéro de contrôle. Par exemple, I5C laisse quatre positions et la valeur maximale est 9999. Le numéro de contrôle repasse ensuite à 1.
I*n*V	Groupe, transaction	*n* octets sont extraits du numéro de contrôle de l'EDI. Pour les octets restants de la zone de numéro de contrôle de transaction ou de groupe, une valeur incrémentale est utilisée, de sorte que le premier groupe ou transaction a la valeur 1, le deuxième la valeur 2, etc.
I*n*V*m*	Transaction	*n* octets sont extraits du numéro de contrôle de l'EDI. Pour les octets restants, jusqu'à *m* octets de la zone du numéro de contrôle de transaction, une valeur incrémentale est utilisée, de sorte que la première transaction a la valeur 1, la deuxième la valeur 2, etc.
I*n*G*m*	Transaction	*n* octets sont extraits du numéro de contrôle de l'EDI et un maximum de *m* octets sont extraits du numéro de contrôle de groupe. Si *n* plus *m* est supérieur à 9, alors seulement 9 - *n* octets sont extraits du numéro de contrôle de groupe. Par exemple, avec I4G6, 4 octets sont extraits de l'EDI.
I*n*G*m*C	Transaction	*n* octets sont extraits du numéro de contrôle de l'EDI et *m* octets sont extraits du numéro de contrôle de groupe. Les octets restants de la zone du numéro de contrôle de transaction sont utilisés pour maintenir un numéro de contrôle. Le nombre de positions laissées détermine la valeur maximale du numéro de contrôle. Par exemple, I2G4C laisse trois positions et la valeur maximale est 999. Le numéro de contrôle repasse ensuite à 1.
I*n*G*m*V	Transaction	*n* octets sont extraits du numéro de contrôle de l'EDI et *m* octets sont extraits du numéro de contrôle de groupe. Pour les octets restants de la zone de numéro de contrôle de transaction, une valeur incrémentale est utilisée, de sorte que la première transaction a la valeur 1, la deuxième la valeur 2, etc.

Tableau 28. Masques des numéros de contrôle (suite)

Code	Numéro de contrôle	Description
I*n*G*m*V*o*	Transaction	*n* octets sont extraits du numéro de contrôle de l'EDI et *m* octets sont extraits du numéro de contrôle de groupe. Pour les octets restants, jusqu'à *0* octets de la zone du numéro de contrôle de transaction, une valeur incrémentale est utilisée, de sorte que la première transaction a la valeur 1, la deuxième la valeur 2, etc.

Initialisation du numéro de contrôle

Pourquoi et quand exécuter cette tâche

Pour configurer les numéros de contrôle qui seront utilisés par l'enveloppeur, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Initialisation du numéro de contrôle**.
2. Entrez le nom d'un partenaire et cliquez sur **Rechercher** ou cliquez sur **Rechercher** sans entrer de nom, pour afficher tous les partenaires. Si vous laissez **Prêt pour l'EDI** coché, vous limitez la recherche aux partenaires qui bénéficient de fonctions business-to-business de document EDI. Si vous décochez la case, vous effectuez une recherche sur tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.
4. Les affectations actuelles du numéro de contrôle du partenaire (s'il existe) sont indiquées sur la page Caractéristiques de configuration du numéro de contrôle. Cliquez sur l'icône **Edition** pour ajouter des valeurs ou en modifier.
5. Tapez ou modifiez la valeur en regard de l'**échange** pour indiquer le numéro que vous souhaitez utiliser pour initialiser la génération du numéro de contrôle pour les échanges.
6. Tapez ou modifiez la valeur en regard du **groupe** pour indiquer le numéro que vous souhaitez utiliser pour initialiser la génération du numéro de contrôle pour les groupes. Vous pouvez également cliquer sur **Masque** et taper un masque à utiliser à la place d'une valeur fixe.
7. Tapez ou modifiez la valeur en regard de la **transaction** pour indiquer le numéro que vous souhaitez utiliser pour initialiser la génération du numéro de contrôle pour les transactions. Vous pouvez également cliquer sur **Masque** et taper un masque à utiliser à la place d'une valeur fixe.
8. Cliquez sur **Sauvegarder**.

Numéros de contrôle en cours

Pour une paire de partenaires dont la table de contrôle contient déjà des données, vous pouvez modifier la génération des numéros de contrôle. Vous pouvez :

- Réinitialiser la génération de numéros de contrôle de la paire sur un état initial.
- Modifiez le numéro d'EDI, de groupe ou de transaction (ou toute combinaison de ces numéros) et enregistrez-le avec une nouvelle valeur.

Remarque : La réinitialisation de la génération des numéros de contrôle ou l'édition d'un groupe ou d'un masque doivent être effectués avec précaution, afin

d'éviter les numéros hors séquence ou en double. Ces opérations peuvent cependant être nécessaires dans le cadre de tests ou si un partenaire exige des numéros de contrôle différents.

Pour déterminer quels partenaires ont des numéros de contrôle (et identifier ces numéros), utilisez la fonctionnalité Numéros de contrôle actuels.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Numéros de contrôle actuels**.
2. Appliquez l'une des procédures suivantes :
   - Si vous souhaitez consulter le statut actuel de tous les partenaires, laissez **Tout partenaire** sélectionné dans la liste des partenaires et cliquez sur **Afficher le statut en cours**.
   - Pour consulter le statut des partenaires sélectionnés, procédez comme suit :
     a. Entrez le nom des partenaires source et cible et cliquez sur **Rechercher**. Si vous souhaitez limiter les résultats de la recherche aux partenaires qui échangent des documents EDI, laissez **Rechercher les partenaires prêts pour l'EDI** coché.
     b. Dans les listes obtenues, sélectionnez un ou plusieurs partenaires et cliquez sur **Afficher le statut en cours**.

Définition des échanges de documents

Vous pouvez définir manuellement les échanges de document ou en utilisant des assistants. Si vous souhaitez définir vos connexions à l'aide d'assistants, consultez «Définition des échanges de documents à l'aide d'assistants». Si vous souhaitez le faire manuellement, ou modifier manuellement vos connexions, consultez «Définition manuelle des échanges de documents», à la page 213.

Définition des échanges de documents à l'aide d'assistants

WebSphere Partner Gateway comprend deux assistants pour vous aider à définir des échanges de documents. Il s'agit de l'assistant Importation EIF et de l'assistant Connexion EDI.

L'assistant Importation EIF vous guide tout au long des étapes nécessaire à l'importation des mappes contenues dans les fichiers EIF, affiche les détails des mappes téléchargées, associe ces mappes avec les objets de routage adéquats et crée des interactions logiques. A la fin de l'assistant, les nouvelles mappes sont téléchargées et toutes les interactions nécessaires sont créées dans le système. Vous devez ensuite utiliser l'Assistant de connexion EDI pour créer des connexion à l'aide de vos mappes récemment téléchargées.

Remarque : Pour éviter toute confusion, un seul utilisateur peut utiliser l'assistant Importation EIF à la fois.

L'Assistant Connexion EDI peut être utilisé après l'assistant EIF et vous guide tout au long des étapes nécessaires à la configuration d'une interaction EDI (envoi ou réception d'un document EDI). A la fin de l'assistant, les partenaires sélectionnés sont entièrement configurés pour l'interaction EDI. Cela comprend l'activation des fonctions business-to-business, la création d'interactions valides, la création de connexions de partenaire et l'affectation des attributs EDI nécessaires. L'Assistant de connexion génère les connexions de partenaire suggérées sur vos entrées. La liste complète complète des connexions possibles générées est indiquée ici :

- Désenveloppeur de message de base

- Transformation
- Enveloppeur de message de base
- Génération de TA1
- Génération FA
- Enveloppeur pour TA1 et/ou FA
- Désenveloppeur pour TA1 et/ou FA

ces deux assistants sont situés dans l'onglet Assistants dans la console.

Importation de mappes à l'aide de l'assistant Importation EIF

Pourquoi et quand exécuter cette tâche

Pour importer des mappes à l'aide de l'assistant Importation EIF, procédez comme suit :

1. Lancez la console WebSphere Partner Gateway.
2. Cliquez sur **Assistants**.
3. Cliquez sur **Assistant Importation EIF**.
4. Saisissez le nom du fichier que vous voulez importer, ou cliquez sur **Parcourir** pour le localiser.

   Remarque : Pendant l'importation d'un fichier EIF contenant plusieurs mappes, veillez à ce que les noms de mappes contenus dans le fichier soient uniques. Si plusieurs mappes sont téléchargées dans le même fichier EIF avec le même nom de mappe, la dernière mappe correspondante écrase les précédentes mappes correspondantes dans la base de données.
5. Cliquez sur **Importer**.
6. Une liste des mappes qui ont été correctement importées s'affiche. Cliquez sur **Terminer** pour accepter les valeurs par défaut ou cliquez sur **Suivant** pour les voir ou les modifier.
7. Si vous avez cliqué sur **Suivant**, il vous est ensuite demandé de réviser les mappes de transformation et de modifier toute interaction. Sélectionnez une mappe de transformation. Si une interaction existe, elle s'affiche en lecture seule. Pour ajouter une interaction, cliquez sur **Ajouter une interaction**.
8. Dans la fenêtre Ajouter une interaction, sélectionnez une interaction et cliquez sur **Ajouter cette interaction** pour ajouter une interaction à la liste.
9. Lorsque vous avez fini de réviser les mappes de transformation, cliquez sur **Suivant** pour réviser les mappes de validation.
10. Révisez les mappes de validation importées. Si elles sont correctes, cliquez sur **Terminer**. Si vous souhaitez voir les mappes FA, cliquez sur **Suivant**.
11. Révisez les mappes FA importés et cliquez sur **Terminer** une dernière fenêtre s'affiche, présentant les mappes qui ont été correctement importées ainsi que les interactions qui ont été créées. .

Configuration des connexions à l'aide de l'assistant Connexion EDI

Pourquoi et quand exécuter cette tâche

Avant de configurer les connexions à l'aide de l'assistant Connexion EDI, les éléments suivants doivent avoir été créés :

- Le partenaire interne
- Au moins un partenaire externe

- Un ID entreprise EDI pour chaque partenaire. Dans cet assistant, un ID entreprise EDI est défini comme Identificateur entreprise Freeform ayant la forme *qq-xxxxxxxxx*, où *qq* est la qualificateur EDI à deux chiffres et *xxxxxxxxx* est l'Identificateur d'échange EDI à 9 chiffres.
- Destinations et destinations par défaut
- Profil de l'enveloppe

Plusieurs étapes de configuration supplémentaires peuvent être nécessaires avant que les flux EDI puissent être correctement exécutés. Ce qui suit sont des exemples :

- Configurez les formats XML (si vous envoyez ou recevez du XML)
- Configurez les récepteur avec les utilitaires de fractionnement ROD (si vous recevez des ROD)
- Configurez des attributs de connexion supplémentaires pour AS ou AS2 (si vous utilisez le package AS)

Pour créer des connexions à l'aide de l'assistant Connexion EDI, procédez comme suit :

1. Lancez la console WebSphere Partner Gateway.
2. Cliquez sur **Assistants**.
3. Cliquez sur **Assistant Connexion EDI**.
4. Cliquez sur le type de tâche à configurer(**Envoyer un document EDI à un partenaire EDI** ou **Recevoir un document EDI d'un partenaire EDI**), puis cliquez sur **Suivant**.
5. Selon que vous avez sélectionné **recevoir un document EDI d'un partenaire EDI** ou **Envoyer un document EDI à un partenaire EDI**, saisissez le partenaire source ou cible et cliquez sur **Rechercher**.
6. Sélectionnez un partenaire source ou cible dans la liste déroulante, puis cliquez sur **Suivant**.
7. Sélectionnez les propriétés générales pour votre partenaire source ou cible. Si la syntaxe est EDI, vous devez également spécifier les propriétés EDI. Lorsque vous avez sélectionné toutes les propriétés que vous voulez, cliquez sur **Suivant**.

   Remarque :

   a. Les propriétés TA1 et FA ne sont visibles que si la source est un partenaire externe. Le temps requis par FA n'est visible que si la cible est un partenaire externe.

   b. L'Assistant Connexion EDI contient une liste des valeurs communes à utiliser comme valeurs du délimiteur EDI. Si vous souhaitez utiliser une valeur qui n'est pas dans la liste fournie, vous devez éditer l'attribut de connexion à la main après avoir terminé l'assistant. Vous pouvez éditer les attributs de connexion en cliquant sur **Administrateur de compte > Connexions**.

   c. Vous êtes obligé de spécifier une Destination pour chaque mode d'opération. Cela signifie que vous ne pouvez pas sélectionner l'option vierge(“Pas de destination sélectionnée”) option. La plupart des situations d'envoi ou de réception de documents n'est pas gênée par la nécessité de cette configuration de connexion supplémentaire. Si vous devez supprimer des spécifications de destination à partir de Connexion, vous pouvez le faire après avoir terminé avec l'assistant en cliquant sur **Administrateur de compte > Connexions**.

8. Sélectionnez la **Mappe de validation** source ou cible, **Action**, puis **Mappe de transformation** pour le partenaire source ou cible. Les descriptions de mappe s'affichent après avoir sélectionné une mappe. L'empaquetage est vierge pour éviter la confusion dans les cas où l'EDI utilise le package AS. Lorsque vous avez sélectionné ces éléments, cliquez sur **Suivant**.
9. Révisez les connexions suggérées, cliquez sur **Attributs**, **Actions**, ou **Destinations** pour réviser ces paramétrages.

   Remarque : les connexions qui existent déjà et qui ne sont pas en cours de création sont grisées. ces connexions ont également une icône Existe à côté d'elle et n'ont pas de case à cocher Créer. Si les connexions existent déjà, elles ne sont pas écrasées par cet assistant. Dans ce cas, un avertissement apparaît expliquant la situation.
   Si les connexions doivent être modifiées, cliquez sur **Retour**. Lorsque vous êtes satisfait des connexions indiquées, cliquez sur **Terminer**. Si elles doivent être modifiées cliquez sur **Retour**. et une dernière fenêtre s'affiche présentant les connexions que vous avez correctement créées.

Définition manuelle des échanges de documents

L'assistant Importation EIF et l'assistant Connexion EDI peuvent vous aider à définir les échanges de documents (pour plus d'informations sur ces assistants, voir «Définition des échanges de documents à l'aide d'assistants», à la page 210. Il vous est cependant possible de définir ces documents manuellement. Cette section présente de façon détaillée les tâches à exécuter pour établir l'échange de documents pour les EDI qui entrent dans le concentrateur, les documents ou transactions qu'il transforme ou les EDI qu'il envoie. Les procédures décrites dans les sections qui suivent sont générales et ne s'appliquent qu'à l'importation de mappes et à la configuration d'interactions. Les étapes générales pour activer les fonctions business-to-business des partenaires (pour tous les types d'échanges de documents) sont décrites dans «Configuration des fonctions business-to-business», à la page 28. Les procédures de gestion des connexions (pour tous les types d'échanges de documents) sont décrites dans le Chapitre 12, «Gestion des connexions», à la page 253. Pour étudier un exemple d'échange de document EDI, depuis l'importation des mappes jusqu'à la gestion des connexions, consultez l'Chapitre 20, «Exemples d'EDI», à la page 351. Cette annexe propose les exemples suivants :

- « Exemple EDI vers ROD», à la page 351
- « Exemple EDI vers XML», à la page 365
- « Exemple ROD vers EDI», à la page 378
- « Exemple XML vers EDI», à la page 370

Importation manuelle de mappes

Pourquoi et quand exécuter cette tâche

Il est possible de créer des mappes de transformation pour des documents EDI, XML ou ROD (record-oriented-data), à l'aide du programme client Data Interchange Services. Le client Data Interchange Services est utilisé pour créer et maintenir des définitions de documents de schéma XML et de documents DTD XML, des standards EDI, des définitions de document ROD et des mappes.

Les mappes WTX sont créées à l'aide de WTX design studio et importées dans WebSphere Partner Gateway.

Le client Data Interchange Services est un programme installé séparément, fourni sur le support de WebSphere Partner Gateway, mais qui réside généralement sur un autre ordinateur. Le spécialiste de mappage crée une mappe qui précise la façon dont les éléments d'un document sont déplacés vers les éléments d'un autre document différent. Data Interchange Services doit recevoir des instructions expliquant comment changer le format d'un document et connaître la présentation ou le format des documents source et cible. Dans Data Interchange Services, la présentation d'un document est une *définition de document*.

Lorsque la mappe de transformation est importée dans WebSphere Partner Gateway, les définitions de document créées dans Data Interchange Services sont affichées en tant que définitions de documents (package, protocole et type de documents) sur les pages Mappe de transformation et Gérer des définitions de documents.

Par exemple, si vous convertissez un document XML en transaction X12, importez la mappe qui détermine la définition de document de transaction XML et X12 et la transformation qui doit avoir lieu.

Il existe deux méthodes pour recevoir des fichiers de mappe à partir de Data Interchange Services. Si le client est directement connecté à la base de données WebSphere Partner Gateway, le spécialiste de mappage peut exporter le fichier directement dans la base de données. Un scénario plus probable est que vous recevrez les fichiers dans un e-mail ou en tant que transfert FTP. Dans ce dernier cas, les fichiers doivent être de forme binaire.

Si une erreur survient lors de l'exportation d'une mappe à partir du client Data Interchange Services, vous devriez toujours voir le nom de la mappe dans la console de communauté. La mappe ne peut servir à transformer les documents. Vous devrez avertir le spécialiste Data Interchange Services du problème d'exportation et lui demander d'exporter de nouveau la mappe, pour pouvoir l'utiliser afin de transformer des documents.

Pour importer une mappe, procédez comme suit :

1. Ouvrez une fenêtre de commande.
2. Entrez la commande ou le script suivant :
   - Sous UNIX :

     `<ProductDir>/bin/bcgDISImport.sh <mappe_chaîne_contrôle>`
   - Sous Windows :

     `<ProductDir>\bin\bcgDISImport.bat <mappe_chaîne_contrôle>`

     où *<ID_utilisateur_base_de_données>* et *<mot_de_passe>* sont les valeurs que vous avez utilisées lors de l'installation de la base de données, dans le cadre de l'installation de WebSphere Partner Gateway. La *<mappe_de_chaîne_de_contrôle>*est le chemin complet du fichier de chaîne de contrôle de mappe, exporté depuis le client Data Interchange Services.
3. Pour des mappes de transformation, vérifiez que la définition de documents a été importée.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de transformation**.
   b. Dans la page Mappes de transformation, cliquez sur l'icône **Afficher les détails** en regard de la mappe de Data Interchange Services. Vous remarquerez que les définitions de documents pour la source et la cible sont affichées, indiquant le format dans lequel le document sera reçu au niveau du concentrateur et celui dans lequel il sera fourni par le concentrateur.

c. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
d. Développez les packages et protocoles associés aux définitions de documents affichées dans la page Mappes de transformation, pour vérifier que les types de documents sont affichés sur la page Gérer les définitions de documents.

Vous pouvez utiliser des mappes de validation avec les mappes de transformation pour ajouter une validation des standards EDI à tout processus de translation impliqué dans les standards EDI. Les mappes de validation vous donnent le contrôle complet de la validation d'un document EDI.

Notez que les mappes de transformation et de validation qui ont été exportées depuis le client Data Interchange Services ou importées par l'utilitaire bcgDISImport ne peuvent pas être téléchargées depuis la console de communauté de WebSphere Partner Gateway. Le spécialiste de mappage Data Interchange Services peut administrer ces mappes en se connectant à la base de données WebSphere Partner Gateway par le client Data Interchange Services.

Importation de mappes WTX
Pourquoi et quand exécuter cette tâche

Les mappes WTX créées à l'aide de WTX design studio doivent être importées dans WebSphere Partner Gateway de manière à l'associer à une connexion de participant en particulier. Vous devez créer manuellement un DFD. Les DFD créés sont exportés depuis WTX design studio sous la forme d'une mappe conforme au système d'exploitation natif. Pour importer dans WebSphere Partner Gateway, allez dans **hubadmin > Mappes > Mappes de transformation** et cliquez sur **Créer**. La mappe importée sera stockée dans le système de fichiers commun sous un dossier spécifique dédié aux mappes WTX (commun/mappes).

Importation d'EIF standard depuis WDI
Pourquoi et quand exécuter cette tâche

Pour valider les transactions EDI dans WebSphere Partner Gateway, la forme compilée de l'EDI standard doit être accessible dans WebSphere Partner Gateway. Pour créer cette chaîne de contrôle de standard compilé, procédez comme suit :

1. Téléchargez le standard EDI depuis le site Web de support WDI.
2. Créez une mappe de transformation de données pour la transformation et sélectionnez la transaction EDI que vous voulez valider dans WebSphere Partner Gateway. Par exemple, si vous voulez valider la transaction 810 de X12V4R1, créez une mappe de transformation de données de X12V4R1-810 vers X12V4R1-810.
3. Ne mappez qu'un seul segment obligatoire et compilez la mappe de transformation.
4. Exportez la chaîne de contrôle de transformation de données dans la base de données du gestionnaire de documents. Cela exportera également le standard compilé, qui peut alors être utilisé pour validation.

Remarque : Sinon, quelques exemples d'EIF sont fournis qui comprennent uniquement la chaîne de contrôle de standard compilé.

Configuration d'un flux EDI vers EDI

Pourquoi et quand exécuter cette tâche

Cette section décrit les interactions nécessaires pour recevoir un EDI et le désenvelopper, transformer une transaction d'un format EDI en un autre, envelopper la transaction et la livrer.

1. Vérifiez qu'une définition de documents existe pour l'EDI reçu par le concentrateur. Souvenez-vous qu'une fois l'EDI désenveloppé, le traitement de l'enveloppe d'origine est arrêté. Autrement dit, elle n'a pas de point de livraison. Par conséquent, vous utiliserez le package **N/A** sur l'interaction cible.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
   b. Vérifiez s'il existe déjà une définition de documents. Par exemple, si un partenaire prévoit d'envoyer un EDI en tant que package AS, protocole EDI-X12 et type de documents ISA, la définition est déjà disponible. De la même façon, une définition de documents N/A/EDI-X12/ISA existe déjà.
   c. Entrez une valeur (ou sélectionnez-en une pour tout attribut que vous voulez associer au profil. Par exemple, si vous souhaitez préciser que l'enveloppe doit être annulée en cas d'erreur dans l'une des transactions, cliquez sur l'icône **Edition des valeurs d'attribut** en regard de **Définitions de document**. Sur la ligne **Annuler l'enveloppe en cas d'erreur**, sélectionnez **Oui** dans la liste.
   d. Si aucune définition de documents n'existe, créez-en une en sélectionnant Package, Protocole et Type de documents.

   Remarque : Vous ne pouvez pas utiliser l'attribut Annuler l'enveloppe en cas d'erreur lorsque l'action dans la connexion est la validation d'échange EDI.
2. Créez une interaction pour l'EDI.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sélectionnez les définitions de documents source et cible. A l'exception du package (qui sera **N/A** pour la cible), les définitions de documents seront les mêmes.
   d. Sélectionnez **Désenveloppement EDI** dans la liste des actions.
3. Importez la mappe de transformation qui fournit des définitions de documents des transactions EDI et décrit le mode de transformation de la transaction d'un format EDI à un autre. Voir « Importation manuelle de mappes», à la page 213.

   Si l'EDI contient plusieurs transactions, répétez cette étape pour chacune d'entre elles.
4. Si vous souhaitez modifier des attributs des définitions de documents associées à la mappe, procédez comme suit :
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
   b. Cliquez sur l'icône **Editer les valeurs des attributs** en regard du protocole. Pour les protocoles EDI, s'affiche une longue liste d'attributs paramétrables.
   c. Entrez une valeur (ou sélectionnez-en une dans la liste) pour tout attribut que vous voulez associer au protocole.
   d. Cliquez sur l'icône **Editer les valeurs des attributs** en regard de la définition de documents. En général, la liste affichée est plus courte que celle des attributs associés au protocole.

e. Entrez une valeur (ou sélectionnez-en une dans la liste) pour tout attribut que vous voulez associer au type de documents. Par exemple, vous pouvez modifier la **Mappe de validation** associée au type de documents.

   Veillez à sélectionner un profil d'enveloppe pour la transaction.

5. Créez une interaction pour la mappe que vous venez d'importer.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sous **Source**, sélectionnez le type de documents associé à la transaction. Développez le package et le protocole et sélectionnez le type de documents. En général, ce sera **N/A** (car la transaction elle-même n'est pas créée à l'origine par le partenaire), le protocole défini dans la mappe (par exemple **X12V4R1**) et le document EDI réel défini dans la mappe (par exemple **850**).
   d. Sous **Cible**, sélectionnez la définition de documents pour le document transformé. Développez le package et le protocole et sélectionnez le type de documents. Comme la transaction sera enveloppée (et donc ne sera pas livrée directement à un partenaire), le package sera de nouveau **N/A**.
   e. A partir de la liste des mappes de transformation, sélectionnez la mappe qui définit le mode de transformation de ce document.
   f. Dans la liste des actions, sélectionnez **Validation et translation EDI** pour WDI natif. Pour WTX, sélectionnez **Validation EDI et transformation WTX**.
6. Vérifiez si une définition de documents existe pour l'EDI envoyé par le concentrateur et configurez tout attribut que vous souhaitez lui associer.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
   b. Vérifiez s'il existe déjà une définition de documents. L'empaquetage source sera N/A, le protocole et le type de documents correspondront à ceux utilisés pour livrer l'EDI. Par exemple, si vous prévoyez de fournir l'EDI en tant que AS/EDI-X12/ISA, la source sera N/A/EDI-X12/ISA.
   c. Editez tout attribut qui s'applique à l'EDI en cours de livraison.
   d. Si aucune définition de documents n'existe, créez-en une en sélectionnant Package, Protocole et Type de documents.
7. Créez une interaction pour l'EDI envoyé par le concentrateur une fois la transaction transformée.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sélectionnez les documents source et cible. A l'exception du package (qui sera **N/A** pour le document source), les définitions de documents seront les mêmes.
   d. Sélectionnez **Passe-système** dans la liste **Action**.

Pour ajouter un accusé de réception au flux, voir «Configuration des accusés de réception», à la page 224.

Après avoir configuré les interactions, créez des fonctions business-to-business pour les partenaires.

- Pour le partenaire source, activez trois définitions de documents (sous **Définition de la source**), un pour le type de documents source, une pour la transaction EDI et une pour l'enveloppe.
- Pour le partenaire cible, activez trois définitions de documents (sous **Définition de la cible**), une pour le type de documents désenveloppé, une pour la transaction EDI et une pour l'enveloppe EDI.

La procédure de création des fonctions business-to-business sont détaillées dans «Configuration des fonctions business-to-business», à la page 28.

Une fois définies les fonctions business-to-business des partenaires, créez les connexions. Vous avez besoin de trois connexions :

- Une pour l'enveloppe depuis le partenaire source vers le concentrateur.
- Une pour la transaction EDI source vers la transaction EDI cible.
- Une pour l'enveloppe depuis le concentrateur vers le partenaire.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 253.

Configuration d'un flux EDI vers XML ou ROD

Pourquoi et quand exécuter cette tâche

Cette section décrit les interactions nécessaires pour recevoir un EDI, le désenvelopper, transformer une transaction depuis le format EDI vers un document XML ou ROD et le livrer.

Remarque : Pour un exemple complet de flux EDI vers XML, voir « Exemple EDI vers XML», à la page 365. Pour un exemple complet de flux EDI vers ROD, voir « Exemple EDI vers ROD», à la page 351.

1. Vérifiez qu'une définition de documents existe pour l'EDI reçu par le concentrateur. Gardez en mémoire qu'une fois l'EDI désenveloppé, le traitement de l'enveloppe est arrêté. Autrement dit, elle n'a pas de point de livraison. Par conséquent, vous utiliserez le package **N/A** sur l'interaction cible.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
   b. Vérifiez s'il existe déjà une définition de documents. Par exemple, si un partenaire prévoit d'envoyer un EDI en tant que package AS, protocole EDI-X12 et type de documents ISA, la définition est déjà disponible. De la même façon, une définition de documents N/A/EDI-X12/ISA existe déjà.
   c. Si aucune définition de document n'existe, créez-en une.
2. Créez une interaction pour l'EDI reçu au niveau du concentrateur.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sélectionnez les documents source et cible. A l'exception du package (qui sera **N/A** pour la cible), les définitions de documents seront les mêmes.
   d. Sélectionnez **Désenveloppement EDI** dans la liste des actions.
3. Importez la mappe de transformation qui fournit les définitions de documents de la transaction EDI et du document XML ou ROD et décrit la façon dont la transaction est transformée en document XML ou ROD. Voir « Importation manuelle de mappes», à la page 213.

Si l'EDI contient plusieurs transactions, répétez cette étape pour chacune d'entre elles.

4. Créez une interaction pour la mappe que vous venez d'importer.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sous **Source**, sélectionnez le type de documents associé à la transaction. Développez le package et le protocole et sélectionnez le type de documents. En général, ce sera **N/A** (car la transaction elle-même n'est pas créée à l'origine par le partenaire), le protocole défini dans la mappe (par exemple **X12V4R1**) et le document EDI réel défini dans la mappe (par exemple **850**).
   d. Sous **Cible**, sélectionnez la définition de documents pour le document (XML ou ROD) transformé. Développez le package et le protocole et sélectionnez le type de documents.
   e. A partir de la liste des mappes de transformation, sélectionnez la mappe qui définit le mode de transformation de ce document.
   f. Dans la liste des actions, sélectionnez **Validation et translation EDI** pour WDI natif. Pour WTX, sélectionnez **Validation EDI et transformation WTX**.

Pour ajouter un accusé de réception au flux, voir «Configuration des accusés de réception», à la page 224.

Après avoir configuré les interactions, créez des fonctions business-to-business pour les partenaires.

- Pour le partenaire source, activez deux définitions de documents (sous **Définition de la source**), une pour la transaction EDI et une pour l'enveloppe.
- Pour le partenaire cible, activez deux définitions de documents (sous **Définition de la cible**), une pour l'enveloppe EDI et une pour le document XML ou ROD.

La procédure de création des fonctions business-to-business sont détaillées dans «Configuration des fonctions business-to-business», à la page 28.

Une fois définies les fonctions business-to-business des partenaires, créez les connexions. Vous avez besoin de deux connections :

- Une pour l'enveloppe depuis le partenaire source vers le concentrateur.
- Une pour la transaction source EDI vers le document ROD ou XML.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 253.

Configuration d'un flux XML ou ROD vers EDI

Pourquoi et quand exécuter cette tâche

Cette section décrit les interactions nécessaires pour recevoir un document XML ou ROD, le transformer en transaction EDI, envelopper la transaction et la livrer.

Remarque : Pour un exemple complet de flux XML vers EDI, voir « Exemple XML vers EDI», à la page 370. Pour un exemple complet de flux ROD vers EDI, voir « Exemple ROD vers EDI», à la page 378.

1. Importez la mappe de transformation qui fournit les définitions du document XML ou ROD et de la transaction EDI, et qui décrit comment le document est transformé en transaction EDI. Voir « Importation manuelle de mappes», à la page 213.

2. Créez une interaction pour la mappe que vous venez d'importer.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sous **Source**, sélectionnez la définition de documents associée au document XML ou ROD. Développez le package et le protocole et sélectionnez le type de documents.
   d. Sous **Cible**, sélectionnez le type de documents associé à la transaction EDI. Développez le package et le protocole et sélectionnez le type de documents. Comme la transaction ne sera pas livrée directement (elle sera placée dans une enveloppe avant d'être livrée), vous utiliserez le package **N/A**.
   e. A partir de la liste des mappes de transformation, sélectionnez la mappe qui définit le mode de transformation de ce document.
   f. Dans la liste Action, sélectionnez **Translation XML et validation EDI** ou **Translation ROD et validation EDI** pour WDI natif. Pour WTX, sélectionnez **Transformation WTX**.
3. Vérifiez si une définition de documents existe pour l'EDI envoyé par le concentrateur et configurez tout attribut que vous souhaitez lui associer.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
   b. Vérifiez s'il existe déjà une définition de documents. Pour le document source (l'EDI envoyé depuis le concentrateur), le package sera **N/A**.
   c. Editez tout attribut qui s'applique à l'EDI en cours de livraison.
   d. Si aucune définition de documents n'existe, créez-en une en sélectionnant Package, Protocole et Type de documents.
4. Créez une interaction pour l'EDI envoyé par le concentrateur une fois le document transformé.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sélectionnez les documents source et cible. Les documents source et cible ont des packages différents (le document source est empaqueté N/A), mais le protocole (EDI-X12 par exemple) et le type de documents (ISA par exemple) doivent être identiques.
   d. Sélectionnez **Passe-système** dans la liste des actions.

Après avoir configuré les interactions, créez des fonctions business-to-business pour les partenaires.

- Pour le partenaire source, le nombre de définitions de documents à définir (sous **Définition de la source**) dépend du type de documents.
  - Par exemple, pour un document XML dont le type de documents est ICGPO et la translation EDI est MX12V3R1, vous activerez trois définitions de documents (sous **Définition de la source**), une pour le document XML (ICGPO), une pour la transaction EDI (MX12V3R1) et une pour l'enveloppe envoyée depuis le concentrateur.
  - Pour les autres documents XML et pour les documents ROD, vous activerez deux définitions de documents (sous **Définition de la source**), une pour le document XML ou ROD document et une pour l'enveloppe envoyée depuis le concentrateur.

- Pour le partenaire cible, activez deux définitions de documents (sous **Définition de la cible**), une pour la transaction EDI et une pour l'enveloppe EDI reçue. Pour la transaction EDI, cliquez sur l'icône **Editer les valeurs des attributs** en regard du protocole et indiquez un profil d'enveloppe. Vous pouvez également indiquer d'autres attributs.

La procédure de création des fonctions business-to-business sont détaillées dans «Configuration des fonctions business-to-business», à la page 28.

Une fois définies les fonctions business-to-business des partenaires, créez les connexions. Vous avez besoin de deux connections :

- Une pour le document source XML ou ROD, vers la transaction EDI.
- Une pour l'enveloppe depuis le concentrateur vers le partenaire.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 253.

Configuration de plusieurs documents XML ou ROD en un flux de fichier vers EDI

Pourquoi et quand exécuter cette tâche

Cette section décrit les interactions nécessaires pour recevoir plusieurs documents XML ou ROD dans le même fichier, les transformer en transactions EDI, envelopper les transactions et livrer l'EDI.

1. Importez la mappe de transformation qui fournit les définitions des documents XML ou ROD et des transactions EDI, et qui décrit la transformation. Voir « Importation manuelle de mappes», à la page 213.
2. Créez une interaction pour les documents source et cible.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Pour WDI natif, sélectionnez les documents source et cible et **Translation XML et validation EDI** ou **Translation ROD et validation EDI** dans la liste des actions. Pour WTX, sélectionnez **Transformation WTX** et **Validation EDI**.
3. Répétez l'étape 2 pour le document source et chaque document cible produit par la mappe de transformation.
4. Vérifiez si une définition de documents existe pour l'EDI envoyé par le concentrateur et configurez tout attribut que vous souhaitez lui associer.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
   b. Vérifiez s'il existe déjà une définition de documents. L'empaquetage source sera N/A, le protocole et le type de documents correspondront à ceux utilisés pour livrer l'EDI. Par exemple, si vous prévoyez de fournir l'EDI en tant que AS/EDI-X12/ISA, la source sera N/A/EDI-X12/ISA.
   c. Editez tout attribut qui s'applique à l'EDI en cours de livraison.
   d. Si aucune définition de documents n'existe, créez-en une en sélectionnant Package, Protocole et Type de documents.
5. Créez une interaction pour l'EDI envoyé par le concentrateur une fois la transaction transformée.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.

b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.

c. Sélectionnez les documents source et cible. Les documents source et cible ont des packages différents (le document source est empaqueté N/A), mais le protocole (EDI-X12 par exemple) et le type de documents (ISA par exemple) doivent être identiques.

d. Sélectionnez **Passe-système** dans la liste des actions.

Après avoir configuré les interactions, créez des fonctions business-to-business pour les partenaires.

- Pour le partenaire source, le nombre de définitions de documents à définir (sous **Définition de la source**) dépend du type de documents.
  - Par exemple, pour un document XML dont le type de documents est ICGPO et la translation EDI est MX12V3R1, vous activerez trois définitions de documents (sous **Définition de la source**), une pour le document XML (ICGPO), une pour la transaction EDI (MX12V3R1) et une pour l'enveloppe envoyée depuis le concentrateur.
  - Pour les autres documents XML et pour les documents ROD, vous activerez deux définitions de documents (sous **Définition de la source**), une pour le document XML ou ROD document et une pour l'enveloppe envoyée depuis le concentrateur.

La procédure de création des fonctions business-to-business sont détaillées dans «Configuration des fonctions business-to-business», à la page 28.

Une fois définies les fonctions business-to-business des partenaires, créez les connexions. Vous avez besoin de plusieurs connections :

- Une pour chaque document XML ou ROD qui est transformé en une transaction EDI.
- Une pour l'enveloppe depuis le concentrateur vers le partenaire.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 253.

Configuration d'un flux de documents XML vers ROD ou ROD vers XML

Pourquoi et quand exécuter cette tâche

Cette section décrit les interactions requises pour recevoir un document XML ou ROD, le transformer dans un autre type (XML vers ROD ou ROD vers XML) et le livrer.

1. Importez la mappe de transformation qui fournit les définitions des documents XML et ROD et qui décrit la méthode de transformation des documents. Voir « Importation manuelle de mappes», à la page 213.
2. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de transformation**, puis cliquez sur l'icône **Afficher les détails** en regard de la mappe que vous venez d'importer.
3. Créez une interaction pour la mappe que vous venez d'importer.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
4. Sélectionnez les documents source et cible et **Translation WTX** pour WTX ou **Translation ROD et validation EDI** dans la liste des actions.

Après avoir configuré les interactions, créez des fonctions business-to-business pour les partenaires.

- Pour le partenaire source, activez les définitions de documents (sous **Définition de la source**) pour le document XML ou ROD.
- Pour le partenaire cible, activez les définitions de documents (sous **Définition de la cible**) pour le document XML ou ROD.

La procédure de création des fonctions business-to-business sont détaillées dans «Configuration des fonctions business-to-business», à la page 28.

Une fois définies les fonctions business-to-business des partenaires, créez les connexions. Vous avez besoin d'une connexion, pour le flux XML vers ROD ou pour le flux ROD vers XML. Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 253.

Configuration d'un flux de documents XML vers XML ou ROD vers ROD

Pourquoi et quand exécuter cette tâche

Cette section décrit les interactions nécessaires pour recevoir un document XML ou ROD, le transformer en un document de même type (XML vers XML ou ROD vers ROD) et le livrer.

1. Importez la mappe de transformation qui fournit les définitions des documents XML ou ROD et qui décrit la méthode de transformation des documents. Voir « Importation manuelle de mappes», à la page 213.
2. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de transformation**, puis cliquez sur l'icône **Afficher les détails** en regard de la mappe que vous venez d'importer.
3. Créez une interaction pour la mappe que vous venez d'importer.
   a. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
   c. Sélectionnez les documents source et cible.
   d. Pour WDI natif, sélectionnez **Translation XML et validation EDI** ou **Translation ROD et validation EDI** dans la liste Action. Pour WTX, sélectionnez **Transformation WTX** et **Validation d'échange EDI**.

Après avoir configuré les interactions, créez des fonctions business-to-business pour les partenaires.

- Pour le partenaire source, activez une définition de documents (sous **Définition de la source**) pour le document XML ou ROD.
- Pour le partenaire cible, activez une définition de documents (sous **Définition de la cible**) pour le document XML ou ROD.

La procédure de création des fonctions business-to-business sont détaillées dans «Configuration des fonctions business-to-business», à la page 28.

Une fois définies les fonctions business-to-business des partenaires, créez les connexions. Vous avez besoin d'une connexion, pour le flux XML vers XML ou pour le flux ROD vers ROD. Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 253.

Configuration des accusés de réception

Cette section explique comment configurer les interactions pour envoyer des accusés de réception d'EDI ou un reçu de transaction à l'émetteur du document.

Accusés de réception fonctionnels

Des mappes d'accusés de réception fonctionnels sont utilisées pour permettre la génération d'accusés de réception fonctionnels en réponse à des documents EDI reçus d'un partenaire. WebSphere Partner Gateway fournit un ensemble de mappes d'accusé de réception fonctionnel qui produisent les accusés de réception fonctionnels EDI généraux. Le spécialiste de mappage peut également créer des mappes d'accusé de réception fonctionnel et de validation, auquel cas les mappes sont téléchargées dans WebSphere Partner Gateway.

Remarque : Une mappe d'accusé de réception fonctionnel ne doit être créée que lorsqu'un accusé de réception fonctionnel personnalisé est requis.

Avec les mappes d'accusé de réception fonctionnel proposées par WebSphere Partner Gateway sont fournis le protocole &FUNC_ACK_METADATA_DICTIONARY et les &FUNC_ACK_META associés. Ils figurent sous **Package : None** dans la page Définitions de documents. &FUNC_ACK_META est la définition de document source de toutes les mappes d'accusé de réception fonctionnel. Cette mappe donne la structure de l'accusé de réception fonctionnel. Un accusé de réception fonctionnel est envoyé aux partenaires et la mappe correspondante indique au système comment le générer. Le nom de la définition du document source ne peut être modifié. Le spécialiste de mappage du client Data Interchange Services ne peut créer de mappe d'accusé de réception fonctionnel sans cette définition de document dans votre base de données.

La définition du document cible dans une mappe d'accusé de réception fonctionnel décrit la présentation de ce dernier. Il doit s'agir d'une définition de document EDI, ayant pour nom 997, 999 ou CONTRL.

Les mappes d'accusé de réception fonctionnel suivantes sont installées avec WebSphere Partner Gateway et apparaissent sur la page Gérer des définitions de documents sous **Package : N/A** :

Tableau 29. Mappes d'accusé de réception fonctionnel fournies par le produit

Protocole	Type de document	Description
&DTCTL21	CONTRL	Accusé de réception fonctionnel CONTRL – UN/EDIFACT Version 2 Edition 1 (D94B)
&DTCTL	CONTRL	Accusé de réception fonctionnel CONTRL – UN/EDIFACT antérieur à D94B
&DT99933	999	Accusé de réception fonctionnel 999 – UCS Version 3 Edition 3
&DT99737	997	Accusé de réception fonctionnel 997 – X12 Version 3 Edition 7
&DT99735	997	Accusé de réception fonctionnel 997 – X12 Version 3 Edition 5
&DT99724	997	Accusé de réception fonctionnel 997 – X12 Version 2 Edition 4

De plus, le protocole &X44TA1 (avec un type de documents TA1 associé) figure sous **Package : N/A**. TA1 est un accusé de réception fonctionnel généré pour les EDI X12 entrants.

Le protocole &WDIEVAL (avec un X12ENV associé) est également fourni sous **Package : N/A**.

Comme les transactions EDI, les accusés de réception fonctionnels sont toujours placés dans un EDI avant d'être livrés.

Accusés de réception TA1

TA1 est un segment EDI qui fournit des accusés de réception X12. Il accuse réception et valide la syntaxe d'une paire (ISA ou IEA) d'en-tête et d'élément de fin d'un EDI X12. L'émetteur peut demander un TA1 en donnant à l'élément 14 de l'en-tête de commande de l'IDE ISA la valeur **1**. Le numéro de contrôle EDI d'un TA1 est comparé avec les EDI X12 précédemment transmis pour trouver un numéro de contrôle identique et terminer le processus d'accusé de réception.

Comme les transactions EDI et les accusés de réception fonctionnels, les TA1 sont toujours placés dans un EDI avant d'être livrés.

Ajout d'un accusé de réception au type de documents

Pourquoi et quand exécuter cette tâche

Pour ajouter un accusé de réception à un flux, procédez comme suit :

Procédure

1. Si la mappe d'accusé de réception fonctionnel n'est pas fournie par WebSphere Partner Gateway, importez-la depuis le client Data Interchange Services. Voir « Importation manuelle de mappes», à la page 213.
2. Associez la mappe FA à une définition de documents :
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes d'accusé de réception fonctionnel EDI**.
   b. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.
   c. Cliquez sur l'icône **Développer** en regard d'un package pour le développer jusqu'au niveau voulu (par exemple pour développer les dossiers **Package** et **Protocole**, puis sélectionner une transaction).
   d. Cliquez sur **Sauvegarder**.
3. Créez une interaction pour la mappe que vous venez d'importer.
   a. Cliquez sur le lien **Administrateur du concentrateur > Configuration du concentrateur > Définitions de documents > Gérer les interactions**.
   b. Dans l'écran **Gérer les interactions**, cliquez sur le lien **Création d'une interaction**.
   c. Sous **Source**, sélectionnez le type de documents associé à l'accusé de réception fonctionnel. Développez le package et le protocole et sélectionnez le type de documents.
   d. Sous **Cible**, sélectionnez les mêmes valeurs.
   e. Dans la liste des actions, sélectionnez **Passe-système**.
4. Vérifiez si une définition de documents existe pour l'EDI envoyé par le concentrateur et configurez tout attribut que vous souhaitez lui associer.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.

b. Vérifiez s'il existe déjà une définition de documents. L'empaquetage source sera N/A, le protocole et le type de documents correspondront à ceux utilisés pour livrer l'EDI. Par exemple, si vous prévoyez de fournir l'EDI en tant que AS/EDI-X12/ISA, la source sera N/A/EDI-X12/ISA.

c. Editez tout attribut qui s'applique à l'EDI en cours de livraison.

d. Si aucune définition de documents n'existe, créez-en une en sélectionnant Package, Protocole et Type de documents.

5. Créez une interaction pour l'EDI envoyé par le concentrateur une fois le document transformé.

   a. Cliquez sur le lien **Administrateur du concentrateur > Configuration du concentrateur > Définitions de documents > Gérer les interactions**.

   b. Dans l'écran **Gérer les interactions**, cliquez sur le lien **Création d'une interaction**.

   c. Sélectionnez les documents source et cible.

   d. Sélectionnez **Passe-système** dans la liste **Action**.

Résultats

Après avoir configuré les interactions, créez des fonctions business-to-business pour les partenaires. Notez que le partenaire cible dans une transmission d'accusé de réception fonctionnel est le partenaire source du document EDI initial.

- Pour le partenaire source, activez les définitions de documents (sous **Définition de la source**) pour l'accusé de réception fonctionnel. Activez également une définition de documents pour l'enveloppe qui est envoyée par le concentrateur.
- Pour le partenaire cible, activez une définition de documents (sous **Définition de la cible**) pour l'accusé de réception fonctionnel. Activez également une définition de documents pour l'enveloppe qui est reçue.

  Pour l'accusé de réception fonctionnel, cliquez sur l'icône **Editer les valeurs des attributs** en regard du protocole et indiquez un profil d'enveloppe.

La procédure de création des fonctions business-to-business sont détaillées dans «Configuration des fonctions business-to-business», à la page 28.

Une fois définies les fonctions business-to-business des partenaires, créez les connexions. Vous avez besoin de deux connections :

- Une pour l'accusé de réception fonctionnel.
- Une pour l'enveloppe depuis le concentrateur vers le partenaire.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 253.

Concepts associés

Chapitre 12, «Gestion des connexions», à la page 253

Tâches associées

« Importation manuelle de mappes», à la page 213

«Configuration des fonctions business-to-business», à la page 28

Affichage d'échanges et de transactions EDI

Pourquoi et quand exécuter cette tâche

Comme indiqué précédemment dans ce chapitre, l'Afficheur de documents vous sert pour afficher des informations sur les échanges et transactions EDI qui constituent un flux de documents. Vous pouvez afficher des documents bruts ainsi que les détails des traitements et les événements associés, en précisant les critères de recherche. Ces informations sont intéressantes si vous essayez de savoir si un EDI a bien été livré ou de déterminer la cause d'un problème.

Démarrez l'Afficheur de documents, en entrant ce qui suit :

1. Cliquez sur **Afficheurs> Afficheur de documents**.
2. Sélectionnez les critères de recherche appropriés.
3. Cliquez sur **Rechercher**.

Consultez le *Guide d'administration de WebSphere Partner Gateway* pour obtenir plus d'informations sur l'utilisation de l'Afficheur de documents.

Limitations d'OpenPGP pour la réception et l'envoi de documents EDI avec les différents protocoles de transport

Lors de la réception des documents EDI, les ID entreprise sont déterminés d'après le contenu et ils doivent correspondre aux ID entreprise déterminés d'après l'empaquetage ou la structure du dossier. La réception des données d'échange de données informatisé (EDI) avec les différents protocoles de transport est soumise aux limitations suivantes :

1. Lors de la réception d'un document avec HTTP, l'authentification standard détermine le partenaire expéditeur. Si le paramètre 'A' est utilisé, il détermine l'ID entreprise du partenaire destinataire. L'en-tête de transport 'X-receiver' peut aussi être utilisé pour identifier le partenaire destinataire. Il doit contenir l'ID entreprise du partenaire destinataire. Si le partenaire destinataire n'est pas indiqué, c'est le partenaire interne par défaut qui est considéré comme le destinataire. L'authentification standard contient l'id utilisateur et le mot de passe. Il est recommandé d'utiliser HTTP(S) avec l'authentification serveur et l'authentification standard.
2. Lors de la réception d'un document avec FTP(S), le partenaire expéditeur est déterminé d'après la structure de dossier spécifique à WebSphere Partner Gateway, configurée pour des destinataires FTP(S).
3. Dans le cas des documents binaires, lorsque le document est reçu avec SFTP, le partenaire expéditeur est déterminé d'après les valeurs de configuration, fournies dans le gestionnaire pré-processus associé du récepteur SFTP.

Chapitre 11. Création de destinations

Une fois que vous avez créé les partenaires, définissez leurs destinations. Les destinations définissent des points d'entrée dans le système du partenaire.

Ce chapitre contient les rubriques suivantes :

Remarque : Pour effectuer des modifications de configurations sur WebSphere Partner Gateway, vous devez toujours utiliser la même instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Présentation des destinations

WebSphere Partner Gateway fait appel à des destinations pour acheminer les documents jusqu'à leur destination. Le destinataire peut être un partenaire externe ou le partenaire interne.
Les informations utilisées lors de la configuration d'une destination dépendent du

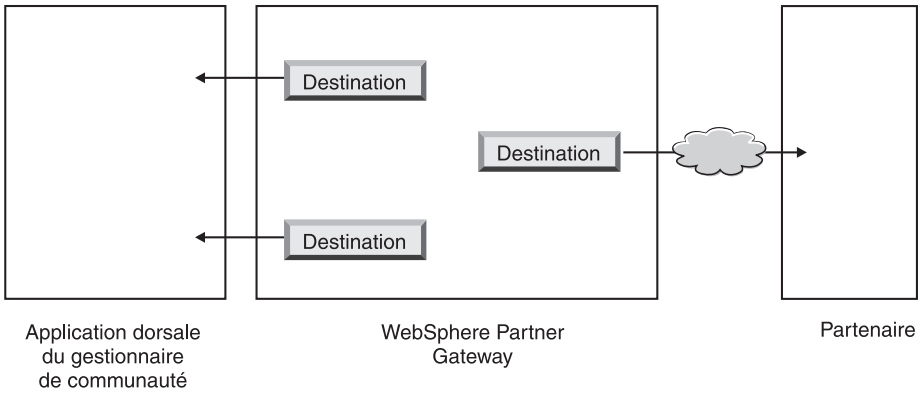


Figure 34. Destinations vers le partenaire interne et les partenaires externes

protocole de transport des documents sortants.

Les transports suivants sont pris en charge (par défaut) pour les destinations du partenaire :

- HTTP/1.1
- HTTPS/1.0
- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP

  Remarque : Vous pouvez définir une destination SMTP uniquement pour les partenaires externes (et non pour le partenaire interne).
- SFTP
- Répertoire de fichiers
- scripts FTP

Vous pouvez également indiquer un type de transport défini par l'utilisateur, que vous téléchargez lors de la création de la destination.

En tant qu'administrateur du concentrateur, vous pouvez définir les destinations de vos partenaires. Vous pouvez également leur laisser le soin d'effectuer cette opération. Dans ce chapitre, vous apprendrez comment exécuter cette tâche pour les partenaires. Pour la gestion des destinations, voir le *Chapitre sur les tâches d'administration du concentrateur du Guide d'administration.*

Définition des valeurs de transport globales

Pourquoi et quand exécuter cette tâche

Définissez les attributs de transport globaux qui s'appliquent à toutes les destinations de script FTP. Si vous ne définissez pas de destinations de script FTP, cette section ne vous concerne pas.

Le mode de transport par script FTP utilise un système de verrou qui empêche que plusieurs instances de script FTP n'accèdent à la même destination au même moment. Des valeurs par défaut sont fournies pour des paramètres comme la durée d'attente des instances de passerelles pour obtenir le verrouillage et le nombre de tentatives au cas où le verrou serait en cours d'utilisation. Vous pouvez utiliser ces valeurs par défaut ou les modifier.

1. Cliquez sur **Administrateur du compte > Profils**.
2. Cliquez sur **Destinations**.
3. Sélectionnez **Attributs de transport globaux** dans les caractéristiques de destination.

   Si vous avez mis à jour **Délai maximal de verrouillage (secondes)** ou **Temps maximal des files d'attente(secondes)** lorsque vous avez spécifié des valeurs de transport global au moment de la création des cibles, ces valeurs sont répercutées ici.
4. Si les valeurs par défaut sont correctes pour votre configuration, cliquez sur **Annuler**. Dans le cas contraire, suivez le reste des étapes de la section.
5. Cliquez sur l'icône **Edition** en regard de **Transport de scripts FTP**.
6. Pour modifier une ou plusieurs valeurs, saisissez-les. Vous pouvez modifier :
   - **Nombre de relances du verrouillage**, le nombre de tentatives de la destination pour obtenir un verrouillage s'il est en cours d'utilisation. La valeur par défaut est 3.
   - **Intervalle entre relances de verrouillage (secondes)**, le temps d'attente entre les tentatives pour obtenir le verrouillage. La valeur par défaut est 260 secondes.
   - **Délai maximal de verrouillage (secondes)**, la durée pendant laquelle la destination peut maintenir le verrouillage. La valeur par défaut est de 240 secondes (à moins que vous ne l'ayez modifié au moment de la création des cibles).
   - **Délai maximal des files d'attente (secondes)**, la durée pendant laquelle la passerelle attendra dans une file d'attente pour obtenir le verrou. La valeur par défaut est de 740 secondes (à moins que vous ne l'ayez modifiée au moment de la création des cibles).
7. Cliquez sur **Enregistrer**

Configuration d'un proxy direct

Pourquoi et quand exécuter cette tâche

Pour les transports HTTP, vous pouvez définir une prise en charge de serveurs proxy directs de sorte que les documents soient envoyés via un serveur proxy configuré. Avec WebSphere Partner Gateway, vous pouvez définir les types suivants :

- Prise en charge de serveurs proxy sur HTTP
- Prise en charge de serveurs proxy sur HTTP avec authentification

- Prise en charge de serveurs proxy sur SOCKS

Remarque : WebSphere Partner Gateway se connecte à un serveur proxy uniquement sur un port HTTP.

Une fois que vous avez défini un proxy direct, vous pouvez le rendre utilisable pour l'ensemble du transport (par exemple, toutes les destinations HTTP utiliseront le proxy direct), en le définissant comme destination par défaut.

^Pour définir un proxy direct, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Destinations**.
3. Cliquez sur **Prise en charge du proxy direct**.
4. Dans la liste des proxy directs, cliquez sur **Créer**.
5. Attribuez un nom au proxy.
6. Indiquez éventuellement une description du proxy.
7. Sélectionnez le type de transport dans la liste.

   Remarque : Les transports disponibles sont HTTP et HTTPS.
8. Entrez les informations suivantes. Indiquez l'hôte ou le port du proxy *ou bien* l'hôte ou le port du proxy SOCKS.
   - Dans **Hôte proxy**, indiquez le serveur proxy à utiliser (par exemple http://proxy.abc.com).
   - Dans **Port proxy**, indiquez le numéro de port.
   - Si le serveur proxy a besoin d'un nom d'utilisateur et d'un mot de passe, entrez-les dans les zones **Nom d'utilisateur** et **Mot de passe**.
   - Dans **Hôte proxy Socks**, indiquez le serveur proxy SOCKS à utiliser.
   - Dans **Port proxy Socks**, indiquez le numéro de port.
9. Cochez la case si vous souhaitez que ce proxy soit celui par défaut (utilisable par tout partenaire bénéficiant d'une prise en charge proxy).
10. Cliquez sur **Sauvegarder**.

Remarque : La technique d'établissement de tunnels HTTP est utilisée dans le proxy direct, mais il n'y a aucune prise en charge pour Sécuriser le proxy direct. Le tunnel HTTP est créé avec le serveur proxy. Vous devez vérifier la connectivité avant de transférer n'importe quel type de données (HTTP ou HTTPS) au partenaire final. Le chiffrement des données est un chiffrement SSL. Le port utilisé pour le proxy direct doit être le port 80 (HTTP). Il s'agit d'un passe-système de l'établissement de liaison SSL entre WebSphere Partner Gateway et le partenaire.

Configuration d'une destination HTTP

Pourquoi et quand exécuter cette tâche

La configuration d'une destination HTTP permet d'envoyer des documents depuis le concentrateur aux adresses IP des partenaires. Lorsque vous configurez une destination HTTP, vous pouvez également demander que les documents soient envoyés via un serveur proxy configuré.

Pour commencer à créer une destination HTTP, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils**.

2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Détails de destination

Pourquoi et quand exécuter cette tâche

Depuis la page **Liste des destinations**, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire. Il s'agit du nom qui apparaîtra dans la liste des destinations.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Sélectionnez éventuellement un serveur proxy à utiliser. La **Liste des proxy directs** répertorie tous les serveurs proxy que vous avez créés, y compris le serveur proxy par défaut. La valeur par défaut de cette zone est **Utiliser le proxy direct par défaut**. Si vous souhaitez que le partenaire sélectionné utilise un serveur proxy différent, choisissez-en un autre dans la liste. Si vous ne voulez pas utiliser cette fonctionnalité avec ce partenaire, sélectionnez **Ne pas utiliser de proxy direct**.
2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est : http://*<nom_serveur>*:*<port_facultatif>*/*<chemin>*

   Exemple :

   ```
   http://anotherserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   Remarque : Si vous spécifiez une adresse IPv6, indiquez le format numérique et non le nom de la machine ou le nom d'hôte.

   Les exemples d'adresse IPv6 comprennent :

   ```
   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]
   ```

   Lorsque vous configurez une destination utilisée par un Service Web, précisez l'adresse URL privée indiquée par le fournisseur du Service Web. Il s'agit du point où WebSphere Partner Gateway appelle le Service Web lorsqu'il se comporte comme un proxy pour le fournisseur de Service Web.

3. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur HTTP le nécessite.
4. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
5. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
6. Dans la zone **Nombre d'unités d'exécution**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option**Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la destination n'a pas été mise en ligne manuellement.
9. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
10. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 250. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination HTTPS

Pourquoi et quand exécuter cette tâche

Configurez une destination HTTPS pour que des documents puissent être envoyés depuis le concentrateur à l'adresse IP de vos partenaires. Lorsque vous configurez une destination HTTPS, vous pouvez également demander que les documents soient envoyés via un serveur proxy configuré.

Pour créer des destinations HTTPS, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Caractéristiques de la destination

Pourquoi et quand exécuter cette tâche

Dans la page Détails sur la destination, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.

2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.
5. Sélectionnez **HTTPS/1.0** ou **HTTPS/1.1** dans la liste **Transport**.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Sélectionnez éventuellement un serveur proxy à utiliser. La **Liste des proxy directs** répertorie tous les serveurs proxy que vous avez créés, y compris le serveur proxy par défaut. La valeur par défaut de cette zone est **Utiliser le proxy direct par défaut**. Si vous souhaitez que le partenaire sélectionné utilise un serveur proxy différent, choisissez-en un autre dans la liste. Si vous ne voulez pas utiliser cette fonctionnalité avec ce partenaire, sélectionnez **Ne pas utiliser de proxy direct**.
2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est : https://*<nom_serveur>*:*<port_facultatif>*/*<chemin>*

   Par exemple :

   ```
   https://anotherserver.ibm.com:57443/bcgreceiver/Receiver
   ```

   Remarque : Si vous spécifiez une adresse IPv6, indiquez le format numérique et non le nom de la machine ou le nom d'hôte.

   Les exemples d'adresse IPv6 comprennent :

   ```
   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. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur HTTP sécurisé le nécessite.
4. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
5. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
6. Dans la zone **Nombre d'unités d'exécution**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
8. Dans la zone **Validation du certificat SSL du client**, sélectionnez **Oui** si vous voulez que le certificat numérique du partenaire expéditeur soit validé par rapport à l'ID entreprise associé au document. La valeur par défaut est **Non**.

9. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option**Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la destination n'a pas été mise en ligne manuellement.
10. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
11. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 250. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination FTP

Pourquoi et quand exécuter cette tâche

Pour créer une destination FTP, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Remarque : Le mode passif FTP n'est pas pris en charge. Pour plus d'informations sur la prise en charge du mode passif, reportez-vous à la section «Configuration d'une destination de script FTP», à la page 245.

Détails de destination

Pourquoi et quand exécuter cette tâche

Dans la page Détails sur la destination, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est : ftp://<*nomserveur_ftp*>:<*numéroport*>

   Par exemple :

```
ftp://ftpserver1.ibm.com:2115
```

Si vous ne définissez pas de numéro de port, le port FTP standard est utilisé.

Remarque : Si vous spécifiez une adresse IPv6, indiquez le format numérique et non le nom de la machine ou le nom d'hôte.

Les exemples d'adresse IPv6 comprennent :

```
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. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur FTP le nécessite.
3. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
4. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
5. Dans la zone **Nombre d'unités d'exécution**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
6. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
7. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option**Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la destination n'a pas été mise en ligne manuellement.
8. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
9. Si vous souhaitez que le document garde son nom original lorsqu'il est envoyé à sa destination, ne sélectionnez pas **Utiliser un nom de fichier unique**. Vous pouvez également sélectionner cette option si vous souhaitez que WebSphere Partner Gateway affecte un nom au fichier.
10. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 250. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination SMTP

Pourquoi et quand exécuter cette tâche

Pour créer une destination SMTP, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.

3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Détails de destination

Pourquoi et quand exécuter cette tâche

Depuis la page Liste des destinations, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est : mailto:<*utilisateur@nomserveur*>

   Par exemple :

   ```
   mailto:admin@anotherserver.ibm.com
   ```
2. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur SMTP le nécessite.
3. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
4. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
5. Dans la zone **Nombre d'unités d'exécution**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
6. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
7. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option**Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la destination n'a pas été mise en ligne manuellement.
8. Dans la zone **Authentification obligatoire**, indiquez si un nom d'utilisateur et un mot de passe doivent être fournis pour le document. La valeur par défaut est **Non**.

9. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 250. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination JMS

Pourquoi et quand exécuter cette tâche

Pour créer des destinations JMS, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Remarque : Pour plus d'informations sur la configuration des bibliothèques d'exécution afin que les fichiers JAR requis de WebSphere MQ soient visibles pour WebSphere Partner Gateway, reportez-vous à la section «Configuration des bibliothèques d'exécution», à la page 42.

Détails de destination

Pourquoi et quand exécuter cette tâche

Depuis la page Liste des destinations, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Dans la zone **Adresse**, entrez l'adresse URL correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Pour WebSphere MQ JMS, le format de l'URL cible est le suivant :

   `file:///<chemin_liaisons_MQ_JNDI_défini_par_utilisateur>`

   Par exemple :

   ```
   file:///opt/JNDI-Directory pour UNIX et
   file://c:/temp/ pour Windows.
   ```

   Le répertoire contient le fichier ".bindings" (liaisons) pour le JNDI à partir de fichiers. Ce fichier indique à WebSphere Partner Gateway comment acheminer le document à destination.

   - Pour une destination interne JMS (la destination de votre système dorsal), ceci doit correspondre à la valeur que vous avez indiquée (le chemin de système de fichiers vers le fichier de liaisons) lors de la configuration de

WebSphere Partner Gateway pour JMS (étape 5, à la page 40). Vous pouvez également indiquer le sous-dossier pour le contexte JMS, comme partie de l'URL de fournisseur JMS.

Par exemple, et sans le contexte JMS, vous entreriez `c:/temp/JMS`. Avec le contexte JMS, vous entreriez `c:/temp/JMS/JMS` .

- Pour ses destinations, le partenaire fournira sans doute le fichier ".bindings".

Cette zone est obligatoire.

2. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès à la file d'attente JMS le nécessite.
3. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
4. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
5. Dans la zone **Nombre d'unités d'exécution**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
6. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
7. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option**Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la destination n'a pas été mise en ligne manuellement.
8. Dans la zone **Authentification obligatoire**, indiquez si un nom d'utilisateur et un mot de passe doivent être fournis pour le document. La valeur par défaut est **Non**.
9. Dans la zone **Nom de la fabrique JMS**, saisissez le nom de la classe Java utilisée par le fournisseur JMS pour se connecter à la file d'attente JMS. Cette zone est obligatoire.

   Pour des destinations JMS internes, ce nom doit correspondre à celui que vous avez indiqué par la commande `define qcf`, lors de la création du fichier de liaison (étape 4, à la page 41).

   Si vous avez entré le sous-dossier pour le contexte JMS à l'étape 1, à la page 239, n'entrez ici que le nom de fabrique (par exemple `Hub`). Si vous n'avez pas indiqué le sous-dossier du contexte JMS dans la zone **Adresse**, indiquez ici le sous-dossier, devant le nom de la fabrique (par exemple `JMS/Hub`).
10. Dans la zone **Classe de message JMS**, entrez la classe de message. Toutes les classes de message JMS valides peuvent être sélectionnées, telles que TextMessage ou BytesMessage. Cette zone est obligatoire.
11. Dans la zone **Type de message JMS**, entrez le type de message. Le composant Récepteur déterminant le mappage de type de message JMS, la valeur du type de message JMS est facultative.
12. Dans la zone **Packages d'URL du fournisseur**, entrez le nom des classes (ou du fichier JAR) utilisé par Java pour comprendre l'URL de contexte JMS. Cette zone est facultative. Si vous ne définissez pas de valeur, le chemin au fichier de liaisons est utilisé.

13. Dans la zone **Nom de file d'attente JMS**, entrez le nom de la file d'attente vers laquelle les documents doivent être envoyés. Cette zone est obligatoire.

    Pour des destinations JMS internes, ce nom doit correspondre à celui que vous avez indiqué par la commande `define q`, lors de la création du fichier de liaison (étape 4, à la page 41).

    Si vous avez entré le sous-dossier pour le contexte JMS à l'étape 1, à la page 239, n'entrez ici que le nom de file d'attente (par exemple `outQ`). Dans le cas contraire (si vous n'avez pas indiqué le sous-dossier du contexte JMS dans l'URL du fournisseur JMS), indiquez ici le sous-dossier, devant le nom de la fabrique (par exemple `JMS/outQ`).
14. Dans la zone **Nom de la fabrique du JNDI du JMS**, entrez le nom de la fabrique utilisé pour la connexion au service annuaire. Cette zone est obligatoire. Vous utiliserez probablement la valeur com.sun.jndi.fscontext.RefFSContextFactory, si vous définissez votre configuration JMS pour WebSphere MQ comme indiqué dans la section «Configuration du concentrateur pour le protocole de transport JMS», à la page 39.
15. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 250. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination fichier-répertoire

Pourquoi et quand exécuter cette tâche

Pour créer des destinations fichier-répertoire, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Détails de destination

Pourquoi et quand exécuter cette tâche

Dans la page Détails sur la destination, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Pour les systèmes UNIX et Windows dans lesquels le répertoire de fichiers est sur la même unité que WebSphere Partner Gateway, le format est : file://<*chemin au répertoire cible*>

   Par exemple :

   ```
   file://répertoire_fichier_local
   ```

   où *répertoire_fichier_local* est un répertoire du répertoire racine.

   Si la destination du répertoire de fichier doit être créée sur une unité de Windows, AUTRE QUE l'unité sur laquelle WebSphere Partner Gateway est installé, le chemin est : file:///<*lettre_unité*>:/<*chemin*>
2. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
3. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
4. Dans la zone **Nombre d'unités d'exécution**, indiquez le nombre de documents devant être traités simultanément. La valeur par défaut est 3.
5. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
6. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option**Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la destination n'a pas été mise en ligne manuellement.
7. Si vous souhaitez que le document garde son nom original lorsqu'il est envoyé à sa destination, ne sélectionnez pas **Utiliser un nom de fichier unique**. Vous pouvez également sélectionner cette option si vous souhaitez que WebSphere Partner Gateway affecte un nom au fichier.
8. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 250. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination FTPS

Pourquoi et quand exécuter cette tâche

Pour créer des destinations FTPS, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Remarque : Le mode passif FTPS n'est pas pris en charge. Pour plus d'informations sur la prise en charge du mode passif, reportez-vous à la section «Configuration d'une destination de script FTP», à la page 245.

Détails de destination

Pourquoi et quand exécuter cette tâche

Dans la page Détails sur la destination, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est : ftp://<*nomserveur_ftp*>:<*numéroport*>

   Par exemple :

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Si vous ne définissez pas de numéro de port, le port FTP standard est utilisé.
2. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur FTP sécurisé le nécessite.
3. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
4. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
5. Dans la zone **Nombre d'unités d'exécution**, indiquez le nombre de documents devant être traités simultanément. La valeur par défaut est 3.
6. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
7. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option**Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la destination n'a pas été mise en ligne manuellement.
8. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
9. Si vous souhaitez que le document garde son nom original lorsqu'il est envoyé à sa destination, ne sélectionnez pas **Utiliser un nom de fichier**

unique. Vous pouvez également sélectionner cette option si vous souhaitez que WebSphere Partner Gateway affecte un nom au fichier.

10. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 250. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination SFTP

Pourquoi et quand exécuter cette tâche

La configuration d'une destination SFTP permet d'envoyer des documents depuis le concentrateur à l'adresse IP du partenaire. L'adaptateur se connecter au serveur SFTP et envoie le document au serveur SFTP. Les données de document sont fournies à l'adaptateur sous forme de flux.

Pour créer des destinations SFTP, appliquez la procédure suivante :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez des critères de recherche et cliquez sur **Rechercher** ou cliquez sur **Rechercher** sans saisir aucun critère de recherche pour afficher une liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les caractéristiques** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Caractéristiques de destination

Pourquoi et quand exécuter cette tâche

Dans la page Caractéristiques de destination, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone doit obligatoirement être renseignée.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est En ligne ou Hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.
5. Sélectionnez **SFTP** dans la liste **Transport** .

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, procédez comme suit :

1. Entrez les **Nom d'hôte / IP de l'hôte SFTP**. Il acceptera un maximum de 100 caractères. Vous pouvez également entrer des adresses IP, IPv4 et IPv6.
2. Entrez le **Numéro de port**. La valeur minimale est 1 et la valeur maximale est 65535. La valeur par défaut est 22.
3. Entrez le **Répertoire de sortie**. Il acceptera un maximum de 100 caractères. Il peut contenir des caractères basés sur l'environnement local.
4. Dans la zone **Type d'authentification**, sélectionnez le nom utilisateur/mot de passe ou l'authentification de clé publique.

5. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** pour que la destination soit mise hors ligne (automatiquement) lorsqu'un incident de distribution se produit. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
6. Entrez le **Nom d'utilisateur** et le **Mot de passe** pour nom d'utilisateur/mot de passe. Si le type d'authentification est l'authentification de clé privée, entrez le **Nom d'utilisateur**, le **Fichier de clé privée** et la **Phrase de passe**. Le **Fichier de clé privée** est le chemin du fichier de clé privée au format OpenSSH.
7. Entrez le **Nombre de relances**. Le nombre de fois où le récepteur essaiera de se connecter au serveur SFTP au cas où la connexion échoue.
8. Entrez l'**Intervalle entre les nouvelles tentatives**. Le temps d'attente du récepteur entre les nouveaux essais.
9. Entrez le **Nombre d'unités d'exécution**
10. Le **Codage EIS** correspond au codage du serveur FTP. Utilisez cette valeur pour définir le codage de la connexion de contrôle du serveur FTP.
11. L'option **Activer l'authentification du serveur** peut être activée pour authentifier le serveur auquel la connexion est établie. Si l'authentification du serveur est activée, entrez le chemin du fichier de clés hôte. Le fichier de clés hôte doit être au format OpenSSH.
12. Cliquez sur **Sauvegarder** pour enregistrer la configuration.
13. Entrez la configuration du gestionnaire et cliquez sur **Sauvegarder** pour sauvegarder les détails de la configuration.

Remarque : Redémarrez le serveur correspondant après avoir sauvegardé la configuration :

- En mode simple, redémarrez le serveur bcgserver.
- En mode réparti simple, redémarrez le cluster bcgserver.
- En mode entièrement réparti, redémarrez le cluster BCGDocMgr.

Configuration d'une destination de script FTP

Une destination de script FTP s'exécute d'après la planification que vous avez définie. Le comportement d'une destination de script FTP est régi par un script de commande FTP.

Remarque : Si la base de données est en panne et que Verrouiller l'utilisateur est configuré sur "Oui", la destination de script FTP peut ne pas fonctionner car elle n'obtiendra pas le verrou de la base de données.

Remarque : Sur la plateforme AIX, utilisez le mode passif pour distribuer des documents avec des volumes de transaction élevés. Dans l'opération Transfert de fichier, indiquez le mode passif dans le script qui est utilisé par la destination de script FTP. Vous pouvez utiliser la commande 'passive' ou 'pasv' dans le script. L'utilisation du mode actif génère une erreur.

Création du script FTP

Pourquoi et quand exécuter cette tâche

Pour utiliser une destination de script FTP, vous devez créer un fichier incluant toutes les commandes FTP requises et pouvant être acceptées par votre serveur FTP.

1. Créez un script pour les destinations de façon à indiquer les actions que vous souhaitez effectuer. Le script suivant est un exemple permettant de se connecter au serveur FTP indiqué (à l'aide du nom et du mot de passe spécifiés), d'accéder au répertoire indiqué sur le serveur FTP et d'envoyer tous les fichiers vers le répertoire spécifié sur le serveur.

```
open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
cd %BCGOPTIONx%
mput *
quit
```

   Lorsque la destination est mise en service, les paramètres fictifs (par exemple %BCGSERVERIP%) sont remplacés par les valeurs saisies lors de la création d'une instance spécifique d'une destination de script FTP, comme indiqué dans la table suivante :

Tableau 30. Mappage des paramètres de script et des informations des zones de destination de script FTP

Paramètre de script	**Informations des zones de la destination de script FTP**
%BCGSERVERIP%	IP serveur
%BCGUSERID%	ID utilisateur
%BCGPASSWORD%	Mot de passe
%BCGOPTIONx%	Option*x*, sous **Attributs définis par l'utilisateur**

   Il peut y avoir jusqu'à 10 options définies par l'utilisateur.
2. Enregistrez le fichier.

Commandes de script FTP

Vous pouvez utiliser les commandes suivantes pour créer le script :

- ascii, binary, passive, epsv

  Ces commandes ne sont pas envoyées au serveur FTP. Elles modifient le mode de transfert (ascii, binaire ou passif) vers le serveur FTP.
- cd

  Cette commande permet de passer au répertoire indiqué.
- delete

  Cette commande supprime un fichier du serveur FTP.
- mkdir

  Cette commande permet de créer un répertoire sur le serveur FTP.
- mput

  Cette commande utilise un seul argument, qui décrit un ou plusieurs fichiers à transférer vers le système éloigné. Cet argument peut contenir les caractères génériques standard ('*' et '?') pour identifier plusieurs fichiers.
- mputren

  Cette commande utilise trois arguments de <source>, <temporaire> et <cible> où un astérisque (*) représente le nom de fichier en cours de traitement.

  source Nom du fichier en cours de téléchargement vers le serveur FTP. La valeur attendue est un astérisque (*).

temporaire
Nom du fichier temporaire à utiliser lors du téléchargement de la <source> vers le serveur FTP.

cible Nom de fichier à utiliser pour renommer le <temporaire>. Une fois que ce fichier a été renommé, le fichier temporaire n'existera plus.

Exemples :

mputren * *.tmp *
Cet exemple place le fichier en cours sur le serveur FTP et porte l'extension .tmp. Une fois que le fichier a été placé sur le serveur, vous le renommerez et lui réattribuerez son nom d'origine.

mputren * *.tmp *.ready
Cet exemple place le fichier en cours sur le serveur FTP et porte l'extension .tmp. Une fois que le fichier a été placé sur le serveur, vous le renommerez et lui réattribuerez son nom d'origine avec l'extension .ready.

mputren * *.tmp /complete/*
Cet exemple place le fichier en cours sur le serveur FTP et porte l'extension .tmp. Une fois que le fichier a été placé sur le serveur, vous le renommerez et lui réattribuerez son nom d'origine et il existera dans le répertoire /complete. Le fichier temporaire *.tmp n'existera plus.

mputren * *.tmp /complete/*.final
Cet exemple place le fichier en cours sur le serveur FTP et porte l'extension .tmp. Une fois que le fichier a été placé sur le serveur, vous le renommerez et lui réattribuerez son nom d'origine et il existera dans le répertoire /complete et portera une extension .final. Le fichier temporaire *.tmp n'existera plus.

- open

  Cette commande utilise trois paramètres : l'adresse IP du serveur FTP, le nom de l'utilisateur et un mot de passe. Ces paramètres correspondent aux variables %BCGSERVERIP%, %BCGUSERID% et %BCGPASSWORD%.

  Par conséquent, la première ligne du script de destination FTP doit être :

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

- quit

  Cette commande arrête la connexion à un serveur FTP.

- quote

  Cette commande indique que tout élément après la commande QUOTE doit être envoyé en tant que commande au système éloigné. Elle permet d'envoyer, à un serveur FTP éloigné, des commandes qui ne seraient pas définies dans le protocole FTP standard.

- rmdir

  Cette commande permet de supprimer un répertoire du serveur FTP.

- site

  Cette commande peut servir à lancer des commandes spécifiques à un site sur un système éloigné. Celui-ci détermine si le contenu de la commande est valide.

Destinations de script FTP

Pourquoi et quand exécuter cette tâche

Si vous pensez utiliser des destinations de script FTP, effectuez les tâches suivantes :

Pour créer des destinations de script FTP, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Créer**.

Détails de destination

Pourquoi et quand exécuter cette tâche

Dans la page Détails sur la destination, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination**, procédez comme suit :

1. Entrez l'adresse IP du serveur FTP auquel vous envoyez des documents. La valeur indiquée ici remplacera %BCGSERVERIP% lorsque le script FTP sera exécuté.

   Remarque : Si vous spécifiez une adresse IPv6, indiquez le format numérique et non le nom de la machine ou le nom d'hôte.

   Les exemples d'adresse IPv6 comprennent :

   ```
   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. Indiquez l'ID utilisateur et le mot de passe requis pour accéder au serveur FTP. Les valeurs indiquées ici remplaceront %BCGUSERID% et %BCGPASSWORD% lorsque le script FTP sera exécuté.
3. Si la cible est en mode sécurisé, cliquez sur **Oui** pour **Mode FTPS**. Sinon, utilisez la valeur par défaut, à avoir **Non**.
4. Chargez le fichier script en procédant comme suit :
   a. Cliquez sur **Charger un fichier script**.
   b. Entrez le nom du fichier contenant le script de traitement des documents, ou utilisez **Parcourir** pour accéder au fichier.
   c. Sélectionnez le **Type de codage de fichier script**.
   d. Cliquez sur **Charger le fichier** pour charger le fichier de script dans la zone de texte **Fichier de script actuellement chargé**.

e. Si le fichier script est celui que vous souhaitez utiliser, cliquez sur **Sauvegarder**.
f. Cliquez sur **Fermer la fenêtre**.

5. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la destination doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
6. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la destination doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
7. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
8. Dans la zone **Verrouiller l'utilisateur**, indiquez si la destination demandera un verrouillage pour qu'aucune autre instance d'une destination de script FTP ne puisse accéder simultanément au même répertoire du serveur FTP.

Remarque : Les valeurs **Attributs de script FTP globaux** sont déjà renseignées et ne peuvent être modifiées dans cette page. Pour modifier ces valeurs, utilisez la page Attributs de transport globaux, de la façon indiquée à la section «Définition des valeurs de transport globales», à la page 231.

Attributs définis par l'utilisateur

Pourquoi et quand exécuter cette tâche

Si vous souhaitez indiquer des attributs supplémentaires, exécutez les étapes ci-après. La valeur indiquée pour l'option remplacera %BCGOPTION*x*% lorsque le script FTP sera exécuté (*x* correspond au numéro de l'option).

1. Cliquez sur **Nouveau**.
2. Saisissez une valeur en regard de **Option 1**.
3. Si vous souhaitez spécifier d'autres attributs, cliquez de nouveau sur **Nouveau** et entrez une valeur.
4. Répétez l'étape 3 aussi souvent que nécessaire pour définir tous les attributs.

Prenons un exemple de script FTP :

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

Dans ce cas, %BCGOPTION% est un nom de répertoire.

Planification

Pourquoi et quand exécuter cette tâche

Depuis la section Planification de la page, exécutez les étapes suivantes :

1. Indiquez si vous souhaitez procéder à une planification en fonction d'un intervalle ou du calendrier.
   - Si vous avez sélectionné **Planification en fonction de l'intervalle**, sélectionnez le nombre de secondes qui doivent s'écouler avant que le serveur destination ne soit interrogé (ou acceptez la valeur par défaut).

- Si vous sélectionnez **Planification en fonction du calendrier**, choisissez le type de planification (**Planification quotidienne**, **Planification hebdomadaire**, ou **Planification personnalisée**).
  - Si vous sélectionnez **Planification quotidienne**, choisissez l'heure de la journée à laquelle la destination doit être interrogée.
  - Si vous sélectionnez **Planification hebdomadaire**, choisissez un ou plusieurs jours de la semaine, en plus de l'heure.
  - Si vous sélectionnez **Planification personnalisée**, choisissez l'heure de la journée puis **Intervalle** ou **Sélection des jours** pour indiquer la semaine et le mois. Dans **Intervalle**, indiquez une date de début et de fin Vous pouvez, par exemple, cliquer sur **Lun** et **Ven** si vous souhaitez que le serveur soit interrogé à une certaine heure uniquement les jours ouvrés. L'option **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.

2. Si vous souhaitez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires». Sinon, cliquez sur **Sauvegarder**.

Configuration de gestionnaires

Pourquoi et quand exécuter cette tâche

Vous pouvez modifier deux points de traitement pour une destination - Traitement préalable et Traitement ultérieur.

Aucun gestionnaire n'est fourni par défaut pour l'étape Traitement préalable ou Traitement ultérieur, par conséquent, aucun gestionnaire n'est répertorié par défaut dans la **Liste disponibles**. Si vous avez chargé un gestionnaire, vous pouvez le sélectionner et le déplacer vers la **Liste des éléments configurés**.

Pour appliquer un gestionnaire écrit par l'utilisateur à ces points de configuration, vous devez d'abord télécharger le gestionnaire. Voir le *Guide de configuration du concentrateur* pour la procédure à suivre concernant le téléchargement du gestionnaire. Ensuite, procédez comme suit :

1. Sélectionnez **Traitement préalable** ou **Traitement ultérieur** dans la liste **gestionnaires des points de configuration**.
2. Sélectionnez un gestionnaire dans la **Liste des éléments disponibles** et cliquez sur **Ajouter**.
3. Si vous souhaitez modifier les attributs du gestionnaire, sélectionnez-le dans la **Liste des éléments configurés** et cliquez sur **Configurer**. La liste des attributs pouvant être modifiés s'affiche. Effectuez les modifications nécessaires et cliquez sur **Définir les valeurs**.
4. Cliquez sur **Sauvegarder**.

Vous pouvez modifier davantage la **Liste des éléments configurés** de la façon suivante :

- Supprimez un gestionnaire en le sélectionnant dans la **Liste des éléments configurés** et cliquez sur **Retrait**. Le gestionnaire est déplacé vers la **Liste des éléments disponibles**.
- Modifiez l'ordre dans lequel les gestionnaires sont traités en le sélectionnant et en cliquant sur **Déplacer vers le haut** ou **Déplacer vers le bas**.

Configuration d'une destination pour un transport défini par l'utilisateur

Pourquoi et quand exécuter cette tâche

Si vous entendez télécharger un transport défini par l'utilisateur, effectuez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Destinations**.
3. Cliquez sur **Gérer les types de transport**.
4. Entrez le nom d'un fichier XML définissant le mode de transport (ou naviguez jusqu'au fichier en cliquant sur le bouton **Parcourir**).
5. Utilisez la valeur par défaut **Oui** pour **Valider dans la base de données**. Sélectionnez **Non** si vous testez ce transport avant de le mettre en production.
6. Indiquez si ce fichier doit remplacer un fichier du même nom figurant déjà dans la base de données.
7. Cliquez sur **Télécharger**.

   Remarque : Dans la page Gérer les types de transports, vous pouvez également supprimer un type de transport défini par l'utilisateur. Vous ne pouvez pas supprimer un transport fourni par WebSphere Partner Gateway. Vous ne pouvez pas non plus supprimer un transport défini par l'utilisateur une fois qu'il a été utilisé pour la création d'une destination.
8. Cliquez sur **Créer**
9. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
10. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
11. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
12. Entrez éventuellement une description de la destination.
13. Complétez les zones (qui seront uniques pour chaque transport défini par l'utilisateur) et cliquez sur **Sauvegarder**.

Spécification d'une destination par défaut

Pourquoi et quand exécuter cette tâche

Une fois que vous avez créé des destinations pour le partenaire interne ou le partenaire, sélectionnez l'une des destinations en tant que destination par défaut.

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
4. Cliquez sur **Destinations**.
5. Cliquez sur **Afficher les destinations par défaut**.

   La liste des destinations définies pour le partenaire s'affiche.
6. Dans la liste **Production**, sélectionnez la destination par défaut pour ce partenaire. Vous pouvez également définir des destinations par défaut pour d'autres types de destinations, tels que **Test**.
7. Cliquez sur **Sauvegarder**.

Chapitre 12. Gestion des connexions

Une fois que vous avez créé les fonctions business-to-business des partenaires et les interactions, vous établissez des connexions entre les partenaires internes et externes. Ce chapitre contient les rubriques suivantes :

- «Présentation des connexions»
- «Activation des connexions de partenaire»
- «Spécification ou modification des attributs», à la page 255

Remarque : Pour modifier la configuration de WebSphere Partner Gateway, vous devez toujours utiliser l'instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Présentation des connexions

Configurez une connexion entre des partenaires pour chaque type de document qui sera échangé. Par exemple, vous pouvez avoir plusieurs connexions depuis le partenaire interne vers le même partenaire, car l'empaquetage, le protocole, le type de document, l'action ou la mappe peuvent être différents.

Lorsque vous activez des connexions, vous pouvez spécifier des attributs pour le partenaire source ou cible. Tout attribut que vous définissez au niveau de la connexion est prioritaire sur les attributs que vous définissez au niveau des fonctions business-to-business (pour un partenaire spécifique) ou au niveau de la définition de document.

Pour les documents EDI, XML et ROD, plusieurs connexions sont nécessaires pour chaque échange, s'il implique un enveloppement ou une transformation. Vous pouvez préciser des connexions pour ces types de documents, en choisissant parmi un ensemble de profils associés à la connexion. Voir «Profils de connexion», à la page 204 pour plus d'informations.

Configuration de plusieurs partenaires internes

Dans WebSphere Partner Gateway, le nombre de partenaires internes n'est pas limité. Le partenaire interne par défaut doit être configuré afin de fournir la compatibilité amont pour les documents de service Web et binaires qui passent par les fonctions de prise en charge FTPScript. Pour de plus amples informations sur la configuration de documents de services Web et binaires pour plusieurs partenaires internes, voir le chapitre sur la configuration des types de documents.

Activation des connexions de partenaire

Pourquoi et quand exécuter cette tâche

Les connexions de partenaires contiennent les informations nécessaires à l'échange adéquat de chaque type de document. Un document ne peut pas être routé à moins qu'une connexion existe entre le partenaire interne et l'un de ses partenaires externes.

Le système établit automatiquement des connexions entre les partenaires internes et externes sur la base de leurs fonctions et interactions business-to-business.

Vous devez rechercher ces connexions puis les activer.

Lorsque vous sélectionnez une source et une cible, assurez-vous que la cible est unique.

Pour rechercher des connexions et les activer, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Connexions**. La page Gestion des connexions s'affiche.
2. Sous **Source**, sélectionnez une source. Par exemple, si vous configurez un échange émis par le partenaire interne, sélectionnez le partenaire interne.
3. Sous **Cible**, sélectionnez une cible. Par exemple, si vous configurez un échange qui sera reçu par un partenaire, sélectionnez ce partenaire.

   Remarque : Lorsque vous créez une nouvelle connexion, la source et la cible doivent être uniques.
4. Cliquez sur **Rechercher** pour afficher les connexions qui correspondent à vos critères.

   Remarque : Vous pouvez également utiliser la page Recherche avancée si vous souhaitez entrer des critères de recherche plus détaillés.
5. Pour activer une connexion, cliquez sur **Activation**. La page Gestion des connexions s'affiche de nouveau, cette fois avec la connexion en vert. Cette page affiche l'empaquetage, le protocole et le type de document pour la source et la cible. Elle comporte par ailleurs des boutons que vous pouvez utiliser pour afficher et modifier l'état et les paramètres de la connexion de partenaires.
6. Pour préciser les attributs de la source ou de la cible ou pour sélectionner un profil de connexion, voir «Spécification ou modification des attributs», à la page 255.

Pour un PIP à deux actions, activez la connexion dans les deux sens pour prendre en charge la deuxième action du PIP. Dans ce cas, la source et la cible de la seconde action sont l'opposé de la source et de la cible de la première action.

Dans le cas des documents EDI, XML ou ROD pour lesquels vous avez défini plus d'une interaction, veillez à activer toutes les connexions associées aux interactions.

Spécification ou modification des attributs

Pourquoi et quand exécuter cette tâche

Lorsque vous activez la connexion, vous pouvez définir ou modifier des attributs. Pour préciser ou modifier les attributs de cette connexion :

1. Cliquez sur **Attributs** pour consulter ou modifier les valeurs des attributs.

   Par exemple, supposons que le partenaire interne envoie un document empaqueté None à un partenaire. Le partenaire va recevoir le document empaqueté en tant que AS. Il est possible que le partenaire interne ait plusieurs ID Métier qui y soient associés. Pour indiquer à WebSphere Partner Gateway l'ID à utiliser :

   a. Cliquez sur **Attributs** sur la partie Source de la connexion.
   b. Lorsque la page des attributs de connexion s'affiche, développez le dossier **None**.
   c. Dans la liste **Mettre à jour** sélectionnez l'ID AS que vous voulez envoyer au partenaire.
   d. Cliquez sur **Sauvegarder**.

   Remarque : Si vous avez indiqué précédemment un ID AS (sur la page des fonctions business-to-business, par exemple), la valeur entrée supplante toute valeur antérieure.

   Un autre exemple de configuration d'attribut consiste à saisir une valeur pour l'adresse MDN lorsque vous recevez d'un partenaire des documents empaquetés en tant que AS. L'adresse indique où la MDN est fournie.
2. Cliquez sur **Actions** pour consulter ou modifier une action ou une mappe de transformation associée à cette connexion. Toute valeur modifiée ici supplante toute autre valeur définie pour l'action ou la mappe.
3. Cliquez sur **Destinations** si vous voulez voir ou modifier la destination source ou cible.
4. Si le bouton **Ajouter profil de connexion** et la liste **Profils actifs** s'affichent, vous pouvez associer cette connexion à un profil particulier défini précédemment.

Les attributs que vous définissez au niveau de la connexion sont prioritaires sur tout attribut que vous définissez au niveau du protocole ou du type de document. Si l'attribut est associé au package, au protocole et au type de document, la valeur du type de document écrasera la valeur définie pour le package et le protocole.

Chapitre 13. Activation de la sécurité pour les échanges de documents

Avec WebSphere Partner Gateway, vous pouvez installer et utiliser plusieurs types de certificats pour sécuriser les transactions entrantes et sortantes. Ce chapitre contient les rubriques suivantes :

Dans WebSphere Partner Gateway, les certificats et les protocoles de sécurité vous permettent de :

- Vérifier l'identité de l'expéditeur du document
- Vérifier que le document n'a pas été altéré lors de son transfert
- Empêcher tout autre utilisateur de voir le contenu du document
- Vérifier que l'expéditeur du document dispose des autorisations nécessaires.

Remarque : Pour modifier la configuration de WebSphere Partner Gateway, vous devez toujours utiliser l'instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Présentation de la sécurité

Mécanismes et protocoles de sécurité utilisés dans WebSphere Partner Gateway

En fonction du protocole de gestion, WebSphere Partner Gateway utilise des certificats afin d'activer les mécanismes suivants et de garantir la sécurité de vos échanges de documents :

Chiffrement et déchiffrement

Le chiffrement consiste à modifier les données de manière à ce qu'elles soient illisibles tant qu'elles n'ont pas été déchiffrées. WebSphere Partner Gateway utilise un système de chiffrement à clé publique pour sécuriser les communications entre les partenaires et le concentrateur. Différents protocoles de gestion, comme AS2 ou RosettaNet, ont des exigences en matière de chiffrement. Le protocole SSL utilise aussi le chiffrement. Dans ce chapitre, sauf mention contraire, le terme *chiffrement* s'applique aux protocoles de gestion.

Le déchiffrement permet de modifier les données chiffrées de manière à ce qu'elles soient lisibles. Cette action est utilisée pour les documents entrants.

WebSphere Partner Gateway peut envoyer des données OpenPGP chiffrées. Le paquet de données reçu est déchiffré à l'aide de la clé privée. S'il est prévu que l'envoi de documents soit toujours chiffré, définissez l'attribut **Chiffrement obligatoire** sur `Oui` du côté cible de la connexion. Si le document chiffré est prévu pour contenir le paquet de code de détection des modifications, définissez **Détection des modifications** sur `True (vrai)` du côté cible de la connexion. Si vous recevez des données chiffrées avec protection de l'intégrité, après le déchiffrement, l'intégrité des données est vérifiée à l'aide du paquet de code de détection des modifications. Le dernier paquet déchiffré dans les données déchiffrées doit être un paquet de code de détection des modifications. Dans un tel scénario, les données chiffrées se composent du paquet de données à intégrité protégée chiffrées de façon symétrique, ce qui permet que l'intégrité des messages soit vérifiée. Vous devez définir les attributs de chiffrement du côté cible de la connexion. Pour le paquet OpenPGP, RFC 4880 est pris en charge. Si vous devez envoyer des données chiffrées avec protection de l'intégrité, définissez la **Détection des modifications** sur `True (vrai)` et sélectionnez les préférences d'algorithme symétrique. Cette fonctionnalité est définie dans RFC 4880 uniquement.

Compression

Pendant l'envoi d'un document, à l'étape de l'empaquetage, les données doivent être compressées de la même manière que selon la préférence d'algorithme de compression définie dans la connexion de la cible. Lorsque vous recevez un message compressé, il est décompacté. S'il est prévu que l'envoi de documents soit toujours compressé, définissez l'attribut **Compression obligatoire** sur `Oui` du côté cible de la connexion. Pour le paquet OpenPGP, RFC 4880 est pris en charge.

Chiffrement et compression

Lorsqu'un document doit être chiffré et compressé, définissez tous les attributs d'objet de routage pour le chiffrement et la compression du côté cible de la connexion. Le chiffrement s'effectue conformément à RFC 4880. Lorsque vous recevez un message chiffré et compressé, un déchiffrement est effectué. Le déchiffrement produit un paquet de données compressées auquel la décompression est appliquée. Pendant l'envoi des données

chiffrées avec protection de l'intégrité, définissez l'attribut Détection des modifications du côté cible de la connexion.

Signature numérique et Vérification de signature numérique
La signature numérique permet de vérifier l'identité de l'expéditeur d'un document et de s'assurer que le document n'a pas été altéré pendant le transfert. Ce mécanisme contribue également à garantir l'irréfutabilité, c'est-à-dire l'impossibilité pour l'expéditeur de nier avoir créé et envoyé le message. De la même manière, le partenaire ne peut pas nier avoir reçu un message.

Remarque : Les informations d'irréfutabilité sont obtenues dans les paramètres de connexion partenaire. Ces derniers sont obtenus suite à une recherche de connexion partenaire ayant réussie. Par défaut, l'irréfutabilité est définie sur "Oui", ce qui signifie que si les informations sont indisponibles dans la connexion partenaire pour quelque raison que ce soit, le document sera placé dans le magasin d'irréfutabilité.

SSL SSL est un protocole couramment utilisé pour la gestion de la sécurité sur Internet. Le protocole SSL sécurise les connexions en permettant à deux applications reliées par une connexion réseau de s'authentifier mutuellement et en chiffrant les données pour assurer la confidentialité. Le chiffrement est indépendant du type de données. L'approche SSL est utilisée pour différents protocoles comme HTTP ou FTP.

Authentification de base
Lorsqu'un message entrant est envoyé sur HTTP ou HTTPS, le récepteur peut authentifier le partenaire expéditeur par le biais des droits d'accès de l'authentification de base. L'ID utilisateur et le mot de passe sont passés dans l'en-tête HTTP. Le mot de passe étant lui aussi envoyé, l'authentification de base doit être utilisé avec SSL/TLS pour garantir le chiffrement des en-têtes. L'authentification est fournie utilisant soit Business ID/username:password ou Username:password au format codé Base64. La valeur dans l'en-tête HTTP est uniquement prise en compte si **Activer l'authentification de base** est défini sur vrai. Sélectionnez l'authentification de base dans la page de la console sur les caractéristiques du récepteur pour la définir sur la valeur Vrai.

Si l'authentification échoue, la réponse de l'échec d'authentification est renvoyée à l'expéditeur. Dans le cas contraire, le document est envoyé pour traitement. Dans le cas d'authentification client SSL, les ID entreprise du partenaire expéditeur est identifié. Une fois le document reçu, le destinataire vérifie si le certificat est associé à des partenaires, sinon une erreur de document se produit. En ce qui concerne la compatibilité amont, définissez l'indicateur **Activer l'authentification de base** sur "Non" u niveau du destinataire pendant que vous envoyez un message SOAP avec l'authentification de base. A moins que l'authentification du document n'échoue au niveau du destinataire, vous pouvez voir le document dans l'afficheur de document. L'authentification de base est prise en charge pour les documents suivants :

- Documents EDI/XML
- Documents AS2 avec charge binaire/EDI/XML
- Demande de services Web
- Message Rosettanet
- Message ebMS

La sécurité peut être activée au niveau du mécanisme de transport ou du protocole de gestion. L'authentification des utilisateurs au niveau du destinataire prend en charge les documents binaires des partenaires externes sur HTTP. Le partenaire expéditeur est identifié en utilisant soit les droits d'accès de l'authentification de base, soit les droits d'accès de l'authentification client SSL.

Certificats et mécanismes de sécurité

Les certificats sont au coeur des trois approches de sécurité : chiffrement, signatures numériques et SSL. Ils permettent la mise en oeuvre de ces approches dans WebSphere Partner Gateway. L'utilisation d'un certificat garantit la sécurité des documents pendant leur transmission.

Chaque partenaire a un ou plusieurs certificats pour échanger des documents avec WebSphere Partner Gateway. WebSphere Partner Gateway, représenté par l'opérateur du concentrateur, a un ou plusieurs certificats pour échanger des documents avec le partenaire.

Remarque : Les certificats utilisés pour un partenaire ou pour l'opérateur du concentrateur s'appliquent à tous les documents. Les certificats ne varient pas en fonction du type de document.

Certificats et chiffrement

Un certificat contient la partie clé publique d'une paire de clés publique/privée liées par une relation mathématique. La clé publique “verrouille” ou chiffre un document avant qu'il ne soit envoyé, de telle sorte que seule la clé privée puisse “déverrouiller” ou déchiffrer ce document. Une clé publique est appelée clé publique car vous la partagez avec des partenaires qui vous envoient des documents chiffrés. En revanche, la clé privée vous est propre et vous permet de les déchiffrer. Un certificat contient la clé publique et celle-ci est associée à un nom d'objet qui correspond au nom de l'entité finale à laquelle appartient le certificat.

Les certificats sont générés par le partenaire et peuvent être auto-signés par le partenaire ou émis par une autorité de certification. Un certificat émis par une autorité de certification est un certificat demandé par un partenaire via une requête de certificat serveur (CSR) et envoyé par une autorité de certification. Ce type de certificat est signé par l'autorité de certification et non par le partenaire. Chaque partenaire dispose d'au moins un certificat pour envoyer ou recevoir des documents.

Le chiffrement des documents de gestion s'applique uniquement si la norme de gestion prend en charge le chiffrement. Toutes les normes ne prennent pas en charge le chiffrement. Pour celles qui le prennent en charge, chaque norme a une manière différente d'appliquer le chiffrement. WebSphere Partner Gateway tient compte des différences entre les normes et du mode d'application du chiffrement.

Si WebSphere Partner Gateway envoie un document à un partenaire, le certificat de ce partenaire est utilisé pour chiffrer le document. Ainsi, seul le partenaire peut en lire le contenu en déchiffrant le document à l'aide de sa clé privée. Le certificat utilisé est le certificat de chiffrement chargé dans WebSphere Partner Gateway pour ce partenaire.

Si un partenaire envoie un document à WebSphere Partner Gateway, ce dernier utilise le certificat de l'opérateur du concentrateur pour chiffrer le document. Ainsi, seul l'opérateur du concentrateur qui détient la clé privée peut en lire le contenu en déchiffrant le document. La clé privée utilisée est celle qui a été chargée pour l'opérateur du concentrateur via l'option Charger PKCS12. Notez que le certificat

de l'opérateur du concentrateur doit être remis au partenaire par l'administrateur.

Remarques :

1. WebSphere Partner Gateway accepte les algorithmes RC2 et TripleDES. L'algorithme RC5 n'est pas pris en charge. Si vous l'utilisiez dans une version précédente, passez à l'un des algorithmes pris en charge.
2. WebSphere Partner Gateway prend également en charge les algorithmes suivants :
   - AES, TripleDES et RC2 : pour les documents ebMS envoyés et reçus.
   - TripleDES et RC2 : pour les documents RNIF.
   - DES : pour ebMS, mais il est recommandé d'utiliser des algorithmes plus puissants comme RC2, TripleDES ou AES.

   Vous pouvez définir ces algorithmes dans la console WebSphere Partner Gateway (Administration système > Administration du gestionnaire de documents > vue Sécurité) ou via l'API Security Service dans les exits utilisateur. Pour plus d'informations sur les propriétés de sécurité, reportez-vous au *Guide d'administration de WebSphere Partner Gateway*. Pour plus d'informations sur le service de sécurité, reportez-vous au *Guide du programmeur de WebSphere Partner Gateway*.

Procédure de base

Pour recevoir un document chiffré, vous devez effectuer les étapes de base décrites ci-dessous. Pour connaître la procédure complète, voir «Utilisation de certificats pour activer le chiffrement et le déchiffrement», à la page 270.

1. Procurez-vous une paire de clés privée/publique en la générant vous-même ou en la demandant à une autorité de certification.
2. Chargez la clé privée sur votre serveur WebSphere Partner Gateway, sous l'opérateur du concentrateur (la clé peut être utilisée par tous les partenaires internes) ou Partenaire interne (la clé peut uniquement être utilisée par ce partenaire en question), afin que le serveur puisse déchiffrer les documents entrants.
3. Donnez le certificat public à votre partenaire d'échanges, afin qu'il puisse charger ce certificat sur le serveur et chiffrer les documents avant de vous les envoyer.

Une fois la procédure terminée, ce partenaire peut utiliser votre certificat pour vous envoyer des documents chiffrés de telle manière que vous seul puissiez les déchiffrer. Pour envoyer à vos partenaires des documents chiffrés, vous devez inverser cette procédure, c'est-à-dire charger leurs certificats et les utiliser pour chiffrer les documents que vous leur envoyez.

Certificats et signature numérique

WebSphere Partner Gateway prend en charge la signature numérique comme le demandent les protocoles business-to-business. Les certificats pour document avec signature numérique s'utilisent comme les certificats de chiffrement, mais la procédure est inversée. Vous devez créer le certificat pour envoyer un document avec une signature numérique à vos partenaires et non pas l'inverse.

Les signatures numériques permettent de vérifier l'identité de l'expéditeur du document et de s'assurer que le document n'a pas été altéré lors de son transfert. Elles peuvent être utilisées uniquement si la norme de gestion prend en charge les signatures numériques. Toutes les normes ne prennent pas en charge les signatures numériques. Pour celles qui les prennent en charge, chaque norme a une manière

différente d'appliquer les signatures numériques. WebSphere Partner Gateway tient compte des différences entre les normes et du mode d'application des signatures numériques.

Si WebSphere Partner Gateway envoie un document à un partenaire, la clé privée de l'opérateur du concentrateur, chargée via l'option Charger PKCS12, est utilisée pour signer le document. Le partenaire utilise le certificat de l'opérateur du concentrateur pour vérifier que WebSphere Partner Gateway a bien signé le document. Si la clé privée de l'opérateur du concentrateur n'a pas été utilisée pour signer le document, le certificat de l'opérateur du concentrateur détenu par le partenaire ne permettra pas de vérifier les signatures. Notez que le certificat de l'opérateur du concentrateur doit être remis au partenaire par l'administrateur.

Si un partenaire envoie un document à WebSphere Partner Gateway, ce dernier utilise le certificat de signature numérique du partenaire pour vérifier que le partenaire a bien signé le document. Si la clé privée du partenaire n'a pas été utilisée pour signer le document, le certificat détenu par WebSphere Partner Gateway pour ce partenaire ne permettra pas de vérifier la signature.

Procédure de base :

Pour envoyer un document chiffré numériquement, vous devez effectuer les étapes de base décrites ci-dessous. Pour connaître la procédure complète, voir «Utilisation de certificats pour activer la signature numérique», à la page 275.

1. Procurez-vous une paire de clés privée/publique en la générant vous-même ou en la demandant à une autorité de certification.
2. Chargez la clé privée sur votre serveur WebSphere Partner Gateway, sous l'opérateur du concentrateur, afin que le serveur puisse signer les documents à envoyer.
3. Donnez le certificat public à votre partenaire d'échanges, afin qu'il puisse charger ce certificat sur le serveur et vérifier les documents que vous lui envoyez.

Une fois que vous avez effectué cette procédure, vous pouvez envoyer des documents signés numériquement à l'aide de votre clé privée, ce qui permet à votre partenaire de s'assurer que vous êtes bien l'expéditeur du document. Pour recevoir des documents signés numériquement de vos partenaires, vous devez inverser cette procédure, c'est-à-dire charger leurs certificats et les utiliser pour vérifier leur origine.

Certificats et SSL/TLS

Lorsque vous envoyez des documents, vous pouvez utiliser le protocole SSL pour chiffrer vos documents, de telle sorte que seul le destinataire puisse les lire, garantissant ainsi la confidentialité.

Le protocole SSL implique la notion de *client* et *serveur*. Un client se connecte à un serveur pour envoyer un document à ce serveur. Lorsqu'un client se connecte au serveur, ce dernier envoie au client un certificat à utiliser pour chiffrer le document. Ce certificat du serveur participe également à l'authentification du serveur : cela signifie que le serveur utilise ce certificat pour s'authentifier auprès des clients. Il peut arriver que le serveur demande également un certificat au client. Cette procédure est appelée authentification du client et permet au serveur de s'assurer qu'il connaît ce client.

Lorsque WebSphere Partner Gateway envoie un document à un partenaire, WebSphere Partner Gateway joue le rôle du client, et le partenaire celui du serveur (le document est envoyé au serveur du partenaire).

Remarque : Le serveur du partenaire est la destination définie dans WebSphere Partner Gateway pour ce partenaire.

Lorsque le partenaire envoie un document à WebSphere Partner Gateway, le partenaire est le client et WebSphere Partner Gateway est le serveur.

Remarque : Il s'agit du destinataire qui a été défini dans WebSphere Partner Gateway.

Lorsqu'un partenaire envoie un document à WebSphere Partner Gateway via SSL, la véritable identité de ce partenaire n'est pas connue. Si l'authentification du client est utilisée, l'identité du partenaire n'est pas connue non plus. Toutefois, une chose est sûre : ce partenaire est autorisé à envoyer des documents à WebSphere Partner Gateway. WebSphere Partner Gateway dispose également d'une fonction supplémentaire permettant d'identifier le partenaire à partir du certificat d'authentification du client fourni par le partenaire.

Si WebSphere Partner Gateway envoie un document à un partenaire, le certificat de ce partenaire est utilisé pour chiffrer le document. Ainsi, seul le partenaire peut en lire le contenu en déchiffrant le document à l'aide de sa clé privée. Lors de l'exécution du protocole SSL, le partenaire envoie à WebSphere Partner Gateway le certificat à utiliser pour le chiffrement. WebSphere Partner Gateway vérifie que ce certificat est valide en générant et en validant le chemin de certification grâce aux certificats chargés en tant que certificats Racine/Intermédiaire sous l'opérateur du concentrateur.

Une procédure facultative du protocole SSL, appelée authentification du client, permet de valider l'expéditeur : le partenaire demande alors un certificat à WebSphere Partner Gateway. WebSphere Partner Gateway envoie le certificat d'authentification du client chargé sous l'opérateur du concentrateur. Notez que le certificat de l'opérateur du concentrateur pour l'authentification du client doit être remis au partenaire par l'administrateur. Si le certificat d'authentification du client est auto-signé, alors ce dernier doit être remis au partenaire. Si le certificat d'authentification du client est émis par une autorité de certification, alors ce certificat devra être remis au partenaire, s'il ne dispose pas déjà d'un exemplaire.

Si un *partenaire* envoie un document à WebSphere Partner Gateway via SSL, le certificat WebSphere Partner Gateway est utilisé pour chiffrer le document. Ainsi, seul WebSphere Partner Gateway peut en lire le contenu en déchiffrant le document à l'aide de sa clé privée. Lors de l'exécution du protocole SSL, WebSphere Partner Gateway envoie au partenaire le certificat à utiliser pour le chiffrement. Le partenaire vérifie que le certificat est valide en le comparant avec le certificat que l'administrateur lui a fourni. Une procédure facultative du protocole SSL, appelée authentification du client, permet de valider l'expéditeur : WebSphere Partner Gateway demande alors un certificat au partenaire. Le partenaire envoie le certificat d'authentification du client à WebSphere Partner Gateway : ce certificat sera comparé à celui que le partenaire avait auparavant transmis à l'administrateur.

Remarque : Pour recevoir des documents provenant de partenaires via SSL, WebSphere Partner Gateway utilise les fonctions sous-jacentes de WebSphere Application Server. Par conséquent, les certificats utilisés lors de l'exécution ne sont

pas chargés à l'aide de la console de WebSphere Partner Gateway, mais dans le fichier de clés et le magasin de relations de confiance WebSphere Application Server.

Avec l'authentification du client, WebSphere Partner Gateway procède à une identification supplémentaire du partenaire, en dehors du transport SSL. Le certificat d'authentification du client fourni par le partenaire est transmis à WebSphere Partner Gateway, qui le compare au certificat chargé pour le client SSL de ce partenaire, afin d'identifier ce dernier.

Une connexion SSL HTTP est toujours lancée par le client avec une URL commençant par https:// au lieu de http://. Une connexion SSL commence par une négociation. Durant cette étape, les applications échangent des certificats, se mettent d'accord sur les algorithmes de chiffrement à utiliser et génèrent des clés de chiffrement pour le reste de la session.

Procédures de base

Pour *envoyer* un document via SSL, vous devez effectuer les étapes de base décrites ci-dessous. Pour connaître la procédure complète, voir «Utilisation de certificats pour activer le protocole SSL», à la page 280.

1. Procurez-vous un certificat auprès de votre partenaire et chargez-le dans le magasin de relations de confiance de WebSphere Application Server.
2. Pour l'authentification du client, procurez-vous une paire de clés privée/publique en la générant vous-même ou en la demandant à une autorité de certification.
3. Chargez la clé privée et le certificat public dans votre fichier de clés WebSphere Application Server.
4. Donnez le certificat public à votre partenaire d'échanges, afin qu'il puisse charger ce certificat sur le serveur et vérifier le certificat d'authentification du client que vous lui envoyez dans le cadre de vos communications SSL.

Pour *recevoir* un document via SSL, vous devez effectuer les étapes de base décrites ci-dessous. Pour connaître la procédure complète, voir «Utilisation de certificats pour activer le protocole SSL», à la page 280.

1. Procurez-vous une paire de clés privée/publique en la générant vous-même ou en la demandant à une autorité de certification.
2. Chargez la clé privée et le certificat public dans votre fichier de clés WebSphere Application Server.
3. Donnez le certificat public à votre partenaire d'échanges, afin qu'il puisse charger ce certificat sur le serveur et vérifier le certificat serveur que vous lui envoyez dans le cadre de vos communications SSL.
4. Pour l'authentification du client, procurez-vous un certificat auprès de votre partenaire et chargez-le dans le magasin de relations de confiance de WebSphere Application Server. Ce certificat sera utilisé dans le cadre des communications SSL.
5. Pour identifier le partenaire à partir du certificat d'authentification du client dans la console WebSphere Partner Gateway, chargez le certificat du partenaire sous l'authentification client du partenaire.

Stockage des certificats dans des fichiers de clés et des magasins de relations de confiance

WebSphere Partner Gateway peut stocker les certificats de 2 façons différentes. Pour les documents envoyés à WebSphere Partner Gateway par un partenaire via

SSL, les certificats sont stockés dans le fichier de clés et dans le magasin de relations de confiance WebSphere Application Server. Les magasins de relations de confiance permettent de stocker des certificats authentifiés, utilisés pour certifier la validité d'un certificat reçu d'un partenaire. Les fichiers de clés permettent de stocker les clés publiques et privées de l'opérateur du concentrateur WebSphere Partner Gateway. Les certificats utilisés pour la sécurité des documents sont chargés via la console WebSphere Partner Gateway. Cette section décrit le fichier de clés et le magasin de relations de confiance utilisés avec WebSphere Application Server. Lorsque vous installez WebSphere Partner Gateway, un fichier de clés et un magasin de relations de confiance sont créés pour le serveur WebSphere Application Server sur lequel le récepteur et la console sont installés.

- Un magasin de clés est un fichier contenant vos clés publiques et privées.
- Un magasin de relations de confiance est un fichier de base de données contenant les clés publiques pour les certificats d'autorités de certification et auto-signés de vos partenaires. La clé publique est stockée comme un certificat de signataire. Pour une autorité de certification commerciale, le certificat de CA racine est ajouté. Etant donné que le magasin de relations de confiance ne contient pas votre clé privée, il peut être accessible à un plus large public que le fichier de clés.
- L'utilitaire iKeyman permet d'administrer le fichier de clés et le magasin de relations de confiance. Il est décrit dans les sections pour lesquelles il est nécessaire.

  Remarque : Vous pouvez également utiliser la console d'administration de WebSphere Application Server pour gérer les certificats, les fichiers de clés et les magasins de relations de confiance du récepteur et de la console. Pour plus de détails sur la gestion des certificats et des fichiers de clés à l'aide de la console d'administration de WebSphere Application Server, consultez l'article "Sécurisation des applications et de leur environnement" dans le centre de documentation de WebSphere Application Server.

Par défaut, un fichier de clés et un magasin de relations de confiance sont créés dans le répertoire *<ProductDir>*/common/security/keystore. Leurs noms sont les suivants :

- bcgSecurity.jks
- bcgSecurityTrust.jks

Modification du mot de passe par défaut

Le mot de passe par défaut permettant d'accéder aux magasins est WebAS. L'application WebSphere Application Server est configurée pour utiliser ces magasins. Vous pouvez utiliser l'utilitaire iKeyman pour changer le mot de passe. Vous pouvez également utiliser une commande de l'outil de clé pour changer le mot de passe du fichier de clés. Sous UNIX, la commande sera la suivante :

```
/<WAS_Installation_Dir>/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
 -storepass $CURRENT_PASSWORD$ -storetype JKS
```

Sous Windows, utilisez la commande précédente mais utilisez plutôt des barres obliques inverses ("\") et des noms d'unités.

Si les mots de passe des magasins de clés sont changés, la configuration de chaque instance de WebSphere Application Server doit l'être également. Pour cela, vous pouvez utiliser le script bcgChgPassword.jacl. Pour l'instance de console, naviguez jusqu'au répertoire suivant :

```
/<ProductDir>/bin
```

et exécutez la commande suivante :

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/
bcgChgPassword.jacl -conntype NONE
```

Répétez cette commande pour les instances de WebSphere Application Server du récepteur et du gestionnaire de documents.

Remarque : Pour Windows, utilisez `bcgwsadmin.bat` au lieu de `./bcgwsadmin.sh`.

Vous êtes alors invité à saisir le nouveau mot de passe.

Remplacement d'un certificat arrivé à expiration

Si un certificat du magasin de relations de confiance arrive à expiration, vous devez le remplacer par un nouveau certificat de la façon suivante :

1. Lancez iKeyman, s'il n'est pas déjà en cours d'exécution.
2. Ouvrez le fichier du magasin de relations de confiance.
3. Saisissez le mot de passe et cliquez sur **OK**.
4. Dans le menu, sélectionnez **Signer les certificats**.
5. Cliquez sur le bouton **Ajouter**.
6. Sélectionnez un **type de donnés**, tel que "données ASCII codées en base 64".

   Ce type de données doit correspondre au type de données du certificat importé.
7. Saisissez un nom de fichier de certificat et un emplacement pour le certificat numérique racine de l'autorité de certification ou cliquez sur **Parcourir** pour sélectionner le nom et l'emplacement.
8. Cliquez sur **OK**.
9. Saisissez un libellé pour le certificat importé.
10. Cliquez sur **OK**.

Utilisation de chaînes de certificats

Une chaîne de certificats se compose des certificats d'un partenaire et de tout certificat utilisé pour les authentifier. Par exemple, si une autorité de certification a été utilisée pour créer le certificat du partenaire, cette autorité de certification peut avoir elle-même été certifiée par une autre autorité de certification. La hiérarchie des relations de confiance commence au CA *racine* (l'ancrage des relations de confiance). Le certificat numérique du CA racine est auto-signé, c'est-à-dire qu'il utilise sa propre clé privée pour signer le certificat numérique. Tous les certificats entre l'ancrage sécurisé et le certificat du partenaire (le certificat cible) sont des certificats *intermédiaires*.

Pour tout certificat émis par le CA, il faut ajouter tous les certificats de la hiérarchie. Par exemple, pour une chaîne de certificats dans laquelle A (l'ancrage des relations de confiance) est l'émetteur de B, et B l'émetteur de C (le certificat cible), les trois certificats doivent être téléchargés en tant que certificats CA.

WebSphere Partner Gateway traite tous les certificats auto-signés en tant qu'ancrages de relations de confiance. Le certificat auto-signé peut être du type CA ou généré par le partenaire.

Pour les communications SSL entrantes, tous les certificats racine (ancrage sécurisé) et les certificats intermédiaires sont stockés dans le magasin de relations de confiance WebSphere Application Server, comme indiqué précédemment. Pour tous les certificats des partenaires, les certificats racine (ancrage sécurisé) et les certificats intermédiaires sont chargés sous l'opérateur du concentrateur.

Utilisation des certificats principaux et secondaires

Vous pouvez créer plusieurs certificats d'un type donné et en désigner un en tant que certificat principal et l'autre en tant que certificat secondaire. Si le certificat principal expire ou est inutilisable, WebSphere Partner Gateway bascule sur le certificat secondaire.

Remarque : Vous pouvez utiliser cette option pour effectuer une transition entre un certificat ancien et un certificat récent sans interrompre le serveur.
La console de communauté sert à préciser celui qui est principal et celui qui est secondaire.

Il est possible de définir des certificats principaux et secondaires pour les certificats suivants :

- Certificat de chiffrement d'un partenaire
- Certificat de signature de l'opérateur du concentrateur
- Certificat client SSL pour l'opérateur du concentrateur

Modification de la puissance du chiffrement

L'environnement Java Runtime Environment (JRE) fourni avec WebSphere Partner Gateway impose des restrictions concernant les algorithmes cryptographiques et les longueurs de chiffrement maximales autorisés. Par exemple, les règles imposent des limites de longueur qui ont des répercussions sur les performances des clés de chiffrement. Ces limitations sont spécifiées dans les fichiers nommés *fichiers de règle de juridiction*. La longueur maximum possible est de 2048 octets.

Si vous souhaitez prendre en charge des certificats avec une taille de clé supérieure à 2048 octets, utilisez la version non limitée des fichiers de règle de juridiction. Vous pouvez préciser que vous souhaitez appliquer une règle non limitée plus efficace, en installant de nouveaux fichiers de règle dans un sous-répertoire de l'environnement JRE installé.

Il existe également des restrictions sur les algorithmes à clé symétrique, tels que 3DES. S'il vous faut un algorithme fort à clé symétrique, le fait de remplacer les fichiers de règle de juridiction lèvera également les restrictions concernant les clés symétriques. Par exemple, si vous utilisez l'algorithme AES, alors des fichiers de règles de cryptographie non restreinte seront requis. Référez-vous au lien http://www.ibm.com/developerworks/java/jdk/security/50 pour plus de détails.

Cependant, en raison des restrictions du contrôle d'importation, les fichiers de règle de juridiction fournis avec IBM SDK pour le kit de développement Java 5 permettent d'utiliser une cryptographie **puissante** mais limitée. Le tableau suivant présente les tailles de clé maximales autorisées par cette version **puissante** des fichiers de règles de juridiction :

Tableau 31. Taille de clé maximale utilisée des algorithmes utilisés dans les fichiers de règles de juridiction puissants

Algorithme	Taille de clé maximale
DES	64

Tableau 31. Taille de clé maximale utilisée des algorithmes utilisés dans les fichiers de règles de juridiction puissants (suite)

Algorithme	Taille de clé maximale
DESede	112 (effectif) ou 168 (effectif)
RC2	128
RSA	2048
* (tous les autres)	128

Remarque : Une exception 'Encryption failure XMLEncryptionException' est survenue au cours du chiffrement d'un message ebMS routé possédant les paramètres suivants :

- Algorithme de chiffrement : aes-192-cbc ou aes-256-cbc
- Protocole de chiffrement : chiffrement XML

Pour résoudre ce problème, si l'action est autorisée, installez des fichiers de règles de cryptographie non restreints.

Instructions d'installation pour les systèmes d'exploitation Windows, Linux et AIX

Pour installer des fichiers de règle de juridiction dans WebSphere Partner Gateway, procédez comme suit :

1. Téléchargez les fichiers de règle de juridiction non limités depuis le lien **IBM SDK Policy files** du site http://www.ibm.com/developerworks/java/jdk/security/50/.
2. Décompressez le fichier téléchargé dans un dossier temporaire.
3. Copiez les fichiers local_policy.jar et US_export_policy.jar depuis ce dossier temporaire.
4. Arrêtez tous les serveurs qui sont hébergés par l'instance de WebSphere Application Server et que vous êtes en train de configurer.
5. Ouvrez le dossier <*WASInstallationDir*>\java\jre\lib\security.
6. Renommez les fichiers local_policy.jar et US_export_policy.jar en local_policy.jar.bak et US_export_policy.jar.bak.
7. Collez les fichiers JAR copiés à l'étape 3 dans le dossier <*WASInstallationDir*>\was\java\jre\lib\security.
8. Redémarrez les serveurs qui sont hébergés par l'instance de WebSphere Application Server et que vous venez de configurer.

Ces étapes s'appliquent à toutes les installations de WebSphere Application Server dans lesquelles les applications de WebSphere Partner Gateway sont installées.

Instructions d'installation pour les systèmes d'exploitation HP-UX et Solaris

Pour les plateformes HP-UX et Solaris, les instructions suivantes s'appliquent :

1. Téléchargez les fichiers de règle de juridiction non limités depuis le lien **IBM SDK Policy files** du site http://www.ibm.com/developerworks/java/jdk/security/50/.
2. Décompressez le fichier téléchargé dans un dossier temporaire.
3. Arrêtez tous les serveurs qui sont hébergés par l'instance de WebSphere Application Server et que vous êtes en train de configurer.

4. Ouvrez le dossier <*WASInstallationDir*>\java\jre\lib\security.
5. Renommez les fichiers local_policy.jar et US_export_policy.jar en local_policy.jar.bak et US_export_policy.jar.bak.
6. Copiez les fichiers local_policy.jar et US_export_policy.jar du dossier temporaire vers le dossier <*WASInstallationDir*>\java\jre\lib\security.
7. Redémarrez les serveurs qui sont hébergés par l'instance de WebSphere Application Server et que vous venez de configurer.

Ces étapes s'appliquent à toutes les installations de WebSphere Application Server dans lesquelles les applications de WebSphere Partner Gateway sont installées.

Configuration du protocole SSL avec authentification du client

Si vous envoyez des documents à l'aide du protocole de transport SSL avec authentification du client, alors une modification supplémentaire doit être effectuée sur le fournisseur JSSE qui est utilisé. Pour plus d'informations, consultez le chapitre 14, "Identification et résolution des incidents "Echec de l'établissement de liaison SSL pour cause de non réception du certificat" du *Guide de l'administrateur de WebSphere Partner Gateway*.

Expiration du certificat

Seuls les certificats utilisés pour le chiffrement, la signature numérique et le protocole SSL sont désactivés après expiration. Ces certificats doivent être des certifications d'entité finale et non pas des certificats de CA. Les certificats de CA ne sont pas désactivés après expiration.

Si les certificats racines ou intermédiaires expirent avant que le serveur redémarre, ils ne sont pas inclus dans la liste des certificats sécurisés. Donc, si la génération du chemin de certification échoue à cause du certificat de CA qui est introuvable, ceci peut être dû à l'expiration du certificat de CA. Si un certificat racine ou intermédiaire a expiré lors de son exécution, la génération du chemin de certification échoue et le certificat d'entité finale correspondant n'est pas utilisé dans la transaction métier. Vous pouvez vérifier la période de validité et le statut du certificat à l'aide de la vue Liste de certificats disponible dans la console de WebSphere Partner Gateway. La date de validité des certificats expirés s'affiche en rouge dans la vue.

Si un certificat de CA a expiré, vous pouvez en obtenir un autre depuis le CA qui l'a émis. Téléchargez le nouveau certificat de CA à l'aide de la console de WebSphere Partner Gateway. Pour plus d'informations sur le téléchargement des certificats, reportez-vous à «Utilisation de certificats pour activer le chiffrement et le déchiffrement», «Utilisation de certificats pour activer la signature numérique», à la page 275 et «Utilisation de certificats pour activer le protocole SSL», à la page 280.

Utilisation de certificats pour activer le chiffrement et le déchiffrement

Cette section décrit le chiffrement et le déchiffrement des certificats.

Création et installation de certificats de chiffrement entrants

Ce certificat est utilisé par le concentrateur pour déchiffrer les fichiers codés, reçus de partenaires. Le concentrateur utilise votre clé privée pour déchiffrer les documents. Le chiffrement est utilisé pour empêcher toute autre personne que l'expéditeur et le destinataire prévu de visualiser les documents en transit.

Prenez note de la limitation importante formulée ci-dessous, concernant la réception de messages AS2 chiffrés envoyés par les partenaires. Si un partenaire envoie un message AS2 chiffré en utilisant le mauvais certificat, le déchiffrage échoue. Toutefois, aucune MDN n'est retournée au partenaire pour indiquer l'échec. Pour que votre partenaire puisse recevoir des MDN dans ce cas-là, créez une connexion vers le partenaire avec la définition de document suivante :

- Package : **AS** vers Package : **None**
- Protocole : **Binaire** vers Protocole : **Binaire**
- Type de document : **Binaire** vers Type de document : **Binaire**

La connexion créée doit être de type AS vers None, c'est-à-dire qu'il faut établir une connexion en activant la fonction business-to-business AS sur un partenaire et la fonction business-to-business None sur l'autre partenaire. Vérifiez que la passerelle source pour AS est une passerelle SMTP (dans le cas de AS1), HTTP (dans le cas de AS2) ou FTP (dans le cas de AS3), et qu'elle est configurée sur une adresse MDN. La MDN de l'échec de échec est ainsi renvoyée sur cette connexion binaire AS vers None.

Etape 1 : Obtention d'un certificat

Pourquoi et quand exécuter cette tâche

Génération d'un certificat auto-signé : Si vous envisagez d'utiliser le déchiffrement, procédez comme suit :

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer un certificat auto-signé et une paire de clés.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.
4. Distribuez le certificat à vos partenaires. Ils doivent importer le fichier dans leur produit B2B pour l'utiliser comme certificat de chiffrement. Conseillez-leur de l'utiliser lorsqu'ils souhaitent envoyer des fichiers chiffrés au partenaire interne. Si votre certificat est signé par une autorité de certification, fournissez également le certificat de CA.
5. Utilisez iKeyman pour sauvegarder les certificat auto-signé et la paire de clés privées sous forme de fichier PKCS12.
6. Allez dans **Profil** > **{Opérateur du concentrateur/Partenaire interne}** > **Certificats** > **Charger le certificat.**
7. Dans la liste déroulante **A quel partenaire ce certificat appartient-il**, sélectionnez le partenaire auquel associer le nouveau certificat téléchargé.
8. Cliquez sur **Rechercher** pour rechercher un partenaire ou sous-ensemble de partenaires particulier.
9. Cliquez sur **Parcourir** à côté de **Emplacement du certificat** pour télécharger le certificat.
10. Cliquez sur **Suivant**.
11. Dans Fournir des détails sur le certificat, entrez les informations suivantes : **Certificat feuille** , **Certificat de CA racine** Ou **Certificat de CA intermédiaire**.
12. Associez ce certificat à **Chiffrement**.
13. Dans **Utilisation du certificat**, sélectionnez **Principale** ou **Secondaire**.
14. Sélectionnez **activé** ou **désactivé** dans **Statut** selon si vous voulez activer ou désactiver le certificat après son téléchargement
15. Sélectionnez le **Mode de fonctionnement**.
16. Cliquez sur **Terminer** pour enregistrer les modifications et fermer l'assistant.

Utilisation d'un certificat signé par une autorité de certification (CA) : Si vous envisagez d'utiliser un certificat signé par une autorité de certification, suivez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le récepteur.
3. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.
4. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le magasin de clés.

Etape 2 : Distribution du certificat
Pourquoi et quand exécuter cette tâche

Distribuez le certificat signé par l'autorité de certification à tous les partenaires.

Installation de certificats de chiffrement sortants

Ce certificat est utilisé lorsque le concentrateur envoie des documents chiffrés aux partenaires. WebSphere Partner Gateway chiffre les documents à l'aide des clés publiques des partenaires et ces derniers déchiffrent les documents avec leurs clés privées.

Le partenaire peut disposer de plusieurs certificats de chiffrement. L'un est le certificat principal, utilisé par défaut. L'autre est le certificat secondaire, utilisé si le certificat principal expire.

Etape 1 : Obtention du certificat du partenaire
Pourquoi et quand exécuter cette tâche

Procurez-vous le certificat de chiffrement de votre partenaire. Le certificat doit être au format X.509 DER. Notez que WebSphere Partner Gateway n'accepte que les certificats X5.09.

Etape 2 : Installation du certificat du partenaire
Pourquoi et quand exécuter cette tâche

Installez le certificat via la console de communauté sous le profil du partenaire, en procédant de la manière suivante :

1. Naviguez jusqu'à **Profil** > **Partenaire externe** > **Certificats** > **Charger le certificat**.
2. Dans la page **Sélectionner partenaire, emplacement de fichier, mot de passe** de l'assistant, entrez les valeurs suivantes :
   - **A quel partenaire ce certificat appartient-il** : Sélectionnez le partenaire auquel associer le nouveau certificat téléchargé. Cliquez sur rechercher pour rechercher un partenaire ou sous-ensemble de partenaires particulier. Si le partenaire est un opérateur du concentrateur ou un partenaire interne, entrez l'emplacement du certificat, l'emplacement de la clé privée et le mot de passe (OU) fournissez le fichier de clés certifiées ou fichier de clés avec un mot de passe. Pour les partenaires externes, entrez l'emplacement du certificat (OU) fournissez l'emplacement du magasin de clés certifiées contenant la chaîne de certificats.
   - **Emplacement du certificat** : Cliquez sur **Parcourir** pour sélectionner l'emplacement du certificat public.

3. Cliquez sur **Suivant** pour atteindre la page **Détails du certificat** de l'assistant.
4. Dans la page **Caractéristiques du certificat** de l'assistant, entrez les caractéristiques suivantes concernant le certificat :
   - **Nom du certificat feuille** - Nom du certificat feuille. Le nom de zone dépend du type de certificat : certificat feuille, certificat de CA racine ou certificat de CA intermédiaire.
   - **Description** - Description du certificat feuille.
   - **Type de certificat** - Associez ce certificat à Chiffrement.
   - **Utilisation du certificat** - Associez une utilisation au certificat. Les valeurs autorisées sont Principale et Secondaire.
   - **Mode de fonctionnement** - Entrez le mode de fonctionnement.
   - **Statut** - Sélectionnez activé ou désactivé selon que vous voulez activer ou désactiver le certificat après son téléchargement. Le bouton Suivant est uniquement actif si le certificat est activé.
   - **Gestion des ensembles** - Vous pouvez associer un certificat à un ensemble existant ou créer un nouvel ensemble. Si le certificat est un certificat secondaire, vous ne pouvez l'associer qu'à un ensemble existant. Vous pouvez l'associer à n'importe quel ensemble d'un partenaire interne avec le type chiffrement ou d'un partenaire externe avec le type SSL (autorisation client entrant) ou signature (vérification).
5. Cliquez sur **Suivant** pour atteindre la page Ensemble de l'assistant. Si le certificat est un certificat principal, vous n'avez pas besoin de créer d'ensembles et d'associer le certificat à un ensemble et une connexion de participants. Si vous avez coché **Créer un ensemble**, la page **Créer un ensemble** de l'assistant s'ouvre. Si vous n'avez pas coché cette option, c'est la page **Ajouter à un ensemble existant** qui s'ouvre. Si le fichier contient une clé privée du partenaire interne ou le certificat public du partenaire externe utilisé pour un chiffrement par SSL ou signature numérique, cliquez sur **Terminer**.
6. Dans la page **Créer un ensemble** de l'assistant, entrez les détails concernant le nouvel ensemble. Pour les certificats principaux, vous n'avez pas besoin de créer d'ensemble et d'y associer un certificat. Entrez les valeurs suivantes :
   - **Nom de l'ensemble** - Nom de l'ensemble.
   - **Description** - Description de l'ensemble.
   - **Statut** - Sélectionnez activé ou désactivé. Si le statut est désactivé, le bouton **Suivant** reste inactif.
   - **Paramétrer par défaut** - Cochez cette case si vous voulez que cet ensemble représente l'ensemble par défaut.
7. Dans la page **Ajouter à un ensemble existant**, sélectionnez l'ensemble ou les ensembles à ajouter au certificat. Entrez les valeurs suivantes :
   - **Sélectionner dans la liste des ensembles disponibles pour le type de certificat sélectionné** - Sélectionnez dans la liste l'ensemble ou les ensembles à ajouter au certificat.
   - **Paramétrer par défaut** - Cochez cette case si vous voulez que cet ensemble représente l'ensemble par défaut.
8. Depuis la page **Créer un ensemble** ou **Ajouter à l'ensemble existant**, cliquez sur **Suivant** pour passer à la page **Paramètres par défaut** de l'assistant. Le bouton **Suivant** sera actif si l'ensemble a pour statut activé.
9. Sélectionnez **activé** ou **désactivé** dans **Statut** selon que vous voulez activer ou désactiver le certificat après son téléchargement.

Remarque : Si vous avez coché **Paramétrer par défaut** à la page précédente (Créer un ensemble ou Ajouter à un ensemble existant), vous devez associer l'ensemble à un mode de fonctionnement. Cela permet un affichage des différentes utilisations selon le mode de fonctionnement utilisé. Le chiffrement sera désactivé pour les partenaires internes. Le client SSL et la signature numérique seront désactivés pour les partenaires externes.

10. Cliquez sur **Suivant** pour passer à la page Configuration. Si vous cliquez sur **Terminer** et qu'il manque certains certificats de Ca racines ou intermédiaires, vous serez invité à procéder à un téléchargement. Si vous cliquez sur "Oui" dans la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur**Annuler** si vous voulez effectuer le téléchargement ultérieurement.
11. Dans la page Configuration, entrez les valeurs suivantes :

    Remarque : Cette page affiche une liste des différentes utilisation des certificats (ensemble) en fonction du mode de fonctionnement utilisé. Les noms sont déjà pré-remplis mais vous pouvez les redéfinir.
    - **Partenaire source** - Cette zone est pré-remplie et contient la valeur du partenaire interne.
    - **Partenaire cible** - cette liste déroulante est pré-remplie et contient tous les partenaires externes. Vous pouvez également sélectionner la valeur "Tout" pour inclure tous les partenaires externes.
    - **Package source** - Dans la liste déroulante, sélectionnez Définitions de flux de documents du partenaire interne.
    - **Package cible** -Dans la liste déroulante, sélectionnez Définitions de flux de documents du partenaire externe.
12. Cliquez sur **Ajouter des connexions** si vous voulez associer l'ensemble à d'autres connexions de participants.
13. Cliquez sur **Ajouter un certificat secondaire** pour ajouter un certificat secondaire à l'ensemble actuel.
14. Cliquez sur **Terminer** pour charger le certificat. S'il manque certains certificats de Ca racines ou intermédiaires, vous serez invité à procéder à un téléchargement. Si vous cliquez sur "Oui" dans la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur **Annuler** dans la fenêtre d'invite pour effectuer le chargement ultérieurement.

Répétez cette étape si le partenaire dispose d'un second certificat de chiffrement.

Etape 3 : Installation des certificats émis par une autorité de certification

Pourquoi et quand exécuter cette tâche

Si le certificat a été signé par une autorité de certification (CA) et si le certificat de CA racine et tout autre certificat de la chaîne de certificats ne sont pas encore installés dans le profil Opérateur du concentrateur, procédez à leur installation de la manière suivante :

Remarque : Il est inutile d'effectuer cette étape si le certificat de CA est déjà installé.

1. Allez dans **Profil**> **< Opérateur du concentrateur> Utilisateur**> **Certificats** > **Charger le certificat.**
2. Dans la liste déroulante **A quel partenaire ce certificat appartient-il**, sélectionnez le partenaire auquel associer le nouveau certificat téléchargé.

3. Cliquez sur **Rechercher** pour rechercher un partenaire ou sous-ensemble de partenaires particulier.
4. Cliquez sur **Parcourir** en regard de **Emplacement du magasin de clés certifiées (ou) fichier de clés**.
5. Entrez **Mot de passe** pour le certificat et le magasins de clés certifiées.
6. Si vous choisissez le magasin de clés certifiées, entrez le **Type de fichier de clés** et cliquez sur **Suivant**.
7. Dans la page **Sélectionner un certificat d'entité finale**, sélectionnez un certificat à télécharger.

   Remarque : Si vous téléchargez des certificats en ayant recours à un magasin de clés certifiées comprenant plusieurs certificats, la liste proposée pour l'option **Sélectionnez la liste des certificats de CA racines et intermédiaires à télécharger** comporte tous les certificats. Vous pouvez également télécharger plusieurs certificats.
8. Cliquez sur **Terminer**.

Etape 4 : Activation du chiffrement

Pourquoi et quand exécuter cette tâche

Activez le chiffrement au niveau package (niveau le plus élevé), partenaire ou connexion (niveau le plus bas). Votre définition peut remplacer les autres définitions au niveau connexion. Le résumé de la connexion vous indique si un attribut requis est manquant.

Par exemple, pour modifier les attributs d'une connexion de partenaire, cliquez sur **Administrateur du compte > Connexions > Connexions partenaire** et sélectionnez les partenaires. Cliquez sur **Attributs**, puis éditez l'attribut (par exemple, **AS chiffré**).

Lorsque le message `Aucun certificat de chiffrement valide n'a été trouvé` est affiché, c'est qu'aucun des certificats (principal et secondaire) n'est valide. Les certificats peuvent avoir expirés ou avoir été révoqués. Si les certificats ont expiré ou ont été révoqués, l'événement correspondant (`Certificat révoqué ou expiré`) peut également être affiché dans l'afficheur d'événements. Notez que ces deux événements peuvent être séparés par d'autres.

Pour lancer l'Afficheur d'événements, procédez de la manière suivante :

1. Cliquez sur **Afficheurs > Afficheur d'événements**.
2. Sélectionnez les critères de recherche appropriés.
3. Cliquez sur **Rechercher**.

Voir le *Guide d'administration de WebSphere Partner Gateway* pour obtenir plus d'informations sur l'utilisation de l'Afficheur de documents.

Utilisation de certificats pour activer la signature numérique

Création d'un certificat de signature de communication sortante

Le gestionnaire de documents utilise ce certificat lorsqu'il envoie des documents signés aux partenaires. Les mêmes certificat et clé sont utilisés pour tous les ports et protocoles.

Vous pouvez avoir plusieurs certificats de signature numérique. L'un est le certificat principal, utilisé par défaut. L'autre est le certificat secondaire, utilisé si le certificat principal expire.

Génération d'un certificat auto-signé

Pourquoi et quand exécuter cette tâche

Si vous envisagez d'utiliser un certificat auto-signé, appliquez la procédure suivante.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer un certificat auto-signé et une paire de clés.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.
4. Distribuez le certificat à vos partenaires. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos partenaires doivent vous appeler et vous demander le mot de passe correspondant au fichier compressé.
5. Utilisez iKeyman pour exporter le certificat auto-signé et la paire de clés privées sous forme de fichier PKCS12.

Installation d'un certificat auto-signé sortant

Pourquoi et quand exécuter cette tâche

1. Accédez à **Profil** > {**Opérateur du concentrateur/Partenaire interne**} > **Certificats** > **Charger le certificat**.
2. Dans la page **Sélectionner partenaire, emplacement de fichier, mot de passe** de l'assistant, entrez les valeurs suivantes :
   - **A quel partenaire ce certificat appartient-il** : Sélectionnez le partenaire auquel associer le nouveau certificat téléchargé. Cliquez sur **Rechercher** pour rechercher un partenaire ou sous-ensemble de partenaires particulier. Si le partenaire est un opérateur du concentrateur ou un partenaire interne, entrez l'emplacement du certificat, l'emplacement de la clé privée et le mot de passe (OU) fournissez le fichier de clés certifiées ou fichier de clés avec un mot de passe. Pour les partenaires externes, entrez l'emplacement du certificat (OU) fournissez l'emplacement du magasin de clés certifiées contenant la chaîne de certificats.
   - **Clé privée :** Cliquez sur **Parcourir** pour sélectionner la clé privée du certificat.
   - **Mot de passe :** Si le certificat dispose d'un mot de passe, entrez-le.
   - **Emplacement du magasin de clés certifiées (ou) fichier de clés :** Cliquez sur **Parcourir** pour sélectionner l'emplacement du fichier de clés. Le fichier de clés regroupe des clés privées ainsi que des certificats de CA et des certificats racines digne de confiance.
   - **Mot de passe :** Entrez le mot de passe pour l'emplacement du fichier de clés.
   - **Type :** Sélectionnez le type de magasin de clés certifiées (ou) de fichier de clés. Les valeurs proposées dans la liste déroulante sont : JKS, JCEKS et PKCS12.

   Remarque : Dans WebSphere Partner Gateway, lors de la création d'une base de données de clé de type CMS (fichier de clés) avec iKeyman, l'erreur suivante s'est affichée :

   ```
   La bibliothèque native java CMS est introuvable. Assurez-vous que le composant SSL requis par
   votre produit est installé et que le chemin d'accès à la bibliothèque est correctement défini.
   ```

WebSphere Application Server et WebSphere Partner Gateway n'utilisant pas les fichiers de clés CMS, utilisez le type de fichier de clés pris en charge, JKS (par défaut), PKCS12 ou JCEKS.

3. Cliquez sur **Suivant** pour atteindre la page **Détails du certificat** de l'assistant. La page **Sélectionner un certificat d'entité finale et de CA** s'affiche lorsque vous téléchargez les certificats via un magasin de clés certifiées comportant plusieurs certificats. La liste des certificats disponibles dans le magasin de clés certifiées s'affiche.
4. Dans la page **Sélectionner un certificat d'entité finale et de CA**, entrez les valeurs suivantes :
   - **Le fichier de clés comporte plusieurs certificats d'entité finale. Sélectionner le certificat à charger ?** - La liste déroulante comporte tous les certificats d'entité finale. Sélectionnez le certificat à charger.
   - **Mot de passe**- Si le fichier de clés dispose d'un mot de passe, cochez cette case et entrez le mot de passe dans la zone de texte.
   - **Sélectionner la liste des certificats de CA racines et intermédiaires à charger** - Sélectionnez les certificats à charger.
5. Cliquez sur **Suivant** pour atteindre la page **Détails du certificat** de l'assistant.
6. Dans la page **Caractéristiques du certificat** de l'assistant, entrez les caractéristiques suivantes concernant le certificat :
   - **Nom du certificat feuille** - Nom du certificat feuille. Le nom de zone dépend du type de certificat : certificat feuille, certificat de CA racine ou certificat de CA intermédiaire.
   - **Description** - Description du certificat feuille.
   - **Type de certificat** - Associez ce certificat à Chiffrement.
   - **Utilisation du certificat** - Associez une utilisation au certificat. Les valeurs autorisées sont Principale et Secondaire.
   - **Mode de fonctionnement** - Entrez le mode de fonctionnement.
   - **Statut** - Sélectionnez activé ou désactivé selon que vous voulez activer ou désactiver le certificat après son téléchargement. Le bouton Suivant est uniquement actif si le certificat est activé.
   - **Gestion des ensembles** - Vous pouvez associer un certificat à un ensemble existant ou créer un nouvel ensemble. Si le certificat est un certificat secondaire, vous ne pouvez l'associer qu'à un ensemble existant. Vous pouvez l'associer à n'importe quel ensemble d'un partenaire interne avec le type chiffrement ou d'un partenaire externe avec le type SSL (autorisation client entrant) ou signature (vérification).

     Remarque : Il n'y a aucune gestion des ensembles pour l'opérateur du concentrateur. Les certificats seront associés à l'ensemble par défaut qui a été créé.
7. Cliquez sur **Suivant** pour atteindre la page Ensemble de l'assistant. Si le certificat est un certificat principal, vous n'avez pas besoin de créer d'ensembles et d'associer le certificat à un ensemble et une connexion de participants. Si vous avez coché **Créer un ensemble**, la page **Créer un ensemble** de l'assistant s'ouvre. Si vous n'avez pas coché cette option, c'est la page **Ajouter à un ensemble existant** qui s'ouvre. Si le fichier contient une clé privée du partenaire interne ou le certificat public du partenaire externe utilisé pour un chiffrement par SSL ou signature numérique, cliquez sur **Terminer**.
8. Dans la page **Créer un ensemble** de l'assistant, entrez les détails concernant le nouvel ensemble. Pour les certificats principaux, vous n'avez pas besoin de créer d'ensemble et d'y associer un certificat. Entrez les valeurs suivantes :

- **Nom de l'ensemble** - Nom de l'ensemble.
- **Description** - Description de l'ensemble.
- **Statut** - Sélectionnez activé ou désactivé. Si le statut est désactivé, le bouton **Suivant** reste inactif.
- **Paramétrer par défaut** - Cochez cette case si vous voulez que cet ensemble représente l'ensemble par défaut.

9. Dans la page **Ajouter à un ensemble existant**, sélectionnez l'ensemble ou les ensembles à ajouter au certificat. Entrez les valeurs suivantes :
   - **Sélectionner dans la liste des ensembles disponibles pour le type de certificat sélectionné** - Sélectionnez dans la liste l'ensemble ou les ensembles à ajouter au certificat.
   - **Paramétrer par défaut** - Cochez cette case si vous voulez que cet ensemble représente l'ensemble par défaut.
10. Depuis la page **Créer un ensemble** ou **Ajouter à l'ensemble existant**, cliquez sur **Suivant** pour passer à la page **Paramètres par défaut** de l'assistant. Le bouton **Suivant** sera actif si l'ensemble a pour statut activé.
11. Sélectionnez **activé** ou **désactivé** dans **Statut** selon que vous voulez activer ou désactiver le certificat après son téléchargement.

    Remarque : Si vous avez coché **Paramétrer par défaut** à la page précédente (Créer un ensemble ou Ajouter à un ensemble existant), vous devez associer l'ensemble à un mode de fonctionnement. Cela permet un affichage des différentes utilisations selon le mode de fonctionnement utilisé. Le chiffrement sera désactivé pour les partenaires internes. Le client SSL et la signature numérique seront désactivés pour les partenaires externes.
12. Cliquez sur **Suivant** pour passer à la page Configuration. Si vous cliquez sur **Terminer** et qu'il manque certains certificats de Ca racines ou intermédiaires, vous serez invité à procéder à un téléchargement. Si vous cliquez sur "Oui" dans la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur**Annuler** si vous voulez effectuer le téléchargement ultérieurement.
13. Dans la page Configuration, entrez les valeurs suivantes :

    Remarque : Cette page affiche une liste des différentes utilisation des certificats (ensemble) en fonction du mode de fonctionnement utilisé. Les noms sont déjà pré-remplis mais vous pouvez les redéfinir.
    - **Partenaire source** - Cette zone est pré-remplie et contient la valeur du partenaire interne.
    - **Partenaire cible** - cette liste déroulante est pré-remplie et contient tous les partenaires externes. Vous pouvez également sélectionner la valeur "Tout" pour inclure tous les partenaires externes.
    - **Package source** - Dans la liste déroulante, sélectionnez Définitions de flux de documents du partenaire interne.
    - **Package cible** -Dans la liste déroulante, sélectionnez Définitions de flux de documents du partenaire externe.
14. Cliquez sur **Ajouter des connexions** si vous voulez associer l'ensemble à d'autres connexions de participants.
15. Cliquez sur **Ajouter un certificat secondaire** pour ajouter un certificat secondaire à l'ensemble actuel.
16. Cliquez sur **Terminer** pour charger le certificat. S'il manque certains certificats de Ca racines ou intermédiaires, vous serez invité à procéder à un

téléchargement. Si vous cliquez sur "Oui" dans la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur **Annuler** dans la fenêtre d'invite pour effectuer le chargement ultérieurement.

Si vous envoyez les certificats principaux et secondaires, pour l'authentification SSL du client et la signature numérique, et que vous envoyez les certificats principaux dans deux entrées séparées, assurez-vous que les certificats secondaires correspondant sont également envoyés comme des entrées séparées.

Obtention d'un certificat signé par une autorité de certification (CA)

Pourquoi et quand exécuter cette tâche

Si vous envisagez d'utiliser un certificat signé par une autorité de certification, suivez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le récepteur.
3. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.
4. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le magasin de clés.
5. Distribuez le certificat signé par l'autorité de certification à tous les partenaires.

Installation d'un certificat de vérification de signature numérique de communication entrante

Pourquoi et quand exécuter cette tâche

Le gestionnaire de documents utilise le certificat signé du partenaire pour vérifier la signature de l'expéditeur lorsque vous recevez des documents. Les partenaires vous envoient leurs certificats de signature auto-signés au format X.509 DER. De votre côté, vous installez les certificats des partenaires via la console de communauté sous leurs profils respectifs.

Pour installer le certificat, utilisez la procédure ci-dessous.

1. Recevez le certificat de signature X.509 du partenaire au format DER.
2. Naviguez jusqu'à **Profil**> **Partenaire externe**> **Certificats**> **Charger le certificat**.
3. Cliquez sur **Rechercher** pour rechercher un partenaire ou sous-ensemble de partenaires particulier.
4. Cliquez sur **Parcourir** à côté de **Emplacement du certificat** pour télécharger le certificat.
5. Cliquez sur **Suivant** pour atteindre la page **Détails du certificat** de l'assistant.
6. Associez ce certificat à **Vérification de signature numérique**.
7. Sélectionnez **activé** ou **désactivé** dans **Statut** selon que vous voulez activer ou désactiver le certificat après son téléchargement.
8. Sélectionnez le **Mode de fonctionnement**. Si vous êtes un opérateur du concentrateur, vous ne disposez pas de l'option de sélection du **Mode de fonctionnement**.
9. Cliquez sur **Terminer** pour enregistrer les modifications et fermer l'assistant.

10. Si le certificat a été signé par une autorité de certification et si le certificat de CA racine et tout autre certificat de la chaîne des certificats ne sont pas encore installés dans le profil Opérateur du concentrateur, procédez à leur installation. Cette action n'est applicable que pour le magasin de clés certifiées/fichier de clés.
    a. Cliquez sur **Administrateur du concentrateur> Profil du partenaire du concentrateur > Certificats** pour afficher la liste des certificats.

       Assurez-vous d'être connecté à la console de communauté en tant qu'opérateur de concentrateur et installez le certificat dans votre propre profil.
    b. Cliquez sur **Charger le certificat**.
    c. Sélectionnez **Racine et intermédiaire**.
    d. Tapez une description du certificat (obligatoire).
    e. Faites passer l'état sur **Activé**.
    f. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
    g. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
    h. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

    Remarque : Il est inutile d'effectuer l'étape précédente si le certificat de CA est déjà installé.
11. Activez la signature au niveau package (niveau le plus élevé), partenaire ou connexion (niveau le plus bas). Votre définition peut remplacer les autres définitions au niveau connexion. Le résumé de la connexion vous indique si un attribut requis est manquant.

    Par exemple, pour modifier les attributs d'une connexion de partenaire, cliquez sur **Administrateur du compte > Connexions** et sélectionnez les partenaires. Cliquez sur **Attributs**, puis éditez l'attribut (par exemple **AS signé**).

Utilisation de certificats pour activer le protocole SSL

Les sections suivantes expliquent comment créer et installer des certificats SSL à utiliser avec WebSphere Partner Gateway. Elles donnent également une vue générale du processus de négociation SSL. Si votre communauté n'utilise pas le protocole SSL, ni vous ni vos partenaires n'avez besoin de certificat SSL pour les communications entrantes ou sortantes.

Etablissement de liaison SSL

Pourquoi et quand exécuter cette tâche

Chaque session SSL commence par une négociation.

Lorsqu'un client (le partenaire ou le partenaire interne) initie un échange de message, le processus est le suivant :

1. Le client envoie un message de salutation "hello" avec ses fonctions cryptographiques (triées en fonction de ses préférences), telles que la version de la couche SSL ainsi que les algorithmes de cryptographie et les méthodes de compression de données qu'il prend en charge. Le message contient également un nombre aléatoire sur 28 octets.

2. Le serveur répond par un message "hello done" indiquant la méthode cryptographique (l'algorithme) et la méthode de compression des données qu'il choisit, un ID de session et un autre nombre aléatoire.

   Remarque : La négociation échoue si le client et le serveur n'ont aucun algorithme de cryptographie en commun. Le serveur choisit généralement l'algorithme commun le plus fort.
3. Le serveur envoie son certificat numérique.

   L'authentification du serveur se produit à cette étape.
4. Le serveur envoie un message de demande de certificat numérique. Dans ce message ("digital certificate request"), il envoie une liste des types de certificats pris en charge et des noms distinctifs des autorités des certifications possibles.
5. Le serveur envoie un message de fin de salutation "hello done" et attend la réponse du client.
6. Dès réception du message de fin de salutation, le client vérifie la validité du certificat numérique du serveur et contrôle que les paramètres de salutation du serveur sont acceptables.
7. Si le serveur a demandé un certificat numérique au client, celui-ci en envoie un, ou si aucun certificat numérique ne convient, il envoie une alerte d'absence de certificat numérique. Cette alerte constitue un simple avertissement, mais le serveur peut faire échouer la session si l'authentification du client est obligatoire.
8. Le client envoie un message d'échange de clé client. Il contient le secret premaster, un nombre aléatoire sur 46 octets, utilisé lors de la génération de clés de chiffrement symétrique et de clés MAC (code d'authentification de message), le tout chiffré avec la clé publique du serveur.
9. Si le client a envoyé un certificat numérique au serveur, il envoie également un message de vérification de certificat numérique, signé avec sa clé privée. En contrôlant la signature de ce message, le serveur peut vérifier la propriété du certificat numérique du client.

   Remarque : Aucune procédure supplémentaire de vérification du certificat numérique n'est nécessaire. Si le serveur ne dispose pas de la clé privée du certificat numérique, il ne peut pas déchiffrer le secret premaster et créer les clés adaptées à l'algorithme de chiffrement symétrique et la négociation échoue.
10. Le client réalise une série d'opérations cryptographiques pour convertir le secret premaster en secret master, à partir duquel sont obtenues toutes les données de clé nécessaires au chiffrement et à l'authentification du message. Ensuite, le client envoie un message "change cipher spec" (modification de l'algorithme de cryptographie) pour faire basculer le serveur sur l'algorithme nouvellement négocié. Le message suivant envoyé par le client (le message "finished") est le premier message chiffré à l'aide de cet algorithme et de ces clés de chiffrement.
11. Le serveur répond par les messages "change cipher spec" et "finished".

L'authentification du client requiert les étapes 4, 7 et 9.

La négociation SSL est terminée et les données d'application chiffrées peuvent être envoyées.

Configuration de certificats SSL pour les communications entrantes

Cette section explique comment configurer l'authentification du serveur et du client pour les demandes de connexion entrantes émises par les partenaires.

Une demande de connexion entrante est générée lorsque le partenaire envoie un document à WebSphere Partner Gateway. Si votre communauté n'utilise pas la couche SSL, vous n'avez pas besoin de certificat SSL pour les communications entrantes ou sortantes.

Remarque : Pour les communications FTPS entrantes, WebSphere Partner Gateway utilise un serveur FTP fourni par le client : la configuration nécessaire pour les communications SSL entrantes dépend donc du serveur FTP utilisé par le client.

Etape 1 : Obtention d'un certificat SSL

Pourquoi et quand exécuter cette tâche

WebSphere Application Server utilise le certificat SSL lorsqu'il reçoit des demandes de connexion de partenaires via SSL. Il s'agit du certificat que le récepteur présente pour identifier le concentrateur auprès du partenaire. Ce certificat serveur peut être auto-signé ou signé par une autorité de certification. Dans la plupart des cas, vous utilisez un certificat d'une autorité de certification pour augmenter la sécurité. Vous pouvez utiliser un certificat auto-signé dans un environnement de test. Utilisez iKeyman ou la console d'administration de WebSphere Application Server pour générer un certificat et une paire de clés. Pour plus d'informations sur l'utilisation de iKeyman ou la console d'administration de WebSphere Application Server, reportez-vous à la documentation disponible auprès d'IBM.

Une fois le certificat et la paire de clés générés, utilisez le certificat pour le trafic SSL entrant de tous les partenaires. Si vous disposez de plusieurs récepteurs ou consoles, copiez le magasin de clés résultant sur chaque instance. Si le certificat est généré à l'aide de la console d'administration de WebSphere Application Server, la clé et le certificat peuvent être importés dans un autre fichier de clés d'un serveur autre grâce à cette console. Si le certificat est auto-signé, fournissez-le aux partenaires. Pour obtenir ce certificat, utilisez l'utilitaire iKeyman afin d'extraire le certificat public dans un fichier.

Génération d'un certificat auto-signé : Si vous avez l'intention d'utiliser des certificats de serveur auto-signés, utilisez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman qui se trouve dans /<*WAS_Installation_dir*>/bin. Si vous utilisez iKeyman pour la première fois, supprimez le certificat “fictif” (dummy) se trouvant dans le magasin de clés.
2. Ouvrez le fichier de clés du récepteur ou de la console à l'aide de l'utilitaire iKeyman, puis utilisez ce dernier pour générer un certificat auto-signé et une paire de clés pour le fichier de clés du récepteur ou de la console.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.

   Enregistrez le fichier de clés dans un fichier JKS, PKCS12 ou JCEKS.
4. Distribuez le certificat à vos partenaires. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos partenaires doivent vous appeler et vous demander le mot de passe correspondant au fichier compressé.
5. A l'aide de la console d'administration de WebSphere Application Server, définissez le nouveau certificat dans la configuration SSL et dans les paramètres

du récepteur et de la console. Vous pouvez également le faire en sélectionnant l'alias du nouveau certificat dans le fichier de clés figurant dans la configuration de chaque noeud ou serveur.

Obtention d'un certificat généré par une autorité de certification (CA) : Si vous envisagez d'utiliser un certificat signé par une autorité de certification, suivez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman qui se trouve dans le répertoire */<WAS_Installation_dir>*/bin.
2. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le récepteur.
3. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.
4. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le magasin de clés.
5. Distribuez le certificat de CA à tous les partenaires, le cas échéant.
6. A l'aide de la console d'administration de WebSphere Application Server, définissez le nouveau certificat dans la configuration SSL et dans les paramètres du récepteur et de la console. Vous pouvez également le faire en sélectionnant l'alias du nouveau certificat dans le fichier de clés figurant dans la configuration de chaque noeud ou serveur.

   Remarque : Vous pouvez également utiliser la console d'administration de WebSphere Application Server pour effectuer les étapes précédentes.

Etape 2 : Authentification des clients

Pourquoi et quand exécuter cette tâche

Si vous souhaitez authentifier les partenaires qui envoient des documents, procédez comme suit.

Installation du certificat client :
Pourquoi et quand exécuter cette tâche

Pour l'authentification client, utilisez la procédure ci-dessous.

1. Procurez-vous le certificat de votre partenaire.
2. Si le certificat est auto-signé, installez le certificat dans le fichier de clés à l'aide de l'utilitaire iKeyman ou de la console d'administration de WebSphere Application Server.
3. Si le certificat est généré à l'aide de la console d'administration, ajoutez les certificats de CA associés au magasin de relations de confiance associé à l'aide de l'utilitaire iKeyman ou de la console d'administration de WebSphere Application Server.

Remarque : Lorsque vous ajoutez plusieurs partenaires à la communauté de votre concentrateur, vous pouvez utiliser iKeyman ou la console d'administration de WebSphere Application Server pour ajouter leurs certificats au magasin de relations de confiance. Si un partenaire quitte la communauté, vous pouvez utiliser iKeyman ou la console d'administration de WebSphere Application Server pour supprimer les certificats du partenaire du fichier de clés certifiées.

Configuration de l'authentification du client :

Pourquoi et quand exécuter cette tâche

Une fois le ou les certificats installés, configurez WebSphere Application Server afin d'utiliser l'authentification client en exécutant le script utilitaire bcgClientAuth.jacl.

1. Passez dans le répertoire : /<*ProductDir*>/bin
2. Pour activer l'authentification client, appelez le script comme suit :

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/bcgClientAuth.jacl
   -conntype NONE set
```

Remarque : Pour désactiver l'authentification client, appelez le script comme suit :

```
./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/bcgClientAuth.jacl
  -conntype NONE clear
```

Vous devez redémarrer le serveur bcgreceiver pour que ces modifications prennent effet. Vous pouvez également activer l'authentification du client à l'aide de la console d'administration de WebSphere Application Server. La valeur "Pris en charge" signifie que le serveur demande le certificat client, mais si ce dernier est indisponible, l'établissement de liaison SSL peut encore être établi. La valeur "Obligatoire" signifie que le certificat client doit être envoyé. Sinon, l'établissement de liaison SSL échoue.

Validation du certificat du client :
Pourquoi et quand exécuter cette tâche

Une fonction supplémentaire peut être utilisée avec l'authentification client SSL. Elle est activée via la Console de communauté. Pour HTTPS, WebSphere Partner Gateway vérifie les certificats par rapport aux ID entreprise contenus dans les documents entrants. Pour pouvoir utiliser cette fonction, créez le profil du partenaire, importez le certificat client et marquez-le comme SSL.

1. Importez le certificat client.
   a. Cliquez sur **Administrateur du compte > Profils > Partenaire** et recherchez le profil du partenaire.
   b. Cliquez sur **Certificats**.
   c. Cliquez sur **Charger le certificat**.
   d. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
   e. Sélectionnez **Client SSL** comme type de certificat.
   f. Tapez une description du certificat (obligatoire).
   g. Faites passer l'état sur **Activé**.
   h. Si vous souhaitez sélectionner un autre mode de fonctionnement que **Production** (valeur par défaut), sélectionnez-le dans la liste.
   i. Cliquez sur **Terminer**.
2. Mettez à jour la destination du client.
   a. Cliquez sur **Administrateur du compte > Profils > Partenaire** et recherchez le profil du partenaire.
   b. Cliquez sur **Destinations**.
   c. Sélectionnez la destination HTTPS précédemment créée. Si vous n'avez pas encore créé la destination HTTPS, consultez «Configuration d'une destination HTTPS», à la page 234.
   d. Cliquez sur l'icône **Edition** pour modifier la destination.
   e. Sélectionnez **Oui** pour **Valider le certificat client SSL**.

f. Cliquez sur **Sauvegarder**.

Configuration séparée des fichiers de clés et des fichiers de clés certifiées pour le récepteur et la console

Par défaut, WebSphere Partner Gateway utilise des fichier de clés et fichier de clés certifiées communs pour le récepteur et pour la console. Cependant, vous pouvez configurer séparément le fichier de clés et le fichier de clés certifiées pour le récepteur et la console dans une installation en mode réparti.

Pour configurer le fichier de clés et le fichier de clés certifiées, créez et définissez séparément le fichier de clés et fichier de clés certifiées pour le récepteur et la console. Créez également des configurations SSL distinctes. Les configurations SSL peuvent être définies au niveau du cluster ou au niveau du serveur. La définition d'une configuration SSL au niveau du cluster est plus aisée puisque la configuration est alors applicable à tous les serveurs dans ce cluster et il n'est pas nécessaire de configurer chaque serveur séparément.

Définition de la configuration SSL au niveau du cluster : Lors de la définition de la configuration SSL avec un nouveau fichier de clés et un fichier de clés certifiées au niveau du cluster, il ne doit y avoir aucune configuration SSL définie au niveau du serveur. S'il existe une configuration SSL définie au niveau du serveur, alors la configuration SSL au niveau du cluster ne sera pas utilisée. A la place, ce sera celle définie au niveau du serveur qui sera utilisée.

Procédez de la manière suivante pour définir la configuration SSL pour bcgconsoleCluster :

1. Créez un fichier de clés pour le cluster Console. Le fichier de clés doit être créé dans la portée du cluster bcgconsole en naviguant jusqu'à **Sécurité > Gestion de clés et certificat SSL > Fichiers de clés et certificats**.
2. Créez un fichier de clés certifiées pour le cluster Console. Le fichier de clés certifiées doit être créé dans la portée du cluster bcgconsole en naviguant jusqu'à **Sécurité > Gestion de clés et certificat SSL > Fichiers de clés et certificats**.
3. Créez une configuration SSL pour le cluster de la console au niveau de la portée du cluster Console en naviguant jusqu'à **Sécurité > Gestion de clés et certificat SSL > Configurations SSL**. Définissez le fichier de clés et le fichier de clés certifiées créés lors des étapes précédentes. Mettez à jour les alias de certificat dans la liste des alias de certificat en cliquant sur **Obtenir des alias de certificat** et sélectionnez l'alias requis à utiliser pour l'authentification du serveur. Attribuez au gestionnaire d'accréditation la valeur **IbmPKIX**.
4. Définissez cette configuration SSL dans bcgconsoleCluster en la substituant à la configuration SSL héritée. Mettez à jour les alias de certificat en cliquant sur **Mettre à jour les alias de certificat** et définissez les alias à utiliser pour l'authentification du serveur.
5. Redémarrez bcgconsoleCluster.

Procédez de la manière suivante pour définir la configuration SSL pour bcgreceiverCluster :

1. Créez un fichier de clés pour le cluster Récepteur. Le fichier de clés doit être créé dans la portée du cluster bcgreceiver en naviguant jusqu'à **Sécurité > Gestion de clés et certificat SSL > Fichiers de clés et certificats**.

2. Créez un fichier de clés certifiées pour le cluster Récepteur. Le fichier de clés certifiées doit être créé dans la portée du cluster bcgconsole en naviguant jusqu'à **Sécurité > Gestion de clés et certificat SSL > Fichiers de clés et certificats**.
3. Créez une configuration SSL pour le cluster récepteur au niveau de la portée du cluster Récepteur en naviguant jusqu'à **Sécurité > Gestion de clés et certificat SSL > Configurations SSL** et définissez le fichier de clés et le fichier de clés certifiées créés lors des étapes précédentes. Obtenez les alias de certificat en cliquant sur **Obtenir des alias de certificat** et sélectionnez l'alias requis à utiliser pour l'authentification du serveur. Attribuez au gestionnaire d'accréditation la valeur **IbmPKIX**.
4. Définissez cette configuration SSL dans bcgreceiverCluster en la substituant à la configuration SSL héritée. Mettez à jour les alias de certificat en cliquant sur **Mettre à jour les alias de certificat** et définissez les alias à utiliser pour l'authentification du serveur.
5. Redémarrez bcgreceiverCluster.

Pour de plus amples informations sur l'utilisation des fichiers de clés, des fichiers de clés certifiées, de la configuration SSL et des configurations des noeuds finaux, reportez-vous à la section *Sécurisation des applications et de leur environnement de la documentation WebSphere Application Server.*

Définition de NodeDefaultTrustStore dans NodeDefaultSSLSetting en mode réparti : Cette configuration s'applique au mode réparti simple. Mais elle peut également s'appliquer au mode entièrement réparti si un fichier de clés et un fichier de clés certifiées communs sont utilisés pour le récepteur et la console. Si un noeud est fédéré dans une cellule, les certificats de signataire provenant du noeud sont ajoutés à CellDefaultTrustStore. Par défaut, NodeDefaultSSLSetting fait référence à CellDefaultTrustStore en tant que fichier de clés certifiées. Pour le récepteur et la console WebSphere Partner Gateway, l'utilisation des certificats de signataire provenant d'autres noeuds n'est pas souhaitable. Pour utiliser un fichier de clés certifiées dédié pour les noeuds sur lesquels WebSphere Partner Gateway est installé, NodeDefaultTrustStore peut être défini dans NodeDefaultSSLSettings comme fichier de clés certifiées.

Les étapes permettant d'effectuer ces modifications sont les suivantes :

1. Dans la console d'administration de WebSphere Application Server, naviguez jusqu'à **Sécurité > Gestion de clés et certificat SSL > Gérer les configurations de sécurité de noeud final > <nom_noeud> > Configurations SSLs > NodeDefaultSSLSettings**.
2. Dans la zone Nom de fichier de clés certifiées, sélectionnez **NodeDefaultTrustStore**.

   Remarque : Assurez-vous que NodeDefaultTrustStore est configuré pour le fichier de clés certifiées que vous souhaitez utiliser ; par exemple, bcgSecurityTrust.jks.
3. Cliquez sur **Appliquer**.
4. Sur la page suivante de la console, cliquez sur **Enregistrer** pour mettre à jour les modifications apportées à la configuration principale.
5. Redémarrez les serveurs dans ce noeud.

Remarque : Pour le mode entièrement réparti, les modifications ci-dessus doivent être effectuées pour tous les noeuds contenant les serveurs bcgreceiver et

bcgconsole. Pour le mode réparti simple, les modifications doivent être effectuées pour tous les noeuds contenant le serveur bcgserver.

Ajout de certificats de signataire à trust.p12 si NodeDefaultTrustStore est défini pour un noeud contenant des serveurs WebSphere Partner Gateway : Actuellement, NodeDefaultTrustStore fait référence à trust.p12. Si NodeDefaultTrustStore est défini pour le noeud contenant des serveurs WebSphere Partner Gateway, bcgSecurityTrust.jks ne sera pas utilisé. Les certificats de signataire émanant de bcgSecurityTrust.jks doivent être ajoutés à trust.p12 comme indiqué.

Configuration de certificats SSL pour les communications sortantes

Une demande de connexion sortante est générée lorsque WebSphere Partner Gateway envoie un document à un partenaire. Si votre communauté n'utilise pas la couche SSL, vous n'avez pas besoin de certificat SSL pour les communications entrantes ou sortantes.

Etape 1 : Authentification du serveur

Pourquoi et quand exécuter cette tâche

Si le protocole SSL est utilisé pour envoyer des documents sortants à vos partenaires, WebSphere Partner Gateway leur demande un certificat côté serveur. Le même certificat de CA peut être utilisé pour plusieurs partenaires. Le certificat doit être au format X.509 DER.

Remarque : Vous pouvez convertir le format avec l'utilitaire iKeyman. Procédez comme suit :

1. Démarrez l'utilitaire iKeyman.
2. Créez un magasin de clés (vide) ou ouvrez-en un.
3. Dans Contenu de la base de données de clés, sélectionnez **Certificats du signataire**.
4. Ajoutez le certificat ARM par l'option **Ajouter**.
5. Exportez ce certificat comme donnée Binary DER, par l'option data **Extraction**.
6. Fermez iKeyman.

Installez le certificat auto-signé du partenaire dans le profil Opérateur du concentrateur. Si le certificat a été signé par une CA et si le certificat de CA racine et tout autre certificat de la hiérarchie des certificats ne sont pas encore installés dans le profil Opérateur du concentrateur, procédez à leur installation.

1. Cliquez sur **Administrateur du compte > Profils > Certificats** pour afficher la liste des certificats.

   Assurez-vous d'être connecté à la console de communauté en tant qu'opérateur du concentrateur ou partenaire interne.
2. Cliquez sur **Charger PKCS12.**.

   Remarque : Le fichier PKCS12 envoyé ne doit contenir qu'une seule clé privée et le certificat associé. Vous pouvez également télécharger le certificat et la clé privée formatée en PKCS#8 séparément.
3. Sélectionnez **Client SSL** comme type de certificat.
4. Tapez une description du certificat (obligatoire).
5. Faites passer l'état sur **Activé**.

6. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
7. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
8. Entrez le mot de passe.
9. Si vous souhaitez sélectionner un autre mode de fonctionnement que **Production** (valeur par défaut), sélectionnez-le dans la liste.
10. Si vous avez deux certificats SSL, indiquez s'il s'agit du certificat principal ou secondaire en sélectionnant **Principal** ou **Secondaire** dans la liste **Utilisation du certificat**.
11. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

Remarque : Il est inutile d'effectuer les étapes précédentes si le certificat de CA est déjà installé.

Etape 2 : Authentification des clients
Pourquoi et quand exécuter cette tâche

Si une authentification SSL client est requise, le partenaire demande, en retour, un certificat au concentrateur. Utilisez la console de communauté pour importer votre certificat dans WebSphere Partner Gateway. Vous pouvez générer le certificat à l'aide de iKeyman. Si le certificat est auto-signé, il doit être fourni au partenaire. S'il s'agit d'un certificat signé par une autorité de certification, il doit être envoyé aux partenaires, de sorte qu'ils puissent l'ajouter à leurs certificats authentifiés.

Vous pouvez attribuer plusieurs certificats. L'un est le certificat principal, utilisé par défaut. L'autre est le certificat secondaire, utilisé si le certificat principal expire.

Utilisation d'un certificat auto-signé :
Pourquoi et quand exécuter cette tâche

Si vous envisagez d'utiliser un certificat auto-signé, appliquez la procédure suivante.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer un certificat auto-signé et une paire de clés.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.
4. Distribuez le certificat à vos partenaires. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos partenaires doivent vous appeler et vous demander le mot de passe correspondant au fichier compressé.
5. Utilisez iKeyman pour exporter le certificat auto-signé et la paire de clés privées sous forme de fichier PKCS12.
6. Installez le certificat auto-signé et la clé via la console de communauté.
   a. Cliquez sur **Administrateur du compte > Profils > Certificats** pour afficher la liste des certificats.

      Veillez à vous connecter à la console de communauté en tant qu'opérateur du concentrateur.
   b. Cliquez sur **Charger PKCS12**.

      Remarque : Le fichier PKCS12 envoyé ne doit contenir qu'une seule clé privée et le certificat associé. Vous pouvez également télécharger le certificat et la clé privée formatée en PKCS#8 séparément.

c. Sélectionnez **Client SSL** comme type de certificat.
d. Tapez une description du certificat (obligatoire).
e. Faites passer l'état sur **Activé**.
f. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
g. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
h. Entrez le mot de passe.
i. Si vous souhaitez sélectionner un autre mode de fonctionnement que **Production** (valeur par défaut), sélectionnez-le dans la liste.
j. Si vous avez deux certificats SSL, indiquez s'il s'agit du certificat principal ou secondaire en sélectionnant **Principal** ou **Secondaire** dans la liste **Utilisation du certificat**.
k. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

Si vous envoyez les certificats principaux et secondaires pour l'authentification SSL du client et la signature numérique et que vous envoyez les certificats principaux dans deux entrées séparées, assurez-vous que les certificats secondaires correspondants sont également envoyés comme des entrées séparées.

Utilisation d'un certificat signé par une autorité de certification (CA) : Pourquoi et quand exécuter cette tâche

Si vous envisagez d'utiliser un certificat signé par une autorité de certification, suivez la procédure ci-dessous.

1. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le récepteur.
2. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.
3. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le magasin de clés.
4. Distribuez le certificat signé par l'autorité de certification à tous les partenaires.

Ajout d'une liste de révocation de certificat (CRL)

WebSphere Partner Gateway inclut une fonction de liste de retrait de certificats. La liste de retrait de certificats, émise par une autorité de certification, identifie les partenaires qui ont révoqué des certificats avant leur date d'expiration prévue. Les partenaires ayant des certificats révoqués se voient refuser l'accès à WebSphere Partner Gateway.

Chaque certificat révoqué est identifié par son numéro de série dans la liste de retrait de certificats. Le gestionnaire de documents analyse cette liste toutes les 60 secondes et refuse un certificat s'il est mentionné dans la liste. Cependant, vous pouvez configurer l'intervalle de temps auquel le répertoire CRL est scanné. L'intervalle de temps est spécifié pour la propriété de configuration bcg.rosettanet.encrypt.CertDbRefreshInterval.

Par défaut, les CRL sont stockées à l'emplacement suivant : /<*shared_data_directory*>/security/crl. WebSphere Partner Gateway utilise le paramètre bcg.CRLDir dans Console > Administration système> Administration du gestionnaire de documents> Sécurité pour identifier l'emplacement du répertoire de la CRL.

Placez les CRL dans le répertoire CRL.

Configuration de CRLDP

Pourquoi et quand exécuter cette tâche

Configurez le fournisseur de données de la liste de révocation de certificat en modifiant les paramètres de la machine virtuelle Java, c'est-à-dire en définissant la valeur suivante : -Dcom.ibm.security.enableCRLDP = True.

En mode entièrement réparti, cette modification doit être faite pour bcgdocmgr, bcgreceiver et bcgconsole. Dans le cas du mode réparti simple et du mode simple, effectuez cette modification pour bcgserver.

Les étapes permettant d'effectuer ces modifications sont les suivantes :

1. Connectez-vous à la console d'administration WebSphere Application Server.
2. Dans **Serveurs > Serveurs d'applications**, sélectionnez **Serveur**.
3. Définissez la propriété comme suit :
   a. Sélectionnez le serveur souhaité (bcgdocmgr, bcgreceiver ou bcgconsole).
   b. Dans la page **Configuration**, développez **Java et gestion de processus** dans la section **Infrastructure de serveur** et sélectionnez **Définition de processus.**
   c. Dans la page **Configuration des définitions de processus**, sélectionnez **Machine virtuelle Java** dans la section **Autres propriétés**.
   d. Ajoutez ce qui suit à la valeur existante (le cas échéant) dans la zone Arguments JVM génériques : -Dcom.ibm.security.enableCRLDP=true.
4. Cliquez sur **Appliquer** et sauvegardez pour terminer la configuration.
5. Redémarrez le serveur.
6. Définissez cette propriété sur tous les serveurs du cluster.

Configuration du protocole SSL pour les communications entrantes pour la console de communauté et le récepteur

Les magasins de clés de WebSphere Partner Gateway sont préconfigurés dans WebSphere Application Server. Cette section s'applique uniquement si vous utilisez des magasins de clés différents.

Pour configurer le protocole SSL pour la console de communauté et le récepteur dans WebSphere Partner Gateway, suivez la procédure ci-dessous.

1. Procurez-vous les informations suivantes :
   - Les noms de chemins d'accès complets du fichier de clés et du fichier de relations de confiance ; par exemple pour le récepteur: *<ProductDir>*/common/security/keystore/bcgSecurity.jks et *<ProductDir>*/common/security/keystore/bcgSecurityTrust.jks

     Vous devez saisir ces noms correctement. L'environnement UNIX fait la distinction entre les majuscules et les minuscules.
   - les nouveaux mots de passe de chaque fichier ;
   - le format de chaque fichier. Il doit être choisi parmi l'un des formats suivants : JKS, JCEKS ou PKCS12. Saisissez cette valeur en majuscules, exactement comme indiqué ;
   - le chemin d'accès au fichier script nommé bcgssl.jacl.
2. Ouvrez une fenêtre console de communauté et ouvrez le répertoire /*<ProductDir>*/bin. Le serveur n'a pas besoin d'être en cours d'exécution pour pouvoir modifier les mots de passe.

3. Entrez la commande suivante, en remplaçant les valeurs placées entre < et >. Toutes les valeurs doivent être saisies.

```
./bcgwsadmin.sh -f /<ProductDir>/
scripts/bcgssl.jacl -conntype NONE install
<nomdechemin_fichierdeclés>
<motdepasse_fichierdeclés> <format_fichierdeclés> <nomdechemin_fichierderelationsdeconfiance>
<motdepasse_fichierderelationsdeconfiance> <format_fichierderelationsdeconfiance>
```

4. Démarrez le serveur. Si le serveur ne parvient pas à démarrer, il se peut que cela soit dû à une erreur d'exécution de bcgssl.jacl. Dans ce cas, vous pouvez exécuter à nouveau le script pour la corriger.
5. Si vous avez utilisé bcgClientAuth.jacl pour définir la propriété SSL clientAuthentication, redéfinissez-la après l'utilisation de bcgssl.jacl. Ceci est dû au fait que bcgssl.jacl écrase toutes les valeurs qui peuvent avoir été définies pour l'authentification du client avec la valeur false.

Remarque :

1. Répétez ces étapes pour la console, en remplaçant **receiver** par **console** dans le chemin d'accès.
2. La configuration du protocole SSL, du fichier de clés et du magasin de relations de confiance peut également s'effectuer à l'aide de la console d'administration de WebSphere Application Server.

WebSphere Partner Gateway 6.1.1 prend en charge par défaut un fichier de clés et un magasin de clés certifiées à la fois pour le récepteur et la console. Cependant, vous pouvez utiliser des fichiers de clés et des magasins de clés certifiées séparés en mode Réparti complet. Pour cela, procédez à la configuration suivante en utilisant la console d'administration WAS pour le récepteur :

1. Créez un fichier de clés pour le récepteur. Reportez-vous à la section Création de la configuration d'un fichier de clés dans la documentation de WAS.
2. Créez un magasin de clés certifiées pour le récepteur. Reportez-vous à la section <*Création de la configuration d'un fichier de clés* dans la documentation de WAS <*Sécurisation des applications et de leur environnement.*
3. Créez une configuration SSL pour le récepteur dans laquelle vous définirez le fichier de clés et le magasin de clés certifiées que vous venez de créer. Sélectionnez l'alias devant servir pour l'authentification du serveur dans le fichier de clés. Attribuez au gestionnaire d'accréditation la valeur **IbmPKIX**. Reportez-vous à la section *Création d'une configuration SSL* dans la documentation de WAS *Sécurisation des applications et de leur environnement.*
4. Définissez cette configuration SSL sur chaque serveur bcgreceiver en la substituant à la configuration SSL héritée. Définissez l'alias devant servir pour l'authentification du serveur.
5. Redémarrez chaque serveur bcgreceiver.

La procédure à suivre est identique pour la configuration de la console. Reportez-vous aux sections appropriées dans la documentation de WAS *Sécurisation des applications et de leur environnement.*

1. Créez un fichier de clés pour la console.
2. Créez un magasin de clés certifiées pour la console.
3. Créez une configuration SSL pour la console dans laquelle vous définirez le fichier de clés et le magasin de clés certifiées que vous venez de créer. Sélectionnez l'alias devant servir pour l'authentification du serveur dans le fichier de clés. Attribuez au gestionnaire d'accréditation la valeur **IbmPKIX**.

4. Définissez cette configuration SSL sur chaque serveur bcgconsole en la substituant à la configuration SSL héritée. Définissez l'alias devant servir pour l'authentification du serveur.
5. Redémarrez chaque serveur bcgconsole.

Pour de plus amples informations sur l'utilisation de fichiers de clés, de magasins de clés certifiés, de la configuration SSL et des configurations des noeuds finaux, reportez-vous à la documentation de WAS *Sécurisation des applications et de leur environnement*.

Remarque : Actuellement, NodeDefaultTrustStore fait référence à trust.p12. Si NodeDefaultTrustStore est défini pour le noeud bcg, bcgSecurityTrust.jks ne sera pas utilisé. Vous devrez ajouter des certificats de signataire de bcgSecurityTrust.jks à trust.p12 comme indiqué.

Téléchargement de certificats à l'aide de l'assistant

Pourquoi et quand exécuter cette tâche

En tant qu'opérateur du concentrateur, vous pouvez télécharger des certificats pour les partenaires internes ou externes :

- Télécharger la clé privée et des certificats pour les partenaires internes.
- Télécharger des certificats pour les partenaires externes.
- Télécharger des certificats de CA racines et intermédiaires.

  Important : Cette fonctionnalité est uniquement disponible pour les certificats X.509.
- Télécharger une chaîne de certificats depuis un magasin de clés certifiées.

  Important : Cette fonctionnalité est uniquement disponible pour les certificats X.509.

L'assistant de téléchargement des certificats est fourni. Avec l'assistant, vous pouvez définir l'utilisation du certificat (Signature / vérification / Chiffrement / déchiffrement /client SSL/serveur FTPS/serveur SFTP), l'associer à un ou plusieurs modes de fonctionnement, l'ajouter à un ensemble (existant ou nouveau), le sélectionner comme certificat par défaut pour toutes les connexions de participants ou sélectionner une connexion spécifique dans laquelle cet ensemble de certificats sera utilisé. L'option pour associer le certificat à une connexion n'apparaît pas si ce dernier n'est pas associé à un ensemble. Lorsque vous téléchargez le certificat, vérifiez qu'il n'est pas arrivé à expiration.

Pour OpenPGP, un fichier de paquet de clé publique peut aussi être utilisé pour télécharger la clé publique et le certificat d'un partenaire externe. Le partenaire externe peut exporter la clé depuis le fichier de clés, la stocker dans un fichier et l'envoyer à l'opérateur du concentrateur. L'opérateur du concentrateur peut télécharger le certificat reçu du partenaire externe. Le fichier de clé publique peut être en format binaire ou en code ASCII Armor.

Pour télécharger des certificats pour les partenaires (internes ou externes) à partir de l'assistant, procédez comme suit :

1. Sélectionnez le partenaire et cliquez sur **Administrateur du compte** > **Profil** > **Certificats**.
2. Cliquez sur **Charger le certificat**.

3. Dans la page **Sélectionner partenaire, emplacement de fichier, mot de passe** de l'assistant, entrez les valeurs suivantes :
   - **A quel partenaire ce certificat appartient-il** : Sélectionnez le partenaire auquel associer le nouveau certificat téléchargé. Cliquez sur **Rechercher** pour rechercher un partenaire ou sous-ensemble de partenaires particulier. Si le partenaire est un opérateur du concentrateur ou un partenaire interne, entrez l'emplacement du certificat, l'emplacement de la clé privée et le mot de passe (OU) fournissez le fichier de clés certifiées ou fichier de clés avec un mot de passe. Pour les partenaires externes, entrez l'emplacement du certificat (OU) fournissez l'emplacement du magasin de clés certifiées contenant la chaîne de certificats.

     Remarque : Si vous cliquez sur **Charger le certificat** sans sélectionner un profil de partenaire, alors la zone **A quel partenaire ce certificat appartient-il** ne s'affiche pas. Le certificat est automatiquement téléchargé pour le profil de partenaire sélectionné.
   - **S'agit-il d'un certificat racine ou intermédiaire** : Cochez cette case si le certificat est un certificat racine ou intermédiaire.

     Remarque : Ces deux types de certificat ne s'appliquant qu'au profil d'administrateur du concentrateur, cette case n'est visible que lorsque le partenaire sélectionné est l'administrateur du concentrateur. Par ailleurs, pour les profils d'administrateur du concentrateur, elle n'est disponible que si vous avez sélectionné Charger le certificat.
   - **Emplacement du certificat** : Cliquez sur **Parcourir** pour sélectionner l'emplacement du certificat (public ou privé).
   - **Clé privée :** Cliquez sur **Parcourir** pour sélectionner la clé privée du certificat.

     Remarque : Cela s'applique uniquement à un partenaire interne.
   - **Mot de passe :** Si le certificat dispose d'un mot de passe, entrez-le.
   - **Emplacement du fichier de clés certifiées (ou) du fichier de clés :** cliquez sur **Parcourir** pour sélectionner l'emplacement du fichier de clés certifiées (ou) du fichier de clés. Le magasin de clés certifiées est un fichier contenant des certificats racines et de CA dignes de confiance. Le fichier de clés regroupe des clés privées ainsi que des certificats d'autorité de certification et des certificats racines dignes de confiance. Le fichier de clés regroupe des certificats au format OpenPGP. Cliquez sur **Parcourir** pour sélectionner le fichier dans le chemin de la boîte de dialogue Fichier du fichier de clés/fichier de clés certifiées ou saisissez le chemin dans la zone de texte. Lorsque vous téléchargez un certificat pour un partenaire interne de fichier de clés de type OpenPGP, indiquez le chemin du fichier de clés confidentielles. Pour un partenaire externe, indiquez le chemin du fichier de clés publiques.
   - **Mot de passe :** Si l'emplacement du magasin de clés certifiées (ou) du fichier de clés dispose d'un mot de passe, entrez-le. Pour un fichier de clés, le mot de passe n'est pas nécessaire.
   - **Type :** sélectionnez le type d'emplacement du fichier de clés (ou) du fichier de clés certifiées. Les valeurs disponibles dans la liste sont : JKS, JCEKS, PKCS12 et OpenPGP.
4. Cliquez sur **Suivant**.
5. La page **Certificats d'entité finale et d'autorité de certification** de l'assistant s'ouvre lorsque vous téléchargez les certificats via un fichier de clés certifiées

comportant plusieurs certificats. La liste des certificats disponibles dans le magasin de clés certifiées s'affiche. **Sélectionner les clés/certifications OpenPGP à télécharger** s'affiche lorsque vous sélectionnez un fichier de clés de type OpenPGP dans la page **Sélectionner partenaire, emplacement de fichier, mot de passe** de l'assistant.

- Sélectionnez un certificat dans la page **Certificat d'entité finale à télécharger** de l'assistant. Si le fichier de clés comporte plusieurs clés privées, en même temps que la clé privée vous devez entrez un mot de passe pour la clé si elle est différente. Dans la page **Certificat d'entité finale et certificat d'autorité de certification** de l'assistant, entrez les valeurs suivantes :
  - **Le fichier de clés comporte plusieurs certificats d'entité finale. Sélectionner le certificat à télécharger**- comporte une liste de tous les certificats d'entité finale. Sélectionnez le certificat à charger.
  - **Mot de passe** - si le fichier de clés comporte un mot de passe, cochez cette case et entrez le mot de passe dans la zone de texte.
  - **Sélectionner la liste des certificats d'autorité de certification racines et intermédiaires à télécharger** - dans la zone de liste, sélectionnez les certificats d'autorité de certification racines et intermédiaires à télécharger.
- Dans la page **Sélectionner les clés/certifications OpenPGP à télécharger** de l'assistant, les certificats associés au fichier de clés sélectionné sont remplis dans la liste.

  Remarque : Vous pouvez cliquer sur **Afficher les caractéristiques** pour afficher les caractéristiques du certificat sélectionné. Pour un certificat, chaque fois que l'ID clé et l'ID émetteur sont les mêmes, le certificat est un certificat auto-signé.
  - Sélectionnez une clé de niveau supérieur dans la liste.
  - Entrez le mot de passe de la clé de niveau supérieur si vous voulez télécharger la clé de niveau supérieur.

    Remarque : S'il existe des sous-clés pour la clé de niveau supérieur, toutes les sous-clés sont affichées dans la liste **Sélectionner la sous-clé à télécharger**.

    Important : Cela ne s'applique pas au chargement des certificats publics pour le chiffrement.
  - Sélectionnez la sous-clé, s'il y a lieu.
  - Entrez le mot de passe de la sous-clé.

  Important : Cela ne s'applique pas au chargement des certificats publics pour le chiffrement.

  A faire : Lorsque vous téléchargez le certificat pour un partenaire externe, le mot de passe pour le niveau supérieur et la sous-clé ne sont pas nécessaires.

6. Cliquez sur **Suivant** pour atteindre la page **Caractéristiques du certificat** de l'assistant.
7. Dans la page **Caractéristiques du certificat** de l'assistant, entrez les caractéristiques suivantes concernant le certificat :

- **Nom du certificat feuille** - nom du certificat feuille. Le nom de zone dépend du type de certificat : certificat feuille, certificat de CA racine ou certificat de CA intermédiaire.
- **Description** - description du certificat feuille.
- **Ce certificat est-il destiné à l'authentification du serveur FTP** - cochez cette case si le certificat téléchargé est destiné à l'authentification du serveur FTP.
- **Ce certificat est-il destiné à l'authentification du serveur SFTP** - cochez cette case si le certificat téléchargé est destiné à l'authentification du serveur SFTP.

  Important : L'authentification du serveur FTP et du serveur SFTP ne s'applique pas aux certificats OpenPGP.
- **Type de certificat** - associez ce certificat à un type de certificat. Les différents types pris en charge sont Signature numérique, Vérification de signature numérique, Chiffrement, Déchiffrement, Serveur SSL et Client SSL.

  A faire :
  - L'option de chiffrement est destinée à un partenaire externe et l'option de déchiffrement à un partenaire interne.
  - Le client SSL n'est pas pris en charge pour le type de certificat OpenPGP.
- **Utilisation du certificat** - associez une utilisation au certificat. Les valeurs autorisées sont Principale et Secondaire.

  Important : Cela ne s'applique pas au déchiffrement, à la vérification de signature et au certificat du serveur SSL.
- **Mode de fonctionnement** - sélectionnez un mode de fonctionnement pour les certificats de chiffrement, de signature et de client SSL.

  Important : Le mode de fonctionnement ne s'applique ni au chiffrement ni à la vérification de signature.
- **Etat** - sélectionnez activé ou désactivé selon que vous souhaitez activer ou désactiver un certificat après téléchargement. Le bouton **Suivant** n'est activé que si le certificat est activé.
- **Gestion d'ensemble** - vous pouvez associer un certificat à un ensemble existant ou créer un nouvel ensemble. Si le certificat est un certificat secondaire, vous ne pouvez l'associer qu'à un ensemble existant. Vous pouvez l'associer à n'importe quel ensemble d'un partenaire interne avec le type chiffrement ou d'un partenaire externe avec le type SSL (autorisation client entrant) ou signature (vérification).

  Remarque : La gestion d'ensemble ne s'applique pas au téléchargement en amont d'un certificat OpenPGP destiné à un partenaire interne,. Pour un chiffrement destiné à un partenaire externe et un certificat de signature ou de client SSL destiné à un partenaire interne, sélectionnez **Ajouter un nouvel ensemble** ou **Mettre à jour un ensemble existant**. Cela s'applique uniquement si vous décidez d'utiliser les ensembles. Sinon, cliquez sur **Terminer**.

8. Cliquez sur **Suivant** pour atteindre la page Ensemble de l'assistant. Si le certificat est un certificat principal, vous n'avez pas besoin de créer d'ensembles et d'associer le certificat à un ensemble et une connexion de participants. Si vous avez coché **Créer un ensemble**, la page **Créer un**

ensemble de l'assistant s'ouvre. Si vous n'avez pas coché cette option, c'est la page **Ajouter à un ensemble existant** qui s'ouvre. Si le fichier contient une clé privée du partenaire interne ou le certificat public du partenaire externe utilisé pour un chiffrement par SSL ou signature numérique, cliquez sur **Terminer**.

Important : Le passage d'un certificat secondaire à un certificat principal n'est pas pris en charge pour les certificats OpenPGP.

9. Dans la page **Créer un ensemble** de l'assistant, entrez les détails concernant le nouvel ensemble. Pour les certificats principaux, vous n'avez pas besoin de créer d'ensemble et d'y associer un certificat. Entrez les valeurs suivantes :
   - **Nom de l'ensemble** - Nom de l'ensemble.
   - **Description** - Description de l'ensemble.
   - **Statut** - Sélectionnez activé ou désactivé. Si le statut est désactivé, le bouton **Suivant** reste inactif.
   - **Paramétrer par défaut** - Cochez cette case si vous voulez que cet ensemble représente l'ensemble par défaut.
10. Dans la page **Ajouter à un ensemble existant**, sélectionnez l'ensemble ou les ensembles à ajouter au certificat. Entrez les valeurs suivantes :
    - **Sélectionner dans la liste des ensembles disponibles pour le type de certificat sélectionné** - Sélectionnez dans la liste l'ensemble ou les ensembles à ajouter au certificat.
    - **Paramétrer par défaut** - Cochez cette case si vous voulez que cet ensemble représente l'ensemble par défaut.
11. Depuis la page **Créer un ensemble** ou **Ajouter à l'ensemble existant**, cliquez sur **Suivant** pour passer à la page **Paramètres par défaut** de l'assistant. Le bouton **Suivant** sera actif si l'ensemble a pour statut activé.
12. Sélectionnez **activé** ou **désactivé** dans **Statut** selon que vous voulez activer ou désactiver le certificat après son téléchargement.

    Remarque : Si vous avez coché **Paramétrer par défaut** à la page précédente (Créer un ensemble ou Ajouter à un ensemble existant), vous devez associer l'ensemble à un mode de fonctionnement. Cela permet un affichage des différentes utilisations selon le mode de fonctionnement utilisé. Le chiffrement sera désactivé pour les partenaires internes. Le client SSL et la signature numérique seront désactivés pour les partenaires externes.
13. Cliquez sur **Suivant** pour passer à la page Configuration. Si vous cliquez sur **Terminer** et qu'il manque certains certificats de Ca racines ou intermédiaires, vous serez invité à procéder à un téléchargement. Si vous cliquez sur "Oui" dans la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur**Annuler** si vous voulez effectuer le téléchargement ultérieurement.
14. Dans la page Configuration, entrez les valeurs suivantes :

    Remarque : Cette page affiche une liste des différentes utilisation des (ensembles de) certificats en fonction du mode de fonctionnement utilisé. Les noms sont déjà pré-remplis mais vous pouvez les redéfinir.
    - **Partenaire source** - Cette zone est pré-remplie et contient la valeur du partenaire interne.
    - **Partenaire cible** - cette liste est pré-remplie et contient tous les partenaires externes. Vous pouvez également sélectionner la valeur "Tout" pour inclure tous les partenaires externes.
    - **Package source** - dans la liste, sélectionnez le package objets de Définitions de flux de documents du partenaire interne.

- **Package cible** -Dans la liste déroulante, sélectionnez Définitions de flux de documents du partenaire externe.

15. Cliquez sur **Ajouter des connexions** si vous voulez associer l'ensemble à d'autres connexions de participants.
16. Cliquez sur **Ajouter un certificat secondaire** pour ajouter un certificat secondaire à l'ensemble actuel.
17. Cliquez sur **Terminer** pour charger le certificat. S'il manque certains certificats de Ca racines ou intermédiaires, vous serez invité à procéder à un téléchargement. Si vous cliquez sur "Oui" dans la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur **Annuler** dans la fenêtre d'invite pour effectuer le chargement ultérieurement.

Remarque : Pour OpenPGP, s'il se produit un échec de téléchargement de certificat malgré le chargement du bon certificat, redémarrez le serveur.

Création d'un ensemble de certificats

Pourquoi et quand exécuter cette tâche

L'ensemble de certificats a été introduit pour les fonctions de sécurité suivantes :

- Authentification client SSL des messages sortants d'un partenaire interne vers un partenaire externe.
- Ajout d'une signature numérique aux messages sortants d'un partenaire interne vers un partenaire externe.
- Chiffrement des messages sortants d'un partenaire interne vers un partenaire externe.
- Les ensembles ne sont pas utilisés pour les scénarios entrants comme la vérification du certificat d'authentification client SSL du partenaire externe dans le magasin de clés certifiées de WebSphere Partner Gateway, la vérification de la signature numérique du partenaire externe et le déchiffrement des messages cryptés destinés au partenaire interne.

Pour créer un ensemble de certificats, procédez comme suit :

1. Dans la console, accédez à **Profil** > **Partenaire** > **Liste des certificats** > **Liste des ensembles de certificats** > **Créer un ensemble**.
2. Cliquez sur **Certificat > Ensembles de certificats > Créer un ensemble**.
3. Entrez le **Nom de l'ensemble** et la **Description** du nouvel ensemble.
4. Définissez le **Type de certificat**.
5. Cochez la case **Activé** ou **Désactivé** pour activer ou désactiver l'**Ensemble de certificats**.
6. Cliquez sur **Charger le certificat**

   Remarque : Les valeurs proposées dans la liste déroulante pour le **Certificat principal** et le **Certificat secondaire** dépendent du **Type de certificat** sélectionné. Si certains certificats déjà créés ne sont pas associés à un ensemble, vous pouvez les ajouter à l'ensemble en cours de création. Si la liste des certificats est vide, la liste déroulante sera vide.
7. Sélectionnez **Certificat principal** et **Certificat secondaire** dans la liste déroulante.
8. Cliquez sur **Sauvegarder**.

Suppression d'un ensemble de certificats

Pourquoi et quand exécuter cette tâche

1. Dans la console, accédez à **Profil** > **Partenaire** > **Liste des ensembles de certificats**. Cette vue répertorie tous les certificats qui ont été créés pour le partenaire.
2. Cliquez sur **Supprimer**. Toutefois, assurez-vous avant d'avoir bien modifié toutes les références à cet ensemble dans la connexion.
3. Si cet ensemble est utilisé par plusieurs connexions, un message d'avertissement s'affiche. Pour vérifier l'emplacement d'utilisation d'un certificat donné, voir «Emplacement d'utilisation d'un certificat».
4. Dans la fenêtre du message d'avertissement, cliquez sur **OK** si vous voulez continuer la suppression ou sur **Annuler** pour l'annuler.

Emplacement d'utilisation d'un certificat

Dans la console, accédez à **Profil** > **{Partenaire}** > **Liste des certificats** > **Liste des ensembles de certificats** > **Cas d'emploi** . La vue qui s'ouvre affiche les détails suivants :

- Partenaire source
- Partenaire cible
- Package source
- Package cible
- Client SSL
- Signature numérique
- Vérification de la signature numérique
- Chiffrement
- Déchiffrement
- Validité.

Remarque : Le certificat peut être non valide pour les raisons suivantes : il n'existe pas de certificat principal, le certificat principal est désactivé, l'ensemble est désactivé, le certificat principal est arrivé à expiration et il n'existe pas de certificat secondaire, les deux certificats, principal et secondaire, sont arrivés à expiration.

Configuration SSL pour un récepteur/une destination de script FTP

Le certificat d'authentification client SSL du récepteur de script FTP est chargé dans le profil de l'opérateur du concentrateur. Même si des certificats sont chargés pour le partenaire interne, il ne supprimera pas par écrasement le paramétrage global.

Ensemble de certificats par défaut fourni pour tous les partenaires internes

WebSphere Partner Gateway prenant en charge plusieurs partenaires internes, chacun d'entre eux doit télécharger des clés privées. Si une organisation souhaite partager un certificat avec ses unités, vous devez le télécharger pour chaque partenaire. Pour simplifier cette opération, vous pouvez fournir une option par défaut permettant à tous les partenaires d'utiliser un même certificat.

Dans la console, accédez à **Certificats** > **Télécharger le certificat**. Téléchargez le certificat et indiquez son type, son utilisation et son mode de fonctionnement. Lorsque vous enregistrez ces informations, le certificat/les clés sont chargés au niveau de l'opérateur du concentrateur. Pendant l'exécution de l'opération, ce certificat par défaut fourni au niveau de l'opérateur du concentrateur est utilisé en l'absence de tout certificat.

Récapitulatif des certificats

Le tableau 32 résume l'utilisation des certificats dans WebSphere Partner Gateway. L'emplacement des certificats est indiqué entre parenthèses "( )".

Tableau 32. Informations récapitulatives concernant les certificats

Mode de livraison des messages (voir la note 1)	**Certificat d'opérateur du concentrateur**	**Obtention du certificat et de l'autorité de certification du partenaire**	**CA (voir note 2)**	**Envoi du certificat au partenaire (voir note 3)**	**Commentaires**
SSL entrant	S'installe sur le SSL WebSphere Application côté serveur (dans le magasin de clés de WebSphere Application Server).	Certificat auto-signé du partenaire.	Ne sert que si l'authentification du client est utilisée (mettez le CA ou le certificat d'auto-signature dans le magasin de relations de confiance de WebSphere Application Server).	Le certificat de l'opérateur du concentrateur s'il est auto-signé ou le certificat racine de CA, le cas échéant, s'il est authentifié par l'autorité de certification.	
SSL sortant	Si l'authentification du client est utilisée. (WebSphere Partner Gateway)	Certificat côté serveur du partenaire ou certificat racine de CA, s'il est authentifié par une autorité de certification.	WebSphere Partner Gateway	Le certificat de l'opérateur du concentrateur s'il est auto-signé ou le certificat du CA s'il est signé par un tiers.	
Déchiffrement entrant	Clé privée (WebSphere Partner Gateway)	N/D	Si le certificat est signé par le CA, les certificats CA doivent être téléchargés en tant que certificats racine/ intermédiaire.	Certificat d'opérateur du concentrateur	Pour déchiffrer le message
Vérification de la signature numérique entrant	N/D	Certificat nécessaire pour valider le certificat qui a servi à la signature numérique. (WebSphere Partner Gateway)	WebSphere Partner Gateway	N/A	Pour vérification et irréfutabilité

Tableau 32. Informations récapitulatives concernant les certificats (suite)

Mode de livraison des messages (voir la note 1)	Certificat d'opérateur du concentrateur	Obtention du certificat et de l'autorité de certification du partenaire	CA (voir note 2)	Envoi du certificat au partenaire (voir note 3)	Commentaires
Chiffrement sortant	N/D	Utilisez le certificat obtenu du partenaire (le certificat est installé dans le profil du partenaire).	La chaîne de certificats de CA du certificat client si elle n'est pas auto-signée	N/D	Pour le chiffrement des messages sortants
Signature sortante	Clé privée et certificat (WebSphere Partner Gateway)	N/D	Chaîne de certificats de CA.	Facultatif, dépend du partenaire ; fournissez le certificat de WebSphere Partner Gateway	
Certificat pour validation d'ID entreprise	N/D	Charger dans le profil du partenaire			Valide que ce certificat est bien pour cet ID entreprise lors du contrôle SSL client.

Remarques :

1. Un message entrant est un message qui arrive dans WebSphere Partner Gateway, en provenance d'un partenaire. Un message sortant quitte WebSphere Partner Gateway, vers un partenaire.
2. Si le certificat est émis par une CA, il faut obtenir et conserver le certificat de cette autorité de certification. Ceci s'applique au certificat de l'opérateur du concentrateur ou au certificat du partenaire.
3. Si une clé privée est impliquée, ce certificat lui correspond.

Utilisation du certificat et de la clé PEM formatés avec WebSphere Partner Gateway

Cette section offre des informations sur l'utilisation des certificats et des clés PEM encodés.

Utilisation de la clé PEM privée formatée

Si vous avez une clé privée au format PEM et voulez la télécharger dans WebSphere Partner Gateway, le téléchargement n'est possible que si la clé privée est convertie au format PKCS#8.

Pour cela, vous pouvez utiliser l'outil OpenSSL.

Utilisez cette commande pour convertir une clé formatée PEM au format PKCS#8 :

```
openssl pkcs8 -topk8 -in usr.key -out usr.p8 -outform DER
```

Cette commande fonctionne sur les clés créées à l'aide d'OpenSSL.

OpenSSL est disponible avec les versions de Linux et peut également être téléchargé depuis le site Web http://www.openssl.org.

Utilisation du certificat PEM formaté

Le certificat peut être téléchargé dans WebSphere Partner Gateway au format PEM. Il fonctionne pour un certificat formaté PEM généré à l'aide d'OpenSSL.

Certificat chiffré PKCS#7 avec WebSphere Partner Gateway

Pourquoi et quand exécuter cette tâche

Sous Windows, si vous avez des certificats encodés au format PKCS#7 (fichier .p7b), suivez la procédure ci-dessous pour extraire les certificats du fichier .p7b :

1. Cliquez deux fois sur le fichier .p7b.
2. Dans le panneau de navigation, développez l'arborescence et cliquez sur **Certificats**. La liste des certificats contenus dans le fichier s'affiche sur la partie droite.
3. Pour copier un certificat dans le système de fichiers, cliquez deux fois sur le certificat. Les détails du certificat s'affichent.
4. Dans les détails du certificat, cliquez sur l'onglet **Détails**.
5. Cliquez sur **Copier vers le fichier** pour copier le fichier vers le système de fichiers.
6. Exportez le certificat en tant que fichier encodé DER.

Chargement de clés SFTP

Etapes pour charger des clés SFTP.

Pourquoi et quand exécuter cette tâche

Pour charger des clés SFTP, procédez comme suit :

1. Naviguez jusqu'à **Administrateur du compte** > **Profils** > **Certificats**.
2. Cliquez sur **Charger des clés SFTP**.
3. Dans la page **Charger des clés SFTP**, cliquez sur **Parcourir** et sélectionnez le fichier de clés depuis votre ordinateur local. Le fichier téléchargé est utilisé pour l'authentification par clé. L'icône **Données indiquées** signale qu'une clé est déjà téléchargée

Conformité aux normes de sécurité FIPS

WebSphere Partner Gateway répond aux normes FIPS (Federal Information processing Standard) et FIPS 140-2. **IBMJCEFIPS** est le fournisseur JCE répondant aux normes FIPS. Le fournisseur **IBMJSSE2 JSSE** utilise **IBM JCE** et ne contient pas de code pour la cryptographie. Il n'est donc pas nécessaire pour la certification de la conformité à la norme FIPS. Bien que le fournisseur **IBMJSSEFIPS JSSE** soit conforme à FIPS, utilisez le fournisseur **IBMJSSE2** dans WebSphere Partner Gateway. **IBMJSSE2** est le dernier fournisseur, il prend en charge plus d'algorithmes et a une maintenabilité améliorée. Le produit peut être exécuté en mode FIPS ou pas. Si le mode FIPS est configuré et qu'un algorithme validé non FIPS est utilisé, une erreur d'événement est générée et la transaction du document est arrêtée. L'algorithme PKCS#12 n'étant pas validé FIPS, il n'est pas possible de télécharger les fichiers PKCS#12 en mode FIPS. Pour configurer WebSphere Partner Gateway en mode FIPS ou en mode par défaut, vous devez être administrateur. En mode FIPS, il est possible de télécharger PKCS#12 sur la console de WebSphere

Partner Gateway au format JCEKS ou JKS à l'aide de l'utilitaire iKeyman.

Le mode FIPS prend en charge les fichiers de clés JKS, JCEKS et OpenPGP, mais pas les fichiers de clés PKCS#12. A partir de la console, vous pouvez télécharger un certificat et saisir le format JKS, JCEKS ou OpenPGP. Sur l'écran **Téléchargement du fichier de clés**, sélectionnez le format dans la liste **Format du fichier de clés**. Les valeurs disponibles dans la liste **Format du fichier de clés** sont : PKCS#12, JKS, JCEKS et OpenPGP.

Configuration de WebSphere Partner Gateway en mode FIPS

Pourquoi et quand exécuter cette tâche

Pour configurer WebSphere Partner Gateway en mode FIPS, procédez comme suit :

1. Définissez les fournisseurs FIPS dans le fichier **java.security**.
2. Définissez la propriété système **bcg.FIPSMode** sur "vrai" dans la Console de WebSphere Partner Gateway.
3. Dans le fichier java.security, vous devez définir le fournisseur IBMJCEFIPS avant le fournisseur IBMJCE. Ce fichier se trouve dans le répertoire <WAS Installation>/java/jre/lib/security directory.
4. Définissez les classes de fabrique de sockets FIPS activés pour la fabrique de socket JSSE et la fabrique de socket du serveur.
5. Redémarrez tous les serveurs.

   Remarque : Un événement d'information est généré indiquant que le produit est exécuté en mode FIPS.

Configuration de WebSphere Partner Gateway en mode par défaut

Pourquoi et quand exécuter cette tâche

Pour configurer WebSphere Partner Gateway en mode par défaut, procédez comme suit :

1. Définissez la propriété système **bcg.FIPSMode** sur "Faux" dans la console de WebSphere Partner Gateway.
2. Réinitialisez les paramètres pour la fabrique de sockets JSSE, la fabrique de sockets du serveur et les fournisseurs dans le fichier **java.security** comme indiqué ci-dessous :
   a. Supprimez la propriété système **com.ibm.jsse2.JSSEFIPS=true** à partir des propriétés JVM génériques pour chaque serveur.
   b. Réinitialisez les valeurs des propriétés suivantes sur leurs valeurs d'origine :
      - ssl.SocketFactory.provider
      - ssl.SocketFactory.provider
   c. Pour chaque installation WAS, commentez le fournisseur IBMJCEFIPS et renumérotez les fournisseurs, en partant de 1, dans le fichier **java.security**.
3. Redémarrez tous les serveurs.

   Remarque : Un événement d'information est généré indiquant le mode utilisé. En mode par défaut, il est possible d'utiliser tous les algorithmes pris en charge, y compris les algorithmes validés non FIPS.

Configuration des fournisseurs JSSE d'IBM en mode FIPS

Pourquoi et quand exécuter cette tâche

Pour configurer les fournisseurs JSSE d'IBM en mode FIPS, procédez comme suit :

1. Définissez la propriété système **com.ibm.jsse2.JSSEFIPS** sur "Vrai". Pour pouvez effectuer cette opération en définissant les propriétés système JVM pour le serveur d'applications utilisant la console d'administration WAS. Naviguez jusqu'à la page <Serveur>/Java et Gestion de processus/Définition de processus/Machine virtuelle Java et spécifiez la propriété **-Dcom.ibm.jsse2.JSSEFIPS=true**. Ce paramètre doit être défini sur chaque serveur.
2. Définissez les propriétés de sécurité suivantes pour le fournisseur IBMJSSE2 afin que toutes les demandes JSSE puissent être traitées :
   - ssl.SocketFactory.provider = com.ibm.jsse2.SSLSocketFactoryImpl
   - ssl.ServerSocketFactory.provider = com.ibm.jsse2.SSLServerSocketFactoryImpl
3. Ajoutez le fournisseur IBMJCEFIPS, com.ibm.crypto.fips.provider.IBMJCEFIPS, à la liste de fournisseurs avant le fournisseur IBMJCE. Ne supprimez pas IBMJCE car il est requis pour la prise en charge du fichier de clés.

   Remarque : Seul le protocole TLS est pris en charge lorsqu'IBMJSSE2 est en mode FIPS.

Algorithmes pris en charge en mode FIPS et mode non FIPS

Les algorithmes suivants sont pris en charge en mode FIPS :

- Diffie-Hellman
- RSA, DSA
- SHA-1, SHA-384, SHA-224, SHA-512
- AES, DES, TDES (Triple DES)
- FIPS 186-2 – Algorithme pour la génération de nombres pseudo aléatoires (PRNG)
- Protocole TLS : TLSv1
- Format de fichier de clés : JKS, JCEKS

Les algorithmes suivants sont pris en charge dans WebSphere Partner Gateway :

- Cryptographie asymétrique : RSA, DSA
- Fonction de hachage : SHA-1, MD5, SHA-384, SHA-224, SHA-512, RIPEMD/160.
- Cryptographie symétrique : AES, DES, 3DES, RC2 (tous avec le mode CBC), CAST5, Blowfish, Twofish.
- PRNG: IBMSecureRandom
- Algorithme de signature : dsa-sha1, rsa-sha1
- Protocole TLS : SSLv3, TLSv1
- Format de fichier de clés : PKCS#12, JKS, JCEKS, OpenPGP
- Algorithmes à clé symétrique : AES et TripleDES avec détection des modifications.

  Restriction : Vous pouvez utiliser les algorithmes TripleDES et AES uniquement lorsque les modes détection des modifications et FIPS sont tous deux définis.

Les algorithmes suivants ne sont pas pris en charge en mode FIPS mais le sont dans WebSphere Partner Gateway :

- Fonction de hachage : MD5. RIPEMD160
- Cryptographie symétrique : RC2, CAST5, Blowfish, Twofish
- Fournisseur PRNG IBMSecureRandom (tous les chemins de WebSphere Partner Gateway).
- Protocole TLS : SSLv3
- Format de fichier de clés : PKCS# 12

Chapitre 14. Gestion des alertes

Les alertes de WebSphere Partner Gateway servent à avertir le personnel clé au sujet de fluctuations inhabituelles dans le volume de transmissions que vous recevez, ou lorsque des erreurs de traitement de documents métier ont lieu.

Une aide dans le module Afficheur, Afficheur d'événements, vous aide à mieux identifier, diagnostiquer et réparer les erreurs de traitement.

Présentation des alertes

Une alerte consiste en un message envoyé par courrier électronique aux contacts souscrits ou à une liste de distribution du personnel clé. Les alertes sont basée sur l'occurrence d'un événement système (alerte basée sur l'événement) ou sur le volume du flux de documents prévu (alerte basée sur le volume).

- Utilisez une **alerte basée sur le volume** pour recevoir une notification d'augmentation ou de baisse du volume de transmissions.

  Par exemple, si vous êtes un partenaire externe, vous pouvez créer une alerte basée sur le volume qui vous avertit lorsque vous ne recevez aucune transmission du partenaire interne lors d'un jour ouvrable (sélectionnez Aucun volume pour le Volume, Quotidien pour la fréquence et Lun à Ven dans l'option Jours de la semaine). Cette alerte peut mettre en évidence les difficultés de transmission du réseau du partenaire interne.

  Si vous êtes un partenaire externe, vous pouvez également créer une alerte basée sur le volume pour vous avertir lorsque le nombre de transmissions du partenaire interne dépasse le taux normal. Par exemple, si vous recevez habituellement environ 1000 transmissions par jour, vous pouvez définir le Volume prévu sur 1000 et l'Ecart de pourcentage sur 25%. L'alerte vous avertira lorsque vous recevrez plus de 1250 transmissions par jour (ainsi que lorsque vous recevrez moins de 750 transmissions par jour). Cette alerte peut identifier une demande accrue du partenaire interne, susceptible, à long terme, d'exiger une augmentation du nombre de serveurs dans votre environnement. Pour plus d'informations sur les alertes basées sur le volume, consultez « Création d'une alerte dépendant du volume», à la page 311.

  Remarque :

  1. Les alertes basées sur le volume contrôlent celui-ci en fonction du type de document que vous sélectionnez lorsque vous créez l'alerte. WebSphere Partner Gateway n'examine que les documents qui contiennent le type de document sélectionné dans votre alerte et ne génère d'alerte que lorsque tous les critères d'alerte sont atteints.
  2. Le partenaire externe peut uniquement créer une alerte basée sur le volume par rapport au volume de documents envoyés au partenaire interne. Pour pouvoir établir une alerte basée sur le volume de documents reçus depuis le partenaire interne vers le partenaire externe, ce dernier doit demander à l'administrateur du concentrateur de configurer pour lui une alerte basée sur le volume, en spécifiant le partenaire externe comme propriétaire de cette alerte. Un partenaire externe peut également créer des alertes basées sur le volume à envoyer aux partenaires externes.
- Utilisez une **alerte basée sur l'événement** pour recevoir une notification lorsque des erreurs se produisent dans le traitement du document. Par exemple, vous

pouvez vouloir créer une alerte pour vous prévenir lorsque le traitement de votre document échoue en raison d'erreurs de validation ou parce que des document ont été reçus en double. Vous pouvez également créer des alertes vous informant lorsqu'un certificat est sur le point d'expirer.

Vous utiliserez les codes événement prédéfinis par WebSphere Partner Gateway pour créer les alertes basées sur l'événement. Il existe cinq types d'événement : Débogage, Informations, Avertissement, Erreur, Critique. Chaque type d'événement englobe de nombreux événements. Vous pouvez afficher et sélectionner des événements prédéfinis sur Alerte : page Evénements. Par exemple : 240601 Echec de la reprise AS ou 108001 Il ne s'agit pas d'un certificat. Pour plus d'informations sur les alertes basées sur les événements, voir « Création d'une alerte de type événement», à la page 313.

Conseil :

- Utilisez une alerte basée sur le volume pour recevoir une notification si le volume de transmission du partenaire interne ou externe prévu devient inférieur aux limites d'exploitation. Cette alerte peut mettre en évidence les difficultés de transmission du réseau du partenaire interne ou externe.
- Utilisez une alerte basée sur l'événement pour recevoir une notification des erreurs dans le traitement des documents. Par exemple, vous pouvez créer une alerte basée sur l'événement qui vous prévient si le traitement de votre document échoue en raison d'erreurs de validation.

Remarque : Pour envoyer des alertes, vous devez configurer un serveur e-mail pour les alertes. Les alertes sont configurées sur la page Attributs du moteur d'alertes à laquelle on accède en cliquant sur **Administration système** > **Administration du gestionnaire de documents** > **Moteur d'alerte**. Pour plus d'informations sur la configuration du serveur e-mail d'alerte, voir "Mise à jour des adresses mail d'alerte" dans le *Guide du partenaire WebSphere Partner Gateway* .

Affichage ou édition des caractéristiques et contacts

Pourquoi et quand exécuter cette tâche

Le partenaire interne peut afficher toutes les alertes, quel que soit le propriétaire de l'alerte (le créateur de l'alerte).

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte. Vous pouvez aussi cliquer sur **Rechercher** sans sélectionner de critère de recherche (le système affiche toutes les alertes).
3. Cliquez sur **Rechercher**. Le système affiche la page Résultats de la recherche d'alerte.
4. Cliquez sur l'icône Afficher les détails pour visualiser les détails d'une alerte.
5. Cliquez sur l'icône Editer pour éditer les détails d'une alerte.
6. Editez les informations si nécessaire.
7. Cliquez sur l'onglet **Notification**.
8. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement). Le partenaire interne peut afficher toutes les alertes, quel que soit le propriétaire de l'alerte.
9. Si vous le souhaitez, éditez les contacts pour cette alerte.
10. Cliquez sur **Sauvegarder**.

Recherche d'alertes

Pourquoi et quand exécuter cette tâche

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte. Vous pouvez aussi cliquer sur **Rechercher** sans sélectionner de critère de recherche (le système affiche toutes les alertes).

Tableau 33. Critères de recherche d'alerte pour les partenaires

Valeur	Description
Type d'alerte	Alerte de volume, d'événement ou tous les types d'alerte.
Nom de l'alerte	Nom de l'alerte.
Etat de l'alerte	Alertes activées, désactivées ou toutes les alertes.
Contrats souscrits	Contacts affectés à l'alerte. Vous pouvez sélectionner Présence d'abonnés, Aucun abonné ou Tout.
Résultats par page	Contrôle le mode d'affichage des résultats de la recherche.

Tableau 34. Critères de recherche d'alerte pour le partenaire interne et l'administrateur du concentrateur

Valeur	Description
Propriétaire de l'alerte	Créateur de l'alerte.
Partenaire d'alerte	Partenaire auquel s'applique l'alerte.
Type d'alerte	Alerte de volume, d'événement ou tous les types d'alerte.
Nom de l'alerte	Nom de l'alerte.
Etat de l'alerte	Alertes activées, désactivées ou toutes les alertes.
Contrats souscrits	Contacts affectés à l'alerte. Vous pouvez sélectionner Présence d'abonnés, Aucun abonné ou Tout.
Résultats par page	Contrôle le mode d'affichage des résultats de la recherche.

3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.

Désactivation ou activation d'une alerte

Procédure

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte.
3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.
4. Localisez l'alerte et cliquez sur **Désactivé** ou **Activé** sous Etat. Seuls l'administrateur du concentrateur et le propriétaire de l'alerte (le créateur de l'alerte) ont le droit d'éditer le statut de l'alerte.

Retrait d'une alerte

Procédure

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte.

2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le **Nom de l'alerte**.
3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.
4. Localisez l'alerte et cliquez sur l'icône Supprimer pour la supprimer. Seuls l'administrateur du concentrateur et le propriétaire de l'alerte (le créateur de l'alerte) peuvent supprimer une alerte.

Ajout d'un contact à une alerte existante

Pourquoi et quand exécuter cette tâche

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et saisissez le Nom de l'alerte.
3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.
4. Cliquez sur l'icône Afficher les détails pour visualiser les détails des alertes.
5. Cliquez sur l'icône Editer pour éditer les détails d'une alerte.
6. Cliquez sur l'onglet **Notification**.
7. Sélectionnez un partenaire (uniquement un partenaire interne ou un administrateur du concentrateur).
8. Si le contact à ajouter se trouve dans la zone de texte Contacts, sélectionnez-le et cliquez sur **Abonner**. Allez à l'étape 13.

   Si le contact à ajouter ne se trouve pas dans la zone de texte Contacts, cliquez sur **Ajouter une nouvelle entrée aux contacts**. Le système affiche la fenêtre instantanée Création d'un contrat.

   Notez que le lien Ajouter une nouvelle entrée aux contacts est disponible uniquement si le partenaire est l'opérateur concentrateur.
9. Saisissez le nom, l'adresse électronique et les numéros de téléphone et de télécopie du contact.
10. Choisissez l'état de l'alerte du contact.
    - Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.
    - Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.
11. Choisissez le niveau de visibilité du contact.
    - Sélectionnez **Local** pour que ce contact soit vu uniquement par votre organisation.
    - Sélectionnez **Global** afin de rendre le contact visible pour l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux souscrire le contact aux alertes.
12. Cliquez sur **Sauvegarder** pour sauvegarder le contact. Cliquez sur **Sauvegarder et souscrire** pour sauvegarder le contact et l'ajouter à la liste des contacts pour cette alerte.
13. Cliquez sur **Sauvegarder**.

Création d'une alerte dépendant du volume

Pourquoi et quand exécuter cette tâche

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte.
2. Cliquez sur **Créer** dans l'angle supérieur droit de la page. Le système affiche l'onglet de définition des alertes.
3. Sélectionnez **Alerte de volume** comme **Type d'alerte** (il s'agit de la configuration par défaut). Le système affiche les zones de texte appropriées pour une alerte de volume.
4. Entrez un **Nom d'alerte** pour l'alerte.
5. Entrez le **texte commercial personnalisé**. Lorsque l'événement d'alerte est généré, ce message sera également envoyé.
6. Sélectionnez un **Propriétaire d'alerte** pour l'alerte.
7. Sélectionnez un **Partenaire** disposant des droits permettant de créer une alerte basée sur le volume (uniquement un partenaire interne ou un administrateur du concentrateur).
8. Sélectionnez **Package**, **Protocole** et **Type de document** à partir des listes déroulantes. Le Package, le Protocole et le Type de document sélectionnés doivent correspondre au Package, au Protocole et au Type de document du partenaire externe source.
9. Sélectionnez une des trois options de volume (Prévu, Intervalle ou Aucun volume) puis allez à l'étape 10, à la page 312 :
   - **Prévu** - Sélectionnez Prévu si vous voulez qu'une alerte soit générée lorsque le volume du type de document s'écarte d'une quantité précise. Suivez les étapes ci-après pour créer une alerte sur un volume de type de document prévu :
     a. Dans la zone de texte Volume, saisissez le nombre de types de document que vous prévoyez de recevoir dans le laps de temps sélectionné à 10, à la page 312. Saisissez uniquement un nombre positif : l'alerte ne fonctionnera pas si vous saisissez un nombre négatif.
     b. Dans la zone de texte Ecart en pourcentage, saisissez un nombre définissant la limite dans laquelle le volume du type de document peut varier avant que l'alerte ne soit activée. Par exemple :
        – Si la zone de texte Volume a pour valeur 20 et que celle d'Ecart de pourcentage a pour valeur 10, un volume de flux de documents inférieur à 18 ou supérieur à 22 déclenchera une alerte.
        – Si la zone de texte Volume a pour valeur 20 et que celle d'Ecart de pourcentage a pour valeur 0, tout volume de flux de documents qui n'est pas égal à 20 déclenchera une alerte.
   - **Intervalle**. Sélectionnez Plage pour qu'une alerte soit déclenchée si le volume du flux de documents sort d'une plage minimale-maximale. Suivez les étapes suivantes pour créer une alerte basée sur une intervalle de valeurs :
     a. Dans la zone de texte Min, saisissez le nombre minimal de flux de documents que vous prévoyez de recevoir durant le laps de temps sélectionné à l'étape 10, à la page 312. L'alerte ne sera déclenchée que si le volume du flux de documents descend en dessous de ce nombre.
     b. Dans la zone de texte Max, saisissez le nombre maximal de flux de documents que vous prévoyez de recevoir durant le laps de temps sélectionné à l'étape 10, à la page 312.

Remarque : Les zones de texte Min et Max doivent être toutes les deux complétées lors de la création d'une alerte basée sur une plage de volume.

- **Aucun volume**. Sélectionnez Aucun volume pour qu'une alerte soit déclenchée si aucun flux de documents ne se présente dans le laps de temps défini à l'étape 10.

10. Sélectionnez Quotidien ou Intervalle pour le laps de temps (Fréquence) qui servira au système pour contrôler le volume du flux de documents et générer une alerte le cas échéant.
    - **Quotidien**. Sélectionnez Quotidien pour contrôler le volume du flux de documents sur un ou plusieurs jours ouvrables de la semaine ou du mois. Par exemple, sélectionnez Quotidien si vous voulez contrôler le volume du flux de documents sur un ou plusieurs jours spécifiques de la semaine (par exemple le lundi ou le lundi et le jeudi) ou du mois (par exemple le 1er et le 15 du mois).
    - **Intervalle**. Sélectionnez Intervalle pour contrôler le volume du flux de documents entre deux jours de la semaine ou du mois. par exemple, sélectionnez Intervalle pour contrôler le volume du flux de documents sur tous les jours entre le lundi et le vendredi ou sur tous les jours entre le 5 et le 20 du mois.
11. Sélectionnez l'**Heure de début** et de **Fin** (journée de 24 heures) du contrôle, par le système, du volume du flux de documents pour les jours sélectionnés dans l'étape suivante. Notez que lorsqu'une fréquence d'Intervalle est sélectionnée, le volume du flux de documents est contrôlé à partir de l'Heure de début du premier jour de l'intervalle jusqu'à l'Heure de fin du dernier jour de l'intervalle.
12. Sélectionnez les jours appropriés de la semaine ou du mois pendant lesquels le contrôle de l'alerte aura lieu. Si vous avez choisi la fréquence Quotidien, sélectionnez les jours ouvrables de la semaine ou les jours du mois pendant lesquels le contrôle de l'alerte aura lieu. Si vous avez choisi la fréquence Plage, sélectionnez deux jours de la semaine ou du mois entre lesquels le contrôle de l'alerte aura lieu.
13. Sélectionnez l'**Etat de l'alerte** sur Activé ou Désactivé pour cette alerte.
14. Cliquez sur **Sauvegarder**.
15. Cliquez sur l'onglet **Notification**.
16. Cliquez sur l'icône **Edition**.
17. Sélectionnez un **Partenaire** (uniquement un partenaire interne et un administrateur du concentrateur).
18. Si le contact à ajouter se trouve dans la zone de texte Contacts, sélectionnez-le et cliquez sur **Abonner**. Allez à l'étape 23, à la page 313.

    Si le contact à ajouter ne se trouve pas dans la zone de texte Contacts, cliquez sur **Ajouter une nouvelle entrée aux contacts**. Le système affiche la fenêtre instantanée Création d'un contrat.

    Notez que l'option Ajouter une nouvelle entrée aux contacts est uniquement présentée au Propriétaire de l'alerte pour créer des contacts qui lui sont associés. Cette fonction ne permet pas au Propriétaire de l'alerte d'ajouter des contacts pour les partenaires d'alerte.
19. Entrez le**nom**, l'**adresse électronique** et les numéros de **téléphone** et de **télécopie** du contact.
20. Choisissez l'**Etat de l'alerte** du contact.
    - Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.

- Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.

21. Choisissez le niveau de visibilité du contact.
    - Sélectionnez **Local** pour que ce contact soit vu uniquement par votre organisation.
    - Sélectionnez **Global** pour que ce contact soit visible par l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux abonner le contact aux alertes.
22. Cliquez sur **Sauvegarder** pour sauvegarder le contact ; cliquez sur **Sauvegarder & Souscrire** pour ajouter le contact à la liste des contacts pour cette alerte.
23. Cliquez sur **Sauvegarder**.

    Remarque : Les modifications effectuées sur les alertes basées sur le volume après la période de contrôle originale prennent effet à la période de contrôle suivante. Par exemple : une alerte effectue un contrôle entre 13h et 15h tous les mercredis et jeudis. Un mercredi à 16h, l'alerte est modifiée de façon à effectuer son contrôle entre 17h et 19h. L'alerte n'effectuera pas de contrôle le jour même : la modification prendra effet le jeudi suivant.

Création d'une alerte de type événement

Pourquoi et quand exécuter cette tâche

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte.
2. Cliquez sur **Créer** dans l'angle supérieur droit de la page. Le système affiche l'onglet de définition des alertes.
3. Sélectionnez **Alerte d'événement** comme **Type d'alerte**. Le système affiche les zones de texte appropriées pour une alerte basée sur l'événement.
4. Saisissez un **Nom d'alerte** pour l'alerte.
5. Entrez le **texte commercial personnalisé**. Lorsque l'événement d'alerte est généré, ce message sera également envoyé.
6. Sélectionnez un **Propriétaire d'alerte** pour l'alerte.
7. Sélectionnez un **Partenaire** qui déclenchera l'alerte (cette option n'est disponible que pour le partenaire interne et l'administrateur du concentrateur). Sélectionnez l'option Tout partenaire pour associer l'alerte à tous les partenaires du système. Lorsque vous effectuez une recherche d'alerte et que vous sélectionnez Tout partenaire comme partenaire de l'alerte, le système affiche toutes les alertes qui ne sont pas associées à un partenaire spécifique.
8. Sélectionnez le **Type d'événement**: Débogage, Information, Avertissement, Erreur, Critique ou Tous.
9. Sélectionnez le **Nom d'événement** qui activera l'alerte, par exemple, BCG240601 Echec de la reprise AS, ou 108001 Il ne s'agit pas d'un certificat. Pour créer une alerte qui vous informe lorsqu'un certificat est sur le point d'expirer, sélectionnez une des propositions suivantes :
    - BCG108005 Le certificat expire dans 60 jours
    - BCG108006 Le certificat expire dans 30 jours
    - BCG108007 Le certificat expire dans 15 jours
    - BCG108008 Le certificat expire dans 7 jours
    - BCG108009 Le certificat expire dans 2 jours

Remarque : Afin qu'un événement soit indiqué ici, il doit pouvoir faire l'objet d'une alerte. Pour associer une alerte à un événement, voir «Définition des événements pouvant faire l'objet d'une alerte», à la page 322.

10. Sélectionnez l'état de cette alerte : Activé ou Désactivé.
11. Cliquez sur **Sauvegarder**.
12. Cliquez sur l'onglet **Notification**.
13. Sélectionnez le **Mode de notification** : Avertir toutes les parties associées ou Avertir uniquement les contacts abonnés. Les contacts abonnés sont notifiés par ***Avertir uniquement les contacts abonnés***. Lors de la création d'alertes, si le mode de notification d'alertes est sélectionné sur ***Avertir toutes les parties associées***, alors la notification est envoyée à toutes les parties associées à l'événement pour lequel l'alerte est définie. Les parties associées pour l'événement correspondent aux contacts combinés de Participant source, Participant cible et Propriétaire d'alerte.
14. Sélectionnez un **Partenaire** (uniquement un partenaire interne et un administrateur du concentrateur).
15. Dans les contacts indiqués dans la zone de texte **Contacts**, sélectionnez le contact que vous voulez avertir et cliquez sur **Abonner**.
16. Sélectionnez le mode de livraison :
    - **Envoi d'alertes immédiat**. Lorsque vous sélectionnez cette option, le système envoie des notifications d'alerte au contact au moment ou l'alerte se déclenche. Utilisez cette option pour les alertes critiques.
    - **Alertes de lot par**. Lorsque vous sélectionnez cette option, vous pouvez préciser à quel moment vous souhaitez que le contact reçoive la notification d'alerte. Utilisez cette option pour les alertes qui ne sont pas critiques.

      Les deux options de cette section, Nombre et Heure, ne s'excluent pas mutuellement.

      Si vous sélectionnez l'option **Nombre**, vous devez toujours sélectionner l'option Heure.
      - Si nombre d'alertes (Nombre) est atteint pendant le délai que vous avez sélectionné (Heure), le système génère une notification d'alerte.
      - Si une alerte a lieu mais que le nombre d'alertes (Nombre) n'est pas atteint pendant le délai que vous avez sélectionné (Heure), le système générera une notification d'alerte à la fin du délai.

      L'option **Heure** peut être utilisée sans l'option Nombre, mais l'option Nombre doit toujours être associée à une limite de temps (Heure).
      - **Nombre**. Vous devez aussi utiliser l'option Heure lorsque vous sélectionnez cette option. Saisissez un nombre (n). C'est le nombre d'alertes qui doivent avoir lieu pendant le délai sélectionné (Heure) pour que le système envoie une notification d'alerte au contact de l'alerte.

        Voici un exemple de la manière dont ces deux options fonctionnent ensemble :

        Dans notre exemple, les options Alertes de lot par se voient affecter la valeur de 10 pour le Nombre (10 alertes) et de 2 pour l'Heure (délai de 2 heures). Le système conserve toutes les notifications pour cette alerte jusqu'à ce que 10 alertes aient lieu dans un délai de 2 heures ou bien jusqu'à ce que la fin du délai soit atteint.

        Lorsque le nombre de 10 alertes est atteint dans un délai de 2 heures, le système envoie toutes les notifications d'alerte au contact.

Si une alerte a lieu mais que le nombre de 10 alertes n'est pas atteint pendant le délai (2 heures), le système enverra une notification d'alerte au contact à la fin du délai.

- **Heure**. Sélectionnez le nombre d'heures (n). Le système conserve la notification d'alerte pendant n heures. Toutes les n heures, le système envoie toutes les notifications conservées au contact.

  Par exemple, si vous tapez 2, le système conserve toutes les notifications pour cette alerte qui ont lieu dans chaque intervalle de deux heures. Lorsque l'intervalle de 2 heures est expirée, le système envoie toutes les notifications d'alerte au contact.

17. Cliquez sur **Sauvegarder**.

Chapitre 15. Lancement du flux d'erreur

Dans WebSphere Partner Gateway, vous pouvez surveiller, en tant qu'administrateur, les erreurs d'événements se produisant au cours du traitement des documents. Une erreur de document peut se produire au niveau du récepteur ou du gestionnaire de documents. L'erreur ou l'événement critique est consignée dans Event Engine. Il est possible de créer des alertes pour envoyer des notifications par e-mail à un ou plusieurs abonnés.

Par ailleurs, un administrateur peut lancer un flux de document d'erreur pour les partenaires internes, externes ou les deux. Ce flux sera initié pour une erreur de document en se basant sur l'erreur ou l'événement critique. Il peut être au format de WebSphere Partner Gateway ou du service Web. Vous pouvez configurer le format d'un événement dans la configuration des flux d'erreur.

Configuration du document de flux d'erreur

Pourquoi et quand exécuter cette tâche

L'onglet Flux d'erreur de la console permet à l'opérateur de définir l'appel du flux d'erreur ou du service Web pour certaine erreurs d'événement :

1. Accédez à l'onglet **Administrateur de compte** > **Flux d'erreur**. La liste des flux d'erreur comporte les icônes Afficher et Supprimer pour chacun des flux.
2. Cliquez sur l'icône **Afficher** pour lancer l'écran de configuration des flux d'erreur en lecture seule.
3. Dans la configuration de la vue, cliquez sur **Editer** pour modifier la configuration du flux d'erreur.
4. En mode édition, les valeurs de configuration disponibles sont les suivantes :
   - **Nom** - nom de configuration du document de flux d'erreur.
   - **Partenaire expéditeur** - Cliquez sur la recherche de partenaire et sélectionnez le nom du partenaire. Celui-ci peut être un partenaire interne ou externe.
   - **Type de partenaire** - Sélectionnez le type de partenaire dans la liste déroulante.
   - **Erreur d'événement** - Cette liste déroulante comprend uniquement les événements de type *Erreur* ou *Critique*.
   - **Type de flux d'erreur** - Ce peut être *Document de flux d'erreur* ou *Appeler un service Web*.
   - **Envoyer à** - sélectionnez les destinataires de l'erreur de document. Il s'agit d'un *Expéditeur* ou d'un *Récepteur* ou *Les deux*.
5. Cliquez sur **Sauvegarder**.
6. Cliquez sur **Annuler** pour annuler.
7. Activez les fonctionnalités B2B pour le flux d'erreur configuré.
8. Si le service Web est appelé, créez alors l'interaction et activez la connexion Participant.

Les définitions de documents de flux d'erreur pour XML et le service Web sont téléchargés par défaut dans WebSphere Partner Gateway. Vous pouvez les activer pour les partenaires et établir les connexions suivantes :

- Connexion XML de ErrorFlowDocument.
- ErrorFlowDocument sur les services Web pour le style de document.
- ErrorFlowDocument sur les services Web pour le style RPC.

Limitations et restrictions

1. Les limitations suivantes s'appliquent au document de flux d'erreur via les services Web :
   - Les demandes des services Web doivent être des demandes unilatérales.
   - Si le style de liaison est **document**, alors le type de paramètre d'entrée est celui de l'élément **ErrorFlowDocument** défini dans BCGErrorFlowSchema.xsd.
   - Si le style de liaison est **rpc**, alors le type de paramètre d'entrée sera **String** et il y aura un paramètre d'entrée unique.
2. Le routage du flux d'erreur ne fonctionnera pas dans le cas d'ID métier erronés. Si le document de flux d'erreur est requis pour un événement particulier et même si le document métier ayant des ID incorrects échoue avec le même événement configuré, alors le routage du document de flux d'erreur ne fonctionnera pas puisque les ID métier spécifiés ne sont pas valides.

Chapitre 16. Parachèvement de la configuration

Ce chapitre décrit les opérations supplémentaires que vous pouvez effectuer pour configurer le concentrateur. Il contient les rubriques suivantes :

Remarque : Pour modifier la configuration de WebSphere Partner Gateway, vous devez toujours utiliser l'instance de navigateur avec laquelle vous vous êtes connecté à la console de communauté. Si vous utilisez plusieurs instances de navigateur, vous risquez d'annuler vos modifications de la configuration.

Prise en charge de fichiers volumineux pour les documents AS

La prise en charge de fichiers volumineux avec un ordre de taille en Go a été étendue pour AS2 et AS3. La taille de fichier maximale traitée avec des tableaux d'octets est configurable. Lorsque le volume de mémoire allouée est supérieur à la taille de pile disponible, l'erreur OutOfMemoryError se produit. Si la taille des données est inférieure au volume de mémoire disponible, l'erreur OutOfMemoryError se produira si la mémoire allouée augmente le volume de mémoire disponible. Au moment de l'exécution, la possibilité de prendre en charge la taille de fichier configurée est déterminée en fonction de la pile disponible. Vous pouvez indiquer la taille de fichier maximale pouvant être utilisée avec des tableaux d'octets via la propriété **bcg.maximumFileSizeForByteArrays**. La valeur de cette propriété est exprimée en Mo. Si la taille de fichier est supérieure à cette valeur, elle est traitée en utilisant des flux. Si elle est inférieure, et que la mémoire disponible n'est pas suffisante, l'événement en erreur BCG210050 est généré.

Lorsque vous vous connectez en tant qu'opérateur de concentrateur, accédez à l'onglet **Administration système** > onglet **Propriétés communes**. Remplacez la valeur par défaut de la propriété **bcg.maximumFileSizeForByteArrays** par la taille de fichier maximale à utiliser avec les tableaux d'octets. Augmentez la valeur de cette propriété pour de meilleures performances.

Activation d'API

Pourquoi et quand exécuter cette tâche

WebSphere Partner Gateway intègre un ensemble d'API que vous pouvez utiliser pour accéder à certaines fonctions habituellement effectuées au niveau de la console de communauté. Ces API sont décrites dans le *Guide du programmeur de WebSphere Partner Gateway*.

Cette procédure vise à activer des API XML pour que les partenaires puissent les appeler via le serveur WebSphere Partner Gateway.

Procédure

1. Dans le menu principal, cliquez sur **Administration du système > Administration de la fonction > API de l'administration**.
2. Cliquez sur l'icône **Edition** en regard de **Activer l'API XML**.
3. Cochez la case pour permettre l'utilisation de l'API XML.
4. Cliquez sur **Sauvegarder**.

Résultats

Remarque : L'API d'administration basée sur XML est obsolète.

L'utilitaire de migration peut également être utilisé à la place de l'API d'administration pour créer et mettre à jour les tâches. Le fichier d'importation de migration comporte des informations nouvelles ou mises à jour.

Le fichier d'importation est décrit par le schéma XML qui est fourni avec l'utilitaire de migration. Vous pouvez utiliser un outil de développement tel que Rational Application Developer pour produire un fichier XML d'importation conforme au schéma. En important ce fichier avec l'utilitaire de migration, vous pouvez charger de nouvelles définitions de partenaire comprenant les contacts et les ID métier de vos partenaires. Vous pouvez également mettre à jour les définitions de partenaire existantes en les important avec l'utilitaire de migration. L'API d'administration vous permet de répertorier des artefacts de configuration d'un système. L'exportation complète du système via l'utilitaire de migration fournit les listes des fonctionnalités des partenaires, les connexions des partenaires et les récepteurs (cibles) dans le fichier XML exporté.

Le fichier de traitement par lots**bcgmigrate.bat/bcgmigrate.sh** est utilisé pour initier le processus de migration. Lors de l'exécution de la commande bcgmigrate, assurez-vous de disposer d'un droit d'accès aux fichiers d'**exécution** pour (bcgmigrate.bat/bcgmigrate.sh). Cela s'applique particulièrement à la plateforme UNIX.

Définition des files d'attente utilisées pour les événements

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer le concentrateur pour fournir des événements à une file d'attente externe configurée à l'aide de la configuration JMS.

La configuration JMS par défaut est établie lorsque vous installez le concentrateur. Certaines de ces valeurs sont visibles sur la page Propriétés de la publication de l'événement.

Si vous voulez une configuration JMS différente, indiquez les valeurs de configuration appropriées pour la publication des événements dans les files d'attente de messages internes de WebSphere Partner Gateway/WAS ou d'autres serveurs de messagerie. Modifiez également le nom de la file d'attente afin qu'il corresponde à celui de la file d'attente dans laquelle sont publiés les événements.

Pour indiquer où les événements doivent être livrés, procédez comme suit :

1. A partir du menu principal, cliquez sur **Administration système> Administration du gestionnaire de documents > Moteur des événements > Evénements externes**.

2. Cliquez sur l'icône **Edition** en regard de **Activer la livraison d'événement**.
3. Cochez la case /**Activer la livraison d'événement** pour activer la publication des événements.
4. Si les valeurs par défaut sont correctes pour votre installation, ne les modifiez pas. Elles prennent en charge la remise d'événements sur la file d'attente nommée DeliveryQ, fournie par le serveur JMS configuré lors de l'installation.

   Si vous souhaitez modifier l'endroit où sont placés les événements, mettez à jour les zones en utilisant les informations suivantes comme référence :

   - Entrez des valeurs dans les zones **ID utilisateur** et **Mot de passe**, si un ID utilisateur et un mot de passe sont requis pour accéder à la file d'attente.
   - Comme **Nom de fabrique de la file d'attente JMS**, entrez le nom de la fabrique de connexion de file d'attente JMS contenu dans le fichier JMS .bindings que vous utilisez.

     Remarque : Sur certaines versions de Windows (avant XP), vous pourrez avoir à modifier la valeur par défaut de la zone **Nom de fabrique de la file d'attente JMS** si vous voulez utiliser la fonction Sortie d'événement par défaut. Vous changerez la valeur de **Nom de fabrique de la file d'attente JMS** (`WBIC/QCF`) en `WBIC\\QCF`.
   - Comme **Type de message JMS**, indiquez le type de message qui sera livré. Les options possibles sont octet ou texte. Le composant Récepteur déterminant le mappage de type de message JMS, la valeur du type de message JMS est facultative.
   - Comme **Nom de file d'attente JMS**, indiquez le nom de la file d'attente JMS sur laquelle les événements seront publiés. Cette file d'attente doit être déjà définie dans le fichier JMS .bindings que vous utilisez dans WebSphere MQ.

     Remarque : Sur certaines versions de Windows (avant XP), vous pourrez avoir à modifier la valeur par défaut de la zone **Nom de la file d'attente JMS**, si vous voulez utiliser la fonction Sortie d'événement par défaut. Vous changerez la valeur de **Nom de la file d'attente JMS** (`WBIC/DeliveryQ`) en `WBIC\\DeliveryQ. WBIC/QCF`.
   - Comme **Nom de la fabrique JNDI**, indiquez le nom utilisé pour accéder au fichier .bindings. La valeur par défaut permet d'accéder à la liaison par défaut du système de fichiers.
   - Comme **Packages d'URL du fournisseur**, indiquez une URL permettant d'accéder au fichier de liaisons JMS. Cette URL doit être cohérente avec le nom de la fabrique JNDI. Cette zone est facultative et si elle n'est pas renseignée, l'emplacement du système de fichiers par défaut est utilisé pour les liaisons JMS.
   - Comme **Jeu de caractères du message**, indiquez le jeu de caractères à utiliser lors de la création du message de type octet sur la file d'attente JMS. La valeur par défaut est UTF-8. Cette zone ne s'applique qu'aux messages de type octet.
   - Comme **URL du fournisseur JMS**, indiquez l'URL du fournisseur JMS. Cette zone est facultative et si elle n'est pas renseignée, le fournisseur JMS par défaut, identifié lors de l'installation, est utilisé.
5. Cliquez sur **Sauvegarder**.

Définition des événements pouvant faire l'objet d'une alerte

Pourquoi et quand exécuter cette tâche

Lorsqu'un événement se produit dans WebSphere Partner Gateway, un code d'événement est généré. A l'aide de la page Codes événement, vous pouvez définir l'état d'alerte du code événement. Lorsqu'un événement est défini comme pouvant faire l'objet d'une alerte, l'événement apparaît dans la liste Nom de l'événement de la page d'alerte. Vous pouvez alors définir une alerte pour l'événement.

Pour indiquer les événements qui peuvent faire l'objet d'une alerte, procédez comme suit :

Procédure

1. Cliquez sur **Administrateur de concentrateur > Configuration du concentrateur > Codes d'événement**. La page Codes événement s'affiche.
2. Pour chaque événement que vous voulez définir comme pouvant faire l'objet d'une alerte :
   a. Cliquez sur l'icône **Afficher les détails** en regard du code d'événement. La page Détails du code événement s'affiche.
   b. Sélectionnez **Alerte possible**.
   c. Cliquez sur **Sauvegarder**.

Mise à jour d'un transport défini par l'utilisateur

Comme décrit dans Chapitre 7, «Définition des récepteurs», à la page 61 et Chapitre 11, «Création de destinations», à la page 229, vous pouvez télécharger un fichier XML décrivant un transport défini par l'utilisateur. Vous utiliserez pour cela **Gérer les types de transports**. Une fois le fichier XML envoyé, le transport peut être utilisé lors de la définition d'un récepteur ou d'une destination.

Le fichier XML qui décrit le transport défini par l'utilisateur inclut les attributs du transport. Ces attributs sont affichés (dans la section **Attributs de transport personnalisés**) sur la page du récepteur ou de la destination lorsque vous spécifiez un transport défini par l'utilisateur. Par exemple, un transport défini par l'utilisateur pour une destination peut inclure l'attribut DestinationRetryCount.

L'auteur du fichier XML décrivant le transport peut mettre à jour les attributs (en ajoutant, supprimant ou modifiant les attributs). Si le fichier XML est modifié, vous utiliserez de nouveau **Gérer les types de transports** pour envoyer le fichier. Toute modification apportée aux attributs apparaît dans la page de la destination ou du récepteur.

Exemples

WebSphere Partner Gateway comprend des packages avec quelques exemples qui fournissent des illustrations et décrivent des fonctionnalités personnalisées. Ces packages se trouvent dans le répertoire où l'installation de WebSphere Partner Gateway est extraite, sous les dossiers **DevelopmentKits** et **Integration**.

Le dossier DevelopmentKits contient les exemples suivants :

- API d'administration : puisque les API d'administration sont obsolètes, l'utilitaire Migration de partenaire est utilisé pour créer et mettre à jour des tâches.

- Migration : contient des exemples de configuration d'importation et d'exportation.
  - Configuration d'exportation : illustre la procédure permettant d'exporter les configurations WebSphere Partner Gateway à l'aide d'un composant java à partir du fichier script de ligne de commande.
  - Configuration d'importation : illustre la procédure permettant d'importer les configurations WebSphere Partner Gateway à l'aide d'un composant java à partir du fichier script de ligne de commande.
- Exits utilisateur : comprend des exemples permettant d'écrire du code d'exit utilisateur pour traduction et validation.
  - L'exemple *EDITransTypeBusinessProcess* présente des fonctionnalités personnalisées pour des documents EDI qui passent dans le système. Cet exemple d'exit utilisateur est conçu pour faire une analyse syntaxique du type de transaction EDI à partir d'un document EDI X12. En modifiant les critères d'analyse syntaxique, il est possible d'extraire d'autres valeurs.
  - L'exemple *exit utilisateur de traduction personnalisée* présente des fonctionnalités de traduction personnalisées pour un document XML entrant.
  - L'exemple *exit utilisateur de validation personnalisée* présente des fonctionnalités de validation personnalisées pour un document XML entrant.
- Exemples de scénarios : comprend des exemples qui présentent des instructions de configuration du système WebSphere Partner Gateway pour les protocoles mentionnés ci-dessous, avec Aucun empaquetage ainsi que Empaquetage AS. Pour chaque protocole, le fichier d'importation de configuration est également fourni.
  - XML personnalisé
  - EDI-X12
  - Documents binaires

Le dossier Intégration contient les exemples d'intégration suivants :

- Intégration WebSphere Transformation Extender : exemple démontrant l'intégration à WebSphere Transformation Extender pour la transformation d'un document XML en fichier à plat.
- Exemple WebSphere Business Integration Message Broker : exemple démontrant comment WebSphere Partner Gateway communique avec WebSphere Business Integration Message Broker.
- Intégration WebSphere Process Server : exemple démontrant comment WebSphere Partner Gateway s'intègre à WebSphere Process Server via JMS.
- Intégration WebSphere Interchange Server : exemple démontrant comment WebSphere Partner Gateway s'intègre à Interchange Server via HTTP et JMS.

Chapitre 17. Editeur CPP/CPA

L'éditeur CPP/CPA est un plug-in Eclipse permettant de créer des documents CPP/CPA à partir d'un modèle et d'éditer avec un format table. Il traite également les données et la validation de schéma.

Prérequis :

- Les versions WID/RAD 6.1 et ultérieures sont nécessaires
- Placez le plug-in éditeur CPP/A téléchargé dans le dossier des plug-ins d'IDE

Il est également possible de créer un document Collaboration-Protocol Agreement (CPA) à partir de deux documents Collaboration-Protocol Profile (CPP). CPP définit les fonctions d'une partie engagée avec d'autres partie dans des questions électroniques. CPA décrit l'accord d'échange de messages entre deux parties. Pour créer un CPP, entrez les valeurs d'éléments XML individuels (les éléments XML individuels se composent de divers attributs) via l'interface utilisateur de l'éditeur. Une fois le document CPA créé avec l'éditeur et qu'il a le statut "ACCEPTE", vous pouvez l'importer dans WebSphere Partner Gateway. Les fichiers importés créent automatiquement les éléments suivants :

- Partenaires
- Passerelles B2B
- Interactions et connexions

Ils définissent également automatiquement les définitions des documents et activent les fonctions B2B requises.

Vous pouvez effectuer les opérations suivantes via l'interface utilisateur de l'éditeur CPP/CPA :

- «Création d'un document CPP»
- «Création d'un document CPA», à la page 326
- «Edition des valeurs dans l'éditeur», à la page 327

Pour paramétrer l'éditeur CPP/CPA comme éditeur par défaut, procédez comme suit :

1. Dans l'environnement de plug-in Eclipse, cliquez sur le menu **Fenêtre** et sélectionnez **Préférences**
2. Dans la fenêtre des préférences, cliquez sur **Général > Editeur > Association de fichiers**.
3. Sélectionnez "*.xml" dans la liste **Types de fichiers** et "CPPEditor Multi – page Editeur" dans la liste **Editeurs associés**.
4. Cliquez sur **Valeur par défaut**.

Création d'un document CPP

Pour créer un document CPP, procédez comme suit :

1. Dans la zone IDE, sélectionnez **Fichier** >**Nouveau**.
2. Dans la fenêtre **Nouveau**, sélectionnez **CPAEditor** > **Fichier Collaboration Protocol Profile**
3. Cliquez sur **Suivant** et entrez les valeurs CPP/CPA.
4. Cliquez sur **Terminer**. Le nouveau fichier est créé sous le conteneur spécifié.

5. Si vous avez configuré CPAEditor comme éditeur par défaut, modifiez alors les valeurs dans le modèle, sinon le fichier s'ouvrira dans l'éditeur XML. Pour ouvrir le fichier dans CPAEditor, cliquez avec le bouton droit de la souris et sélectionnez **Ouvrir avec** > **Multi-Page Editeur**.
6. Entrez les valeurs des attributs de tous les éléments. Pour certains attributs, vous pouvez sélectionner la valeur appropriée à partir de différentes options.
7. Cliquez sur **Sauvegarder**. Un message s'affiche confirmant la création d'un document CPP.

Création d'un document CPA

Vous devez sélectionner l'une des deux options suivantes :

- Cas numéro 1 : Création d'un document CPA à partir d'un modèle. Cela permet d'entrer les valeurs d'éléments XML individuels (les éléments XML individuels se composent de divers attributs) via l'interface utilisateur de l'éditeur.
- Cas numéro 2 : Création d'un CPA à partir de deux CPP

Pour créer un CPA à partir d'un modèle, procédez comme suit :

1. Dans la zone IDE, sélectionnez **Fichier** >**Nouveau**.
2. Dans la fenêtre **Nouveau**, sélectionnez **CPAEditor** > **Fichier Collaboration Protocol Agreement**
3. Cliquez sur **Suivant** et entrez les valeurs CPP/CPA.
4. Cliquez sur **Terminer**. Le nouveau fichier est créé sous le conteneur spécifié.
5. Si vous avez configuré CPAEditor comme éditeur par défaut, modifiez alors les valeurs dans le modèle, sinon le fichier s'ouvrira dans l'éditeur XML. Pour ouvrir le fichier dans CPAEditor, cliquez avec le bouton droit de la souris et sélectionnez **Ouvrir avec** > **CPPEditor Multi-Page Editeur**.
6. Entrez les valeurs des attributs de tous les éléments. Pour certains attributs, vous pouvez sélectionner la valeur appropriée à partir de différentes options.
7. Cliquez sur **Sauvegarder**. Un message s'affiche confirmant la création d'un document CPA.

Pour créer un CPA à partir de deux CPP, procédez comme suit :

1. Dans la zone IDE, sélectionnez **Fichier**> **Nouveau** > **Autre**.
2. Dans la fenêtre **Nouveau**, sélectionnez **CPAEditor** > **Fusionner les Collaboration Protocol Profiles**.
3. Cliquez sur **Suivant**
4. Entrez les valeurs CPP/CPA ainsi que le chemin et le nom des fichiers CPP que vous voulez fusionner.
5. Cliquez sur **Terminer**. Les fichiers fusionnés sont créés dans le conteneur qui a été spécifié.
6. Si vous avez configuré CPAEditor comme éditeur par défaut, modifiez alors les valeurs dans le modèle, sinon le fichier s'ouvrira dans l'éditeur XML. Pour ouvrir le fichier dans CPAEditor, cliquez avec le bouton droit de la souris et sélectionnez **Ouvrir avec** > **CPPEditor Multi-Page Editeur**.

Edition des valeurs dans l'éditeur

Pour éditer les valeurs dans le tableau d'éditeur, placez le curseur sur la cellule et modifiez les valeurs. Chaque élément PartyInfo a un nom partyName qui lui est associé. Les différents sous-éléments qui se produisent sous PartyInfo sont PartyId, PartyRef, Collaboration Role, Certificate, SecurityDetails, DeliveryChannel, Transport, DocExchange, et OverrideMshActionBinding. Ces valeurs sont accessibles dans différents onglets de l'éditeur CPP/CPA. PartyName sert d'identificateur unique pour associer les sous-éléments de l'élément PartyInfo à l'élément PartyInfo correspondant.

Par exemple, l'élément Certificate qui est un sous-élément de l'élément PartyInfo peut se produire une ou plusieurs fois. L'élément PartyInfo peut lui-même se produire à plusieurs reprises dans un CPP.

Chapitre 18. Boîte aux lettres Web

Les nouvelles fonctions fournies dans l'édition de la boîte aux lettres Web complètent la prise en charge antérieure de WebSphere Partner Gateway. Cela permet aux partenaires, clients et fournisseurs d'interagir avec le concentrateur en utilisant uniquement les navigateurs pris en charge, c'est-à-dire la prise en charge Web de l'interaction business-to-business. La version Web de la console WebSphere Partner Gateway s'ouvre dans un navigateur et il n'y pas besoin d'infrastructure externe, telle qu'un serveur FTP, une fonction de message, etc. Les tâches supplémentaires suivantes peuvent être exécutées dans cette version de WebSphere Partner Gateway :

- Télécharger des documents pour des transactions
- Surveiller l'état des documents commerciaux
- Télécharger le document commercial reçu

Cette fonction est essentiellement destinée aux partenaires externes qui ne disposent pas d'une infrastructure leur permettant de participer aux transactions. Ce chapitre décrit les étapes préalable requises pour pouvoir utiliser les fonctions de la boîte aux lettres Web.

Remarque : Cette édition prend en charge les documents uniquement dans le package "None".

Prérequis

Pour qu'un partenaire externe utilise les fonctions de boîte aux lettres Web, l'administrateur de concentrateur doit fournir les droits suivants :

- «Activation de la boîte aux lettres Web au niveau du concentrateur»
- «Activation de la boîte aux lettres Web au niveau du partenaire»
- «Activation de WebBoxReceiver», à la page 330

Activation de la boîte aux lettres Web au niveau du concentrateur

Pourquoi et quand exécuter cette tâche

Pour activer les droits pour la boîte de réception et la boîte d'envoi :

1. Accédez à la page **Administrateur du concentrateur** > **Configuration de la console** > **Droits**.
2. Dans la page de la liste **Droits**, activez la boîte de réception et la boîte d'envoi.

Remarque : C'est une activité ponctuelle pour l'administrateur de concentrateur.

Activation de la boîte aux lettres Web au niveau du partenaire

Pourquoi et quand exécuter cette tâche

Etapes à exécuter pour un nouveau partenaire externe :

1. Connectez-vous à la console en tant qu'administrateur de concentrateur.

Remarque : Lorsque vous créez un nouveau partenaire externe, un groupe Webuser par défaut est créé automatiquement. De même, lorsque ce module de correction est installé, le groupe Webuser par défaut est créé pour les partenaires existants.

2. Dans la page **Groupes**, cliquez sur l'icône Afficher les autorisations pour le groupe nouvellement créé.
3. Sélectionnez **Lire / écrire** pour la boîte de réception et la boîte d'envoi.
4. Créez un nouvel utilisateur.
5. Dans la page **Appartenances**, attribuez l'utilisateur au groupe.

Remarque : C'est une activité ponctuelle pour l'administrateur de concentrateur.

Activation de WebBoxReceiver

Pourquoi et quand exécuter cette tâche

Après installation de la fonction de boîte aux lettres Web, l'administrateur de concentrateur doit activer le récepteur avant d'envoyer des documents au partenaire interne. L'état par défaut de WebBoxReceiver est désactivé.

Remarque : WebBoxReceiver est créé par le système et ne peut pas être supprimé. Les étapes pour activer WebBoxReceiver sont les suivantes :

1. Accédez à **Administrateur du concentrateur** > **Récepteurs**.
2. Activez WebBoxReceiver.

Remarque : Pour modifier l'intervalle d'interrogation de WebBoxReceiver, modifiez son attribut d'intervalle d'interrogation en conséquence.

Limitations de la boîte aux lettres Web

Les limitations de boîte aux lettres Web sont les suivantes :

- Possibilité d'envoyer un maximum de 10 Mo aux partenaires internes.

  Remarque : Cela peut être plus ou moins en fonction du réseau, du navigateur ou de la mémoire.
- Impossible de supprimer le récepteur de la boîte Web.
- Impossible d'envoyer les documents EDI/XML en format binaire.

Chapitre 19. Exemples de base

La présente annexe propose des exemples de configuration du concentrateur. Il contient les rubriques suivantes :

- « Configuration de base – Echange de documents EDI avec passe-système»
- « Configuration de base - Configuration de sécurité pour les documents entrants et sortants», à la page 337
- «Extension de la configuration de base», à la page 343

Une autre annexe contient des exemples d'EDI qui ont recours au désenveloppement, à la transformation, à l'enveloppement et à la transmission fonctionnelle d'accusé de réception. Voir Chapitre 20, «Exemples d'EDI», à la page 351.

Le but de ces exemples est de vous présenter rapidement les étapes nécessaires pour configurer un système. Si vous utilisez ces exemples pour configurer votre système, veillez à modifier les données pour correspondre à vos besoins (par exemple les noms et ID entreprise).

Configuration de base – Echange de documents EDI avec passe-système

Dans cet exemple, la configuration du concentrateur est relativement simple — deux récepteurs sont définis (un pour les documents entrant dans le concentrateur émis par un partenaire et un autre pour les documents entrant dans le concentrateur émis par le système dorsal du partenaire interne). Les échanges définis dans cet exemple utilisent les définitions de documents fournies par WebSphere Partner Gateway. Vous avez donc uniquement à créer des interactions basées sur ces flux. Cet exemple ne fait appel à aucun format XML.

Cet exemple illustre un échange entre une application dorsale du partenaire interne et un partenaire externe (Partenaire B).

Configuration du concentrateur

La première étape de configuration du concentrateur consiste à créer les deux récepteurs.

- Un récepteur HTTP (appelé “RécepteurHttp”) pour recevoir des documents via HTTP (du partenaire B) qui doivent être envoyés au système dorsal du partenaire interne.
- Un récepteur de répertoire de fichiers (appelé “RécepteurSystèmeFichiers”) pour extraire des documents du système de fichiers (à partir du système dorsal du partenaire interne) qui doivent être envoyés au partenaire B.

Définition des récepteurs

Pourquoi et quand exécuter cette tâche

Pour créer un récepteur pour la réception de documents sur HTTP :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Cliquez sur **Créer le récepteur**.

3. Dans la zone Nom du récepteur, entrez **RécepteurHttp**.
4. Dans la liste Transport, sélectionnez **HTTP/S**.
5. En ce qui concerne le mode Opération, optez pour la valeur par défaut, à savoir, **Production**.
6. Dans la zone Identificateur URI, tapez **/bcgreceiver/submit**
7. Cliquez sur **Sauvegarder**.

L'étape suivante consiste à créer un récepteur afin d'interroger un répertoire dans le système de fichiers. La création du récepteur entraîne celle, automatique, d'un nouveau répertoire dans le système de fichiers.

Pour créer le récepteur dans le système de fichiers, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Cliquez sur **Créer le récepteur**.
3. Dans la zone Nom du récepteur, entrez **RécepteurSystèmeFichiers**.
4. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
5. En ce qui concerne le mode Opération, optez pour la valeur par défaut, à savoir, **Production**.
6. Pour le chemin principal du document entrez : **\temp\FileSystemReceiver**

   Remarque : Le répertoire RécepteurSystèmeFichiers est alors créé dans le répertoire temp. Assurez-vous qu'il existe un répertoire temp dans le système de fichiers.
7. Cliquez sur **Sauvegarder**.

Définition des types de documents et des interactions

Pourquoi et quand exécuter cette tâche

Dans cet exemple, vous paramétrez l'échange de documents conformes au standard EDI-X12. Ici, les documents ne font que passer par le concentrateur. L'EDI n'est pas désenveloppé et aucune transformation n'a lieu. Consultez l'Chapitre 23, «Attributs», à la page 445 pour découvrir des exemples de désenveloppement d'EDI, de transformation des transactions et d'envoi d'accusés de réception.

Dans cette section, les échanges suivants sont décrits :

- Envoi d'un document EDI-X12, sans empaquetage, du partenaire interne vers le Partenaire B
- Envoi d'un document EDI-X12, empaqueté dans AS2, du partenaire B vers le partenaire interne

Du fait de l'empaquetage et des protocoles mis en oeuvre, il n'est pas utile de créer une nouvelle définition de documents. Les packages, protocoles et types de documents sont ceux prédéfinis dans le système.

Toutefois, vous devez définir des interactions basées sur ces types de documents prédéfinis.

Créez la première interaction, dont la source est un document au format ISA conforme au standard EDI-X12 sans empaquetage et la cible un document ISA conforme au standard EDI-X12 avec empaquetage AS.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.

2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Dans la colonne **Source**, développez :
   a. **Package : None**
   b. **Protocole : EDI-X12**
4. Cliquez sur **Type de documents : ISA**
5. Dans la colonne **Cible**, développez:
   a. **Package : AS**
   b. **Protocole : EDI-X12**
6. Cliquez sur **Type de documents : ISA**
7. Dans la liste des **actions**, sélectionnez **Passe-système**.
8. Cliquez sur **Sauvegarder**.

Créez une seconde interaction, dont la source est un document au format ISA conforme au standard EDI-X12 avec empaquetage AS et la cible un document ISA conforme au standard EDI-X12 sans empaquetage :

1. Cliquez sur le **lien Créer une interaction**.
2. Dans la colonne **Source**, développez :
   a. **Package :AS**
   b. **Protocole : EDI-X12**
3. Cliquez sur **Type de documents : ISA**
4. Dans la colonne **Cible**, développez:
   a. **Package : None**
   b. **Protocole : EDI-X12**
5. Cliquez sur **Type de documents :ISA**
6. Dans la liste des **actions**, sélectionnez **Passe-système**.
7. Cliquez sur **Sauvegarder**.

Création de partenaires et de connexions de partenaire

Dans cet exemple, un partenaire externe est créé, en plus du partenaire interne. Les destinations des partenaires comprennent des transports standard. En outre, aucun point de configuration n'est défini pour les destinations.

Création des partenaires

Créez deux nouveaux partenaires. Pour définir le partenaire interne, procédez comme suit :

1. Cliquez sur **Administrateur du compte** dans le menu principal. La page Recherche du partenaire est la vue par défaut.
2. Cliquez sur **Créer**.
3. Dans la zone **Nom de connexion de l'entreprise**, tapez : **GestCom**.
4. Dans la zone **Nom affiché du partenaire**, entrez : **Gest Com**.
5. Pour le **Type de partenaire**, sélectionnez **Partenaire interne**.
6. Sous **ID Métier**, cliquez sur **Nouveau**.
7. Laissez le paramètre **Type** associé à la valeur **DUNS**, puis entrez l'identificateur **123456789**.

   Remarque : Ici comme partout ailleurs dans ce document, les numéros DUNS ne sont que des exemples.

8. Sous **ID Métier**, cliquez sur **Nouveau**.
9. Sélectionnez **A format libre** et entrez l'identificateur **12-3456789**.
10. Cliquez sur **Sauvegarder**.

Pour définir le Partenaire B, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Créer**.
3. Dans la zone **Nom de connexion de l'entreprise**, tapez **partenaireB**
4. Dans la zone **Nom affiché du partenaire**, tapez : **Partenaire B**
5. Pour le **Type de partenaire**, sélectionnez **Partenaire externe**.
6. Sous **ID Métier**, cliquez sur **Nouveau**.
7. Laissez le paramètre **Type** associé à la valeur **DUNS**, puis entrez l'identificateur **987654321**.
8. Sous **ID Métier**, cliquez sur **Nouveau**.
9. Sélectionnez **A format libre** et entrez l'identificateur **98-7654321**.
10. Cliquez sur **Sauvegarder**.

Vous venez de définir le partenaire interne et le partenaire B pour le concentrateur.

Les étapes suivantes consistent à configurer les destinations pour le partenaire interne et le partenaire B.

Création des destinations

Pourquoi et quand exécuter cette tâche

Avant de créer une destination pour le répertoire de fichiers du partenaire interne, vous devez créer la structure de répertoire utilisée par cette destination. Créez un nouveau répertoire DestinationSystèmeFichiers sur l'unité principale. Ce répertoire sera utilisé par le partenaire interne pour stocker les fichiers reçus des partenaires externes.

Pour le partenaire interne, la destination représente le point d'entrée dans le système dorsal.

Pour créer une destination pour le partenaire interne, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez **Partenaire interne** en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Destinations** dans la barre de navigation horizontale.
5. Cliquez sur **Créer**.
6. Dans la zone **Nom de destination**, saisissez : **DestinationSystèmeFichiers**.
7. Pour **Transport**, sélectionnez **Répertoire de fichiers**.
8. Dans la zone **Adresse**, entrez **file://C:\PasserelleSystèmeFichiers**.
9. Cliquez sur **Sauvegarder**.

Ensuite, définissez cette destination nouvellement créée comme destination par défaut du partenaire interne.

1. Cliquez sur **Liste** pour afficher la liste de toutes les destinations configurées pour le partenaire interne.
2. Cliquez sur **Afficher les destinations par défaut**.

3. Dans la liste **Production**, sélectionnez **DestinationSystèmeFichiers**.
4. Cliquez sur **Sauvegarder**.

Créez une destination pour le Partenaire B :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**, puis sélectionnez **Partenaire B** en cliquant sur l'icône **Afficher les détails**.
3. Cliquez sur **Destinations** dans la barre de navigation horizontale.
4. Cliquez sur **Créer**.
5. Dans la zone **Nom de destination**, saisissez : **DestinationHttp**.
6. Pour **Transport**, sélectionnez **HTTP/1.1**.
7. Dans la zone **Adresse**, tapez **http://<***adresse_IP***>:80/input/AS2**, où <*adresse_IP*> est celle de l'ordinateur du Partenaire B.
8. Dans la zone **Nom d'utilisateur**, tapez : **Gest Com**.
9. Dans la zone **Mot de passe**, tapez : **Gestcom**.
10. Cliquez sur **Sauvegarder**.

Dans cet exemple, on suppose que le Partenaire B demande un nom d'utilisateur et un mot de passe à tout partenaire se connectant à son système.

Vous devez à nouveau définir une destination par défaut pour ce partenaire.

1. Cliquez sur **Liste** puis sur **Afficher les destinations par défaut**.
2. Dans la liste **Production**, sélectionnez **DestinationHttp**.
3. Cliquez sur **Sauvegarder**.

Définition des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

L'étape suivante consiste à définir les fonctions business-to-business du partenaire interne.

1. Dans le menu principal, cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez **Partenaire interne** en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Fonctions B2B** dans la barre de navigation horizontale.
5. Définissez la source et la cible pour Package : None, Protocole : EDI-X12 et Type de documents : ISA en suivant les étapes suivantes :
   a. Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : None**.
   b. Cliquez sur l'icône **Rôle inactif** sous **Définir la cible** pour **Package : None**.
   c. Cliquez sur l'icône **Développer** en regard de **Package : None**.
   d. Cliquez sur l'icône **Le rôle est inactif** pour **Protocole : EDI-X12 (ALL)** pour la source et la cible.
   e. Cliquez sur l'icône **Développer** en regard de **Protocole : EDI-X12 (TOUT)**.
   f. Cliquez sur l'icône **Rôle inactif** de **Type de documents : ISA** pour la source et la cible.

Ensuite, définissez les fonctions business-to-business du Partenaire B.

Procédure

1. Dans le menu principal, cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez le Partenaire B en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Fonctions B2B** dans la barre de navigation horizontale.
5. Sélectionnez Définition de la source et Définition de la cible pour Package : AS, Protocole : EDI-X12 et Type de documents : ISA en effectuant les opérations suivantes :
   a. Cliquez sur l'icône **Rôle inactif** sous **Définir la source** pour **Package : AS**.
   b. Cliquez sur l'icône **Rôle inactif** sous **Définir la cible** pour **Package : AS**.
   c. Cliquez sur l'icône **Développer** en regard de **Package : AS**.
   d. Cliquez sur l'icône **Le rôle est inactif** pour **Protocole : EDI-X12 (ALL)** pour la source et la cible.
   e. Cliquez sur l'icône **Développer** en regard de **Protocole : EDI-X12 (TOUT)**.
   f. Cliquez sur l'icône **Rôle inactif** de **Type de documents : ISA** pour la source et la cible.

Définition des connexions des partenaires

Pourquoi et quand exécuter cette tâche

Définissez la connexion des partenaires pour les documents EDI sans empaquetage qui sont envoyés du partenaire interne au partenaire B.

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Dans la liste **Source**, sélectionnez **Partenaire interne**.
3. Dans la liste **Cible**, sélectionnez **Partenaire B**.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion comportant les détails suivants :
   a. **Source**
      1) Package : **None (N/A)**
      2) Protocole : **EDI-X12 (ALL)**
      3) Type de documents : **ISA (TOUT)**
   b. **Cible**
      1) Package : **AS (N/A)**
      2) Protocole : **EDI-X12 (ALL)**
      3) Type de documents : **ISA (TOUT)**

Ensuite, définissez la connexion pour les documents EDI encapsulés dans le package AS2 et qui sont envoyés sans empaquetage au partenaire interne par le partenaire B. Cette connexion est très similaire à celle que vous avez définie dans la section précédente, sauf que vous configurez également les attributs AS2.

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Dans la liste **Source**, sélectionnez **Partenaire B**.
3. Dans la liste **Cible**, sélectionnez **Partenaire interne**.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion comportant les détails suivants :
   a. **Source**
      1) Package : **AS (N/A)**

2) Protocole : **EDI-X12 (ALL)**
3) Type de documents : **ISA (TOUT)**

b. **Cible**
1) Package : **None (N/A)**
2) Protocole : **EDI-X12 (ALL)**
3) Type de documents : **ISA (TOUT)**

Ensuite, sélectionnez Attributs en regard de la zone **Package : AS (N\A)** pour le Partenaire B.

1. Modifiez les attributs d'empaquetage : AS (N\A) en faisant défiler la page et en cliquant sur l'icône **Développer** en regard de **Package : AS (N/A)**.
2. Entrez une valeur AS MDN E-Mail Address (AS1). Il peut s'agir de n'importe quelle adresse électronique correcte.
3. Entrez une valeur AS MDN HTTP URL (AS2). Vous devez la saisir de la façon suivante : **http://<***Adresse_IP***>:57080/bcgreceiver/submit,** où <*Adresse_IP*> représente le concentrateur.
4. Cliquez sur **Sauvegarder**.

Configuration de base - Configuration de sécurité pour les documents entrants et sortants

Dans cette section, vous allez découvrir comment ajouter les dispositifs de sécurité suivants à la configuration de base :

- Authentification serveur SSL (Secure Socket Layers)
- Chiffrement
- Signatures numériques

Configuration de l'authentification SSL pour les documents entrants

Pourquoi et quand exécuter cette tâche

Dans cette section, l'authentification serveur est configurée à l'aide de l'outil iKeyman pour permettre au Partenaire B d'envoyer des documents AS2 via HTTPS.

Pour configurer l'authentification serveur, procédez comme suit :

1. Lancez l'application iKeyman en ouvrant le fichier ikeyman.bat à partir du répertoire <*ProductDir*>/was/bin.
2. Ouvrez le magasin de clés par défaut du récepteur, bcgSecurity.jks. Dans la barre de menus, sélectionnez **Key Database File Open**. Dans le cas d'une installation par défaut, bcgSecurity.jks se trouve dans le répertoire : <*ProductDir* >/common/security/keystore
3. Lorsque vous y êtes invité, entrez le mot de passe par défaut associé à bcgSecurity.jks. Ce mot de passe est WebAS.
4. Si vous ouvrez le fichier bcgSecurity.jks pour la première fois, supprimez le certificat “Fictif”.

L'étape suivante consiste à créer un nouveau certificat d'auto-signature. En créant un certificat d'auto-signature personnel, vous créez également une clé privée et une clé publique dans le fichier "magasin de clés" du serveur.

Pour créer un nouveau certificat d'auto-signature, procédez comme suit :

1. Cliquez sur **New Self Signed**.
2. Attribuez un intitulé de clé au certificat afin de l'identifier de façon unique dans le magasin de clés. Utilisez l'intitulé **CertAutoSign**.
3. Indiquez le nom CN du serveur. Il s'agit de l'identité principale et universelle du certificat. Il doit identifier de façon unique le principal qu'il représente.
4. Indiquez le nom de votre organisation.
5. Acceptez toutes les autres valeurs par défaut, puis cliquez sur **OK**.

Supposons que le Partenaire B souhaite envoyer un message EDI via AS2 et le protocole HTTP sécurisé. Pour ce faire, le Partenaire B devra faire référence au certificat public (qui a été créé en même temps que le certificat auto-signé à l'étape précédente).

Pour permettre au Partenaire B d'utiliser le certificat public, exportez ce certificat à partir du fichier de magasin de clés du serveur, comme suit :

1. Sélectionnez le certificat auto-signé nouvellement créé dans l'utilitaire de gestion des clés d'IBM.
2. Cliquez sur **Extraction d'un certificat**.
3. Sélectionnez le type de données **Données DER binaires**.
4. Indiquez le nom de fichier **GestComPublic**, puis cliquez sur **OK**.

Enfin, vous devez exporter le certificat auto-signé et la paire de clés privées sous la forme d'un fichier PKCS12 à l'aide d'iKeyman. Ce fichier PCKS12 sera utilisé pour le chiffrement, qui est décrit dans la section suivante.

Pour exporter le certificat d'auto-signature et la paire de clés privées, procédez comme suit.

1. Cliquez sur **Exporter/Importer**.
2. Sélectionnez le type de fichier de clé **PKCS12**.
3. Indiquez le nom de fichier **GestComPrivé**, puis cliquez sur **OK**.
4. Entrez un mot de passe pour protéger le fichier PKCS12 cible. Confirmez le mot de passe, puis cliquez sur **OK**.

Remarque : Arrêtez puis redémarrez le récepteur pour que ces modifications prennent effet.

Le mot de passe que vous avez indiqué vous servira par la suite lorsque vous importerez ce certificat privé dans le concentrateur.

Le Partenaire B doit également effectuer certaines étapes de configuration, à savoir, importer le certificat et modifier l'adresse de destination des documents AS2 qu'il envoie. Par exemple, le Partenaire B devrait modifier l'adresse comme suit :

`https://<Adresse_IP>:57443/bcgreceiver/submit`

où <*Adresse_IP*> fait référence au concentrateur.

Désormais, le certificat d'auto-signature qui a été placé dans le magasin de clés par défaut du récepteur sera présenté au Partenaire B chaque fois que celui-ci enverra un document par le biais du protocole HTTP sécurisé.

Pour définir la situation inverse, le Partenaire B doit fournir au concentrateur une clé SSL sous la forme d'un fichier .der (dans ce cas, partenaireBSSL.der). Si

nécessaire, le Partenaire B doit également modifier la configuration pour permettre la réception de documents via le mode de transport HTTPS.

Chargez partenaireBSSL.der, le fichier du partenaire B, dans le profil de l'Opérateur de concentrateur, en tant que certificat racine. Un certificat racine est un certificat émis par une autorité de certification et qui est utilisé lors de l'établissement d'une hiérarchie de certificats. Dans cet exemple, le Partenaire B a généré le certificat, qui est chargé en tant que certificat racine pour permettre au concentrateur de reconnaître et habiliter l'expéditeur.

Pour charger le fichier partenaireBSSL.der dans le concentrateur, procédez comme suit :

1. Dans le menu principal, cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez **Opérateur du concentrateur** en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Certificats**, puis sur **Charger le certificat**.
5. Réglez le paramètre **Type de certificat** sur **Certificat racine et intermédiaire**.
6. Modifiez la description en indiquant **Certificat SSL du Partenaire B**.
7. Attribuez au paramètre **Etat** la valeur **Activé**.
8. Cliquez sur **Parcourir** et naviguez jusqu'au répertoire dans lequel vous avez sauvegardé partnerTwoSSL.der.
9. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
10. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

Modifiez la destination du Partenaire B de sorte qu'elle utilise le protocole HTTP sécurisé.

1. Cliquez sur **Administrateur du compte > Profils > Partenaire** dans la barre de navigation horizontale.
2. Cliquez sur **Rechercher** et sélectionnez Partenaire B en cliquant sur l'icône **Afficher les détails**.
3. Cliquez sur **Destinations** dans la barre de navigation horizontale. Ensuite, sélectionnez DestinationHttp en cliquant sur l'icône **Afficher les détails**.
4. Modifiez-le en cliquant sur l'icône **Edition**.
5. Sélectionnez la valeur de transport **HTTPS/1.1**
6. Modifiez la valeur de l'adresse comme suit : **https://<***adresse_IP***>:443/input/AS2**, où<*adresse_IP*> fait référence à la machine du Partenaire B.
7. Toutes les autres valeurs peuvent rester en l'état. Cliquez sur **Sauvegarder**.

Configuration du chiffrement

Pourquoi et quand exécuter cette tâche

Cette section présente les étapes de configuration du chiffrement.

Le Partenaire B doit effectuer les étapes de configuration nécessaires (par exemple, importer le certificat public et le certificat auto-signé) et configurer le chiffrement des documents envoyés au concentrateur.

WebSphere Partner Gateway utilise sa clé privée pour déchiffrer les documents. Pour permettre au concentrateur d'effectuer cette opération, vous devez d'abord

charger la clé privée extraite du certificat d'auto-signature dans la console de communauté. Pour ce faire, vous devez être connecté à la console de communauté en tant qu'Opérateur de concentrateur et installer le certificat dans votre propre profil.

Pour charger le fichier PKCS12, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire** dans la barre de navigation horizontale.
2. Cliquez sur **Rechercher**.
3. Sélectionnez **Opérateur du concentrateur** en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Certificats**, puis sur **Charger PKCS12**.
5. Cochez la case à gauche de **Chiffrement**.
6. Modifiez la description en indiquant **CommManPrivate**.
7. Sélectionnez **Activé**.
8. Cliquez sur **Parcourir** et accédez au répertoire dans lequel le fichier PKCS12, commManPrivate.p12, est stocké.
9. Sélectionnez le fichier, puis cliquez sur **Ouvrir**.
10. Entrez le mot de passe fourni pour le fichier PKCS12.
11. Laissez le paramètre mode Opération associé à la valeur **Production**.
12. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

La procédure de configuration requise pour permettre à un partenaire d'envoyer des transactions chiffrées via HTTP sécurisé vers le concentrateur est à présent terminée.

La section suivante décrit la procédure inverse—le concentrateur envoie une transaction EDI chiffrée à l'aide du protocole HTTP sécurisé.

Le Partenaire B doit générer une paire de clés de chiffrement de document (dans cet exemple, partnerTwoDecrypt.der) et mettre le certificat de clé publique à la disposition du concentrateur.

Comme indiqué précédemment, la clé publique sera utilisée par le concentrateur pour chiffrer les transactions qui doivent être envoyées au partenaire. Pour cela, vous devez charger le certificat public dans le concentrateur.

Procédure

1. Dans le menu principal, cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez le Partenaire B en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Certificats** dans la barre de navigation horizontale.
5. Cliquez sur **Charger le certificat**.
6. Cochez la case en regard de **Chiffrement**.
7. Modifiez la description en indiquant **Déchiffrement Partenaire B**.
8. Attribuez à l'état la valeur **Activé**.
9. Cliquez sur **Parcourir**.
10. Naviguez jusqu'au répertoire dans lequel le certificat de déchiffrement, partnerTwoDecrypt.der, est stocké.

11. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
12. Laissez le mode Opération en tant que **Production**.
13. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

Résultats

La dernière étape de la procédure de configuration du concentrateur pour permettre l'envoi de messages chiffrés à l'aide du protocole HTTP sécurisé et d'AS2 consiste à modifier la connexion qui existe entre le partenaire interne et le Partenaire B.

Pour modifier cette connexion dans la console de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Connexions** dans la barre de navigation horizontale.
2. Dans la liste **Source**, sélectionnez **Gest Com**.
3. Dans la liste **Cible**, sélectionnez **Partenaire B**.
4. Cliquez sur **Rechercher**.
5. Cliquez sur le bouton **Attributs** correspondant à la cible.
6. Dans le récapitulatif de la connexion, vous remarquerez que la valeur actuelle de l'attribut **AS chiffré** est **Non**. Modifiez cette valeur en cliquant sur l'icône **Développer** en regard de **Package : AS (N/A)**.

   Remarque : Pour faire apparaître cette option, vous devez faire défiler la page.
7. Dans la liste, modifiez l'attribut **AS chiffré** en lui donnant la valeur **Oui**, puis cliquez sur **Sauvegarder**.

Configuration de la signature de documents

Pourquoi et quand exécuter cette tâche

Pour créer la signature et signer numériquement une transaction ou un message, WebSphere Partner Gateway utilise votre clé privée. Votre partenaire utilise ensuite votre clé publique pour valider la signature lors de la réception de ce message. C'est dans ce but que WebSphere Partner Gateway utilise les signatures numériques.

Cette section présente les étapes nécessaires pour configurer le concentrateur et un partenaire, afin d'utiliser des signatures numériques.

Le Partenaire B doit effectuer toutes les étapes de configuration requises (par exemple, créer un document d'auto-signature appelé partnerTwoSigning.der, dans cet exemple et configurer la signature des documents). Le Partenaire B doit mettre le fichier partnerTwoSigning.der à la disposition du concentrateur.

Pour charger le certificat numérique dans le concentrateur, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Partenaire** dans la barre de navigation horizontale.
2. Cliquez sur **Rechercher**.
3. Sélectionnez le Partenaire B en cliquant sur l'icône **Afficher les détails**.
4. Choisissez **Certificats** dans la barre de navigation horizontale.
5. Cliquez sur **Charger le certificat**.
6. Activez la case à cocher située en regard de **Signature numérique**.

7. Modifiez la Description en indiquant **Signature Gest Com**.
8. Attribuez au paramètre **Etat** la valeur **Activé**.
9. Cliquez sur **Parcourir**.
10. Naviguez jusqu'au répertoire dans lequel le certificat numérique, partnerTwoSigning.der, est enregistré, sélectionnez-le et cliquez sur **Ouvrir**.
11. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

La configuration initiale des signatures numériques est à présent terminée.

Le partenaire utilise le certificat public pour authentifier les transactions signées envoyées au concentrateur.

Le concentrateur quant à lui utilisera la clé privée pour signer numériquement les transactions sortantes envoyées au partenaire. Vous devez tout d'abord activer la clé privée pour la signature numérique.

Pour activer la clé privée pour la signature numérique, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Certificats** dans la barre de navigation horizontale.
2. Cliquez sur l'icône **Afficher les détails** en regard de **Opérateur du concentrateur**.
3. Cliquez sur l'icône **Afficher les détails** en regard de **GestComPrivé**.

   Remarque : Il s'agit du certificat privé qui a été chargé dans le concentrateur précédemment.
4. Cliquez sur l'icône **Edition**.
5. Activez la case à cocher située en regard de **Signature numérique**.

   Remarque : S'il existe plusieurs certificats de chiffrement, indiquez le primaire et le secondaire en sélectionnant **Primaire** ou **Secondaire** dans la liste **Utilisation du certificat**.
6. Cliquez sur **Sauvegarder**.

L'étape suivante consiste à modifier les attributs de la connexion qui existe entre le partenaire interne et le partenaire B, pour permettre l'envoi d'une transaction AS2 signée.

Pour modifier les attributs de la connexion du partenaire, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Connexions** dans la barre de navigation horizontale.
2. Sélectionnez **Partenaire interne** dans la liste **Source**.
3. Sélectionnez **Partenaire B** dans la liste **Cible**.
4. Cliquez sur **Rechercher**.
5. Cliquez sur le bouton **Attributs** correspondant au Partenaire B.
6. Modifiez l'attribut **AS signé** en cliquant sur l'icône **Développer** en regard de **Package : AS (N/A)**.
7. Sélectionnez **Oui** dans la liste **AS signé**.
8. Cliquez sur **Sauvegarder**.

L'étape de configuration destinée à permettre l'envoi d'une transaction AS2 signée de WebSphere Partner Gateway vers le partenaire est maintenant terminée.

Extension de la configuration de base

Cette section indique comment modifier la configuration de base décrite dans cette annexe. Cette section utilise les mêmes partenaires et la configuration décrite précédemment (un partenaire interne, avec un ID DUNS de 123456789 et une destination du répertoire de fichiers, ainsi qu'une partenaire appelé PartenaireB avec un ID DUNS de 987654321 et une destination HTTP), et décrit la procédure à suivre pour ajouter la prise en charge de :

- mode de transport FTP ;
- documents XML personnalisés ;
- fichiers binaires (sans empaquetage)

Création d'un récepteur FTP

Pourquoi et quand exécuter cette tâche

Le récepteur FTP reçoit les fichiers et les transmet au gestionnaire de documents en vue d'être traités. Comme indiqué dans «Configuration du serveur FTP pour la réception de documents», à la page 35, avant de créer un récepteur FTP, vous devez disposer d'un serveur FTP configuré ainsi que d'un répertoire FTP.

Dans cet exemple, on suppose que le serveur FTP a été configuré pour le Partenaire B et que le répertoire racine est c:/ftproot.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs**.
2. Cliquez sur **Créer le récepteur**.
3. Entrez les informations suivantes :
   a. Nom du récepteur : **Récepteur_FTP**
   b. Transport : **Répertoire FTP**
   c. Répertoire principal FTP : **C:/racineftp**
4. Cliquez sur **Sauvegarder**.

Configuration du concentrateur en vue de la réception de fichiers binaires

Cette section décrit les étapes requises pour configurer le concentrateur afin qu'il reçoive les documents binaires que le partenaire B souhaite envoyer au partenaire interne.

Création d'une interaction pour les documents binaires

Pourquoi et quand exécuter cette tâche

Par défaut, WebSphere Partner Gateway fournit quatre interactions impliquant des documents binaires. Toutefois, il ne propose pas d'interaction pour les documents binaires en empaquetage de type None et destinés à un partenaire dont les documents sont également empaquetés en tant que None. Cette section vous indique comment créer l'interaction nécessaire pour permettre aux documents binaires de transiter par le système.

Procédure

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Création d'une interaction**.

3. Cliquez sur **Création** dans la vue **Gestion des interactions**.
4. Dans la zone **Source**, sélectionnez : **Package : None Protocole : Binaire (1.0) Type de documents : Binaire (1.0)**.
5. Dans la zone **Cible**, sélectionnez : **Package : None Protocole: Binaire (1.0) Type de documents : Binaire (1.0)**.
6. Sélectionnez éventuellement la carte **Transformation** .
7. Dans la liste des **actions**, sélectionnez **Passe-système**.
8. Cliquez sur **Sauvegarder**.

Mise à jour des fonctions business-to-business du partenaire interne

Pourquoi et quand exécuter cette tâche

Cette section explique comment configurer le partenaire interne pour qu'il accepte des documents binaires.

Procédure

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Cliquez sur l'icône **Afficher les détails** en regard de **Gest Com**.
4. Cliquez sur **Fonctions B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Package : None**.
7. Cliquez sur l'icône **Rôle inactif** de **Protocole : Binaire (1.0)** sous **Définition de la cible**.
8. Cliquez sur l'icône **Développer** en regard de **Protocole : Binaire (1.0)**.
9. Enfin, cliquez sur l'icône **Rôle inactif** pour **Type de documents : Binaire (1.0)** sous **Définition de la cible**.

Mise à jour des fonctions business-to-business du Partenaire B

Pourquoi et quand exécuter cette tâche

Cette section explique comment configurer le partenaire A pour lui permettre d'envoyer des documents binaires.

Procédure

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Cliquez sur l'icône **Afficher les détails** en regard du Partenaire B.
4. Cliquez sur **Fonctions B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : None** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Package : None**.
7. Cliquez sur l'icône **Rôle inactif** de **Protocole : Binaire (1.0)** sous **Définition de la source**.
8. Cliquez sur l'icône **Développer** en regard de **Protocole : Binaire (1.0)**.
9. Enfin, cliquez sur l'icône **Rôle inactif** pour **Type de documents : Binaire (1.0)** sous **Définition de la source**.

Création d'une nouvelle connexion de partenaires

Pourquoi et quand exécuter cette tâche

Cette section explique comment configurer une nouvelle connexion partenaire entre le partenaire interne et le partenaire B pour des documents binaires.

Procédure

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Sélectionnez **Partenaire B** dans la liste **Source**.
3. Sélectionnez **Partenaire interne** dans la liste **Cible**.
4. Cliquez sur **Rechercher**.
5. Localisez la connexion **None (N/A), Binaire (1.0), Binaire (1.0)** à **None (N/A), Binaire (1.0), Binaire (1.0)** et cliquez sur **Activation** pour l'activer.

Configuration du concentrateur pour les documents XML personnalisés

Comme indiqué dans «Traitement de documents XML personnalisés», à la page 163, vous devez configurer le concentrateur pour lui permettre d'acheminer des fichiers XML personnalisés. Cette section présente la procédure de configuration à suivre pour permettre au gestionnaire de documents d'acheminer le document XML suivant :

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Tester>
<Tester type="Test type A">
    <From>987654321</From>
    <To>123456789</To>
</Tester>
```

Pour cet exemple, le gestionnaire de documents utilise la balise racine pour identifier le type de document XML. Il extrait ensuite les valeurs à partir des zones origine et destination pour identifier les noms du partenaire d'origine et du partenaire de destination.

Création d'un format de définition de protocole CustomXML

Pourquoi et quand exécuter cette tâche

La première étape consiste à créer le nouveau protocole CustomXML que vous allez échanger.

Procédure

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur **Création d'une définition de documents**.
3. Sélectionnez **Protocole** dans la liste **Type de définition de documents**.
4. Entrez les informations suivantes :
   a. Code : **Custom XML**
   b. Version : **1.0**
   c. Description : **Exemple de définition de protocole**
5. Réglez le paramètre **Niveau du document** sur **Non**.
6. Réglez le paramètre **Etat** sur **Activé**.
7. Réglez le paramètre **Visibilité : Administrateur de concentrateur** sur **Oui**.
8. Réglez le paramètre **Visibilité : Partenaire interne** sur **Oui**.

9. Réglez le paramètre **Visibilité : partenaire** sur **Oui**.
10. Sélectionnez les éléments suivants :
    a. Package : **AS**
    b. Package : **None**
    c. Package : **Backend Integration**
11. Cliquez sur **Sauvegarder**.

Création de la définition de document Testeur_XML

Pourquoi et quand exécuter cette tâche

La deuxième étape consiste à créer une définition de documents pour le nouveau protocole.

Procédure

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur **Création d'une définition de documents**.
3. Sélectionnez **Type de documents** dans la liste **Type de flux de documents**.
4. Entrez les informations suivantes :
    a. Nom : **Tester_XML**
    b. Version : **1.0**
    c. Description : **Exemple de type de document XML personnalisé**
5. Réglez le paramètre **Niveau du document** sur **Oui**.
6. Réglez le paramètre **Etat** sur **Activé**.
7. Réglez le paramètre **Visibilité : Administrateur de concentrateur** sur **Oui**.
8. Réglez le paramètre **Visibilité : Partenaire interne** sur **Oui**.
9. Réglez le paramètre **Visibilité : partenaire** sur **Oui**.
10. Cliquez sur l'icône **Développer** en regard de **Package : AS** et sélectionnez **Protocole : CustomXML**.
11. Cliquez sur l'icône **Développer** en regard de**Package : None** et sélectionnez **Protocole : CustomXML**.
12. Cliquez sur l'icône **Développer** en regard de **Package : Backend Integration** et sélectionnez **Protocole : CustomXML**.
13. Cliquez sur **Sauvegarder**.

Création du format Testeur_XML

Pourquoi et quand exécuter cette tâche

Enfin, vous devez créer le format XML associé au nouveau protocole.

Procédure

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Formats XML**.
2. Cliquez sur **Création d'une famille de documents**.
3. Entrez ou sélectionnez les informations suivantes :
    a. Nom de famille : **Famille exemple**
    b. Protocole : **Custom XML 1.0**
    c. Type de famille : **Balise racine**
    d. Option grand fichier : **None**

e. Identificateur de famille : **Testeur**

4. Cliquez sur **Sauvegarder**.
5. Sur la page Famille de document qui s'affiche, cliquez sur **Créer un format XML**.
6. Dans la liste Type de document, sélectionnez **Tester_XML**.
7. Pour la valeur identificateur de format, saisissez **Type de test A**.
8. Pour l'expression XPath de l'identificateur de format, saisissez **/Tester/@type** .
9. Laissez la zone Espace de nom de préfixe vierge (le document n'utilise pas les mêmes espaces de nom) et précisez le Type de renvoi comme **Texte**.
10. Saisissez **1** dans la zone de valeur de version de format et la zone d'expression XPath. Modifiez le type de renvoi à **Constant**. Cela signifie que tous les documents qui ont l'identificateur de format "Tester" auront la bonne version pour une mise en correspondance avec ce format. Cela vient du fait que la version de tous les documents sera 1, et que la version de ce format est également 1. Par conséquent, la version correspond toujours.
11. Saisissez **/Tester/From** pour l'expression XPath pour l'identificateur entreprise de la source.
12. Saisissez **/Tester/To** pour l'expression XPath pour l'identificateur entreprise de la cible.
13. Laissez les zones restantes dans leur format. Elles sont facultatives et ne sont pas utilisées dans cet exemple.
14. Cliquez sur **Sauvegarder**.

Création d'une interaction pour les documents Testeur_XML

Pourquoi et quand exécuter cette tâche

Maintenant que vous disposez d'un nouveau protocole et d'un type de documents, vous pouvez configurer une interaction.

Procédure

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer une interaction**.
2. Dans l'écran **Gérer une interaction**, cliquez sur le **lien Création d'une interaction**.
3. Au niveau du paramètre **Source**, sélectionnez les éléments suivants :
   a. Package : **None**
   b. Protocole : **Custom XML (1.0)**
   c. Type de documents : **Tester_XML (1.0)**
4. Au niveau du paramètre **Cible**, sélectionnez les éléments suivants :
   a. Package : **None**
   b. Protocole : **Custom XML(1.0)**
   c. Type de documents : **Tester_XML (1.0)**
5. Dans la liste des **actions**, sélectionnez **Passe-système**.
6. Cliquez sur **Sauvegarder**.

Mise à jour des fonctions business-to-business du partenaire interne

Pourquoi et quand exécuter cette tâche

Pour permettre l'échange du document XML personnalisé, vous devez mettre à jour les fonctions business-to-business des partenaires.

Activez d'abord le partenaire interne pour qu'il reçoive les documents Tester_XML (pour qu'il en soit la cible).

Procédure

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez le partenaire interne dans la liste des partenaires (notez que dans cet exemple le partenaire interne possède l'identificateur entreprise 123456789).
4. Cliquez sur **Fonctions B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Package : None**.
7. Cliquez sur l'icône **Rôle inactif** de **Protocole : Custom XML(1.0)** sous **Définition de la cible**.
8. Cliquez sur l'icône **Développer** en regard de **Protocole : Custom XML(1.0)**.
9. Enfin, cliquez sur l'icône **Rôle inactif** de **Type de documents : Tester_XML(1.0)** sous **Définition de la cible**.

Mise à jour des fonctions business-to-business du Partenaire B

Pourquoi et quand exécuter cette tâche

La mise à jour des fonctions business-to-business du Partenaire B permet l'échange de messages à l'aide nouveau format XML personnalisé.

Activez le Partenaire B pour être la source des documents Tester_XML (notez que dans l'exemple, le Partenaire B possède l'identificateur entreprise 987654321).

Procédure

1. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez **Partenaire B** dans la liste des partenaires (notez que dans cet exemple le partenaire B possède l'identificateur entreprise 987654321).
4. Cliquez sur **Fonctions B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : None** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Package : None**.
7. Cliquez sur l'icône **Rôle inactif** de **Protocole : Custom XML(1.0)** sous **Définition de la source**.
8. Cliquez sur l'icône **Développer** en regard de **Protocole : Custom XML(1.0)**.
9. Enfin, cliquez sur l'icône **Rôle inactif** de **Type de documents : Tester_XML(1.0)** sous **Définition de la source**.

Création d'une nouvelle connexion de partenaires

Pourquoi et quand exécuter cette tâche

Enfin, créez une nouvelle connexion de partenaires.

Procédure

1. Cliquez sur **Administrateur du compte > Connexions.**
2. Sélectionnez **Partenaire B** dans la liste **Source**.
3. Sélectionnez **Partenaire interne** dans la liste **Cible**.
4. Cliquez sur **Rechercher**.
5. Localisez la connexion **None (N/A), Custom XML (1.0), Tester_XML (1.0)** à **None (N/A), Custom XML(1.0), Tester_XML(1.0)** et cliquez sur **Activation** pour l'activer.

Routage d'un document à l'aide de Custom XML

Copiez le XML d'exemple au débit de cet exemple et copiez-le dans un éditeur de texte. Sauvegardez le fichier sur votre ordinateur en lui donnant le nom de votre choix. Puis envoyez le fichier vers le concentrateur en le déplaçant dans le répertoire utilisé par le récepteur du fichier. Regardez dans le visualiseur de documents et vous devriez voir le document qui est routé du partenaire B vers le partenaire interne à l'aide de la connexion que vous avez spécifiée à cet effet.

Chapitre 20. Exemples d'EDI

La présente annexe propose des exemples illustrant l'envoi et la réception d'EDI, ainsi que leur transformation depuis et vers des documents XML et ROD (Record-Oriented Data).

Ces exemples ne sont pas liés à ceux de l'Chapitre 19, «Exemples de base», à la page 331. De nouvelles cibles, destinations et profils sont créés.

Remarque : Un exemple d'EDI traversant le concentrateur (sans désenveloppement ni transformation) est proposé en Chapitre 19, «Exemples de base», à la page 331.

Chacun des quatre exemples est indépendant. Ainsi, si vous suivez l'exemple EDI vers XML, vous pourrez suivre toutes les étapes (de la création des cibles à l'activation des connexions) nécessaires à l'exemple.

Cette annexe contient les rubriques suivantes :

Le but de ces exemples est de vous présenter rapidement les étapes nécessaires pour configurer un système. Si vous utilisez ces exemples pour configurer votre système, veillez à modifier les données pour correspondre à vos besoins (par exemple les noms et ID entreprise).

Exemple EDI vers ROD

Cette section présente un exemple d'envoi de transaction EDI (dans une enveloppe) au concentrateur, qui la transforme en document ROD (Record-oriented-data) et l'envoie au partenaire interne.

Désenveloppement et transformation d'un échange EDI

Pourquoi et quand exécuter cette tâche

Dans cet exemple, il est supposé que le spécialiste du mappage Data Interchange Services a créé une mappe de transformation qui transforme une transaction EDI 850 standard (définie avec le dictionnaire X12V5R1 et correspondant à la version 5010 de X12) en document ROD qui sera traité par l'application dorsale du partenaire interne. Dans cet exemple, la mappe est nommée S_DT_EDI_TO_ROD.eif.

Le spécialiste de mappage Data Interchange Services peut exporter la mappe de transformation directement dans la base de données WebSphere Partner Gateway. Il peut aussi vous envoyer le fichier, auquel cas vous utiliserez bcgDISImport pour l'importer dans WebSphere Partner Gateway. Cette annexe suit ce second scénario.

Importation de la mappe de transformation
Pourquoi et quand exécuter cette tâche

La présente section décrit la procédure permettant d'importer une mappe qui transformera une entrée EDI au format ROD. Lors de l'importation de la mappe de transformation, vous importez également la définition de document associée à la mappe.

Avant de pouvoir importer la mappe de transformation, le spécialiste de mappage Data Interchange Services doit vous l'envoyer. Cette procédure suppose que le fichier S_DT_EDI_TO_ROD.eif est présent sur votre système.

1. Ouvrez une fenêtre de commande.
2. Entrez la commande ou le script suivant :
   - Sous UNIX :

     ```
     <ProductDir>/bin/bcgDISImport.sh <ID_utilisateur_base_de_données>
     <mot de passe> S_DT_EDI_TO_ROD.eif
     ```

   - Sous Windows :

     ```
     <ProductDir>\bin\bcgDISImport.bat <ID utilisateur
     base de données>
     <mot de passe> S_DT_EDI_TO_ROD.eif
     ```

     où *<ID_utilisateur_base_de_données>* et *<mot_de_passe>* sont les valeurs que vous avez utilisées lors de l'installation de la base de données, dans le cadre de l'installation de WebSphere Partner Gateway.

Vérification de la mappe de transformation et des définitions de documents
Pourquoi et quand exécuter cette tâche

Pour vérifier que les mappes de transformation et définitions de documents importées sont disponibles sur la console de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de transformation**.

   La mappe S_DT_EDI_TO_ROD s'affiche.
2. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.

   Les définitions de documents auxquelles cette mappe est associée s'affichent :

Tableau 35. Document definition associated with the map

Source	Cible
Package : N/A Protocole : X12V5R1 (ALL)Type de document : 850 (TOUT)	Package : Aucun Protocole : DEMO850CL_DICTIONARY(TOUT) Type de document : DEMO850CLSUW (TOUT)

La mappe S_DT_EDI_TO_ROD a été définie pour transformer une transaction X12 850 (conforme au standard X12V5R1) en un protocole personnalisé (DEMO850CL_DICTIONARY) et en un type de documents (DEMO850CLSUW).

Configuration du récepteur
Pourquoi et quand exécuter cette tâche

Cette section explique comment créer un récepteur de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs** puis sur **Créer un récepteur**.

2. Dans la zone Nom du récepteur, entrez **RécepteurFichierEDI**.
3. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
4. Dans Chemin principal, entrez **/Data/Manager/editarget**.
5. Cliquez sur **Sauvegarder**.

Le partenaire envoie l'échange de données informatisé à ce récepteur.

Création des interactions
Pourquoi et quand exécuter cette tâche

Créez deux interactions : une pour l'enveloppe EDI et l'autre pour la transaction contenue dans l'enveloppe EDI.

Créez une interaction qui représente l'enveloppe EDI.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur **Création d'une interaction**.
3. Sous **Source**, développez **Package : None** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
4. Sous **Cible**, développez **Package : N/A** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Désenveloppement EDI**.

   Remarque : Aucune transformation ne se produit dans cette interaction. Le désenveloppement de l'EDI est effectué, générant la transaction individuelle (850). Vous n'avez donc pas besoin de mappe de transformation pour cette interaction.
6. Cliquez sur **Sauvegarder**.

Créez une interaction dont une source représente la transaction 850 et une cible le document transformé.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur **Création d'une interaction**.
3. Sous **Source**, développez **Package : N/A** et **Protocole : X12V5R1** puis sélectionnez **Type de documents : 850**.
4. Sous **Source**, développez **Package : None** et **Protocole : DEMO850CL_DICTIONARY** puis sélectionnez **Type de documents : DEMO850CLSUW**.
5. Dans la liste Mappe de transformation, sélectionnez **S_DT_EDI_TO_ROD**.
6. Dans la liste des actions, sélectionnez **Validation et translation EDI**.
7. Cliquez sur **Sauvegarder**.

Cette interaction représente la transformation d'une transaction EDI X12 850 standard dans un autre format. Vous devez par conséquent sélectionner une mappe de transformation.

Création des partenaires
Pourquoi et quand exécuter cette tâche

Dans cet exemple, vous disposez de deux partenaires : le partenaire interne (gestionnaire) et un partenaire externe (TP1).

Créez le profil du partenaire interne :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du partenaire, tapez **Gestionnaire**
4. Pour le Type de partenaire, sélectionnez **Partenaire interne**.
5. Cliquez sur **Nouveau** pour ID entreprise et tapez `000000000` pour ID de forme libre.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour ID entreprise et tapez `01-000000000` pour ID de forme libre.
7. Cliquez sur **Sauvegarder**.

Créez le second partenaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du partenaire, tapez **TP1**
4. Pour le Type de partenaire, sélectionnez **Partenaire externe**.
5. Cliquez sur **Nouveau** pour ID entreprise et tapez `000000001` pour ID de forme libre.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour ID entreprise et tapez `01-000000001` pour ID de forme libre.
7. Cliquez sur **Sauvegarder**.

Création des destinations

Pourquoi et quand exécuter cette tâche

Créez des destinations fichier-répertoire pour les deux partenaires de l'exemple. Créez d'abord une destination pour le gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.
   a. Dans Nom, tapez **DestinationFichierGestionnaire**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file://Data/Manager/filedestination**
   d. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les destinations du partenaire interne.
6. Cliquez sur **Afficher les destinations par défaut**.
7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4.
8. Cliquez sur **Sauvegarder**.

Ensuite, créez une destination pour le partenaire.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Sélectionnez l'autre partenaire créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **DestinationFichierTP1**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file://Data/TP1/filedestination**
   d. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Liste** pour dresser la liste de toutes les destinations configurées pour le partenaire.
6. Cliquez sur **Afficher les destinations par défaut**.
7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4.
8. Cliquez sur **Sauvegarder**.

Configuration des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

Activez les fonctions business-to-business des deux partenaires de cet échange. Dans cet exemple, l'échange EDI est émis par le partenaire externe (TP1) et sera transmis au partenaire interne.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du partenaire source de cet exemple (**TP1**).
3. Cliquez sur **Fonctions B2B**.
4. Activez deux ensembles de fonctions pour le partenaire source.
   a. Tout d'abord, activez la définition de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : ISA (TOUT)**.
   b. Ensuite, activez la définition de documents représentant la transaction 850 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : X12V5R1**.
      4) Développez **Protocole X12V5R1 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : 850**.

5. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du partenaire cible de cet exemple (**Gestionnaire**).
7. Cliquez sur **Fonctions B2B**.
8. Activez deux ensembles de fonctions pour le partenaire cible.
   a. Tout d'abord, activez la définition de documents représentant l'enveloppe :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : N/A**, afin de l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : ISA (TOUT)**.
   b. Ensuite, activez la définition de documents représentant le document transformé :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : DEMO850CL_DICTIONARY (TOUT)**.
      4) Développez **Protocole : DEMO850CL_DICTIONARY (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : DEMO850CLSUW(TOUT)**.

Activation des connexions

Pourquoi et quand exécuter cette tâche

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Sélectionnez **TP1** dans la liste des sources.
3. Sélectionnez **Gestionnaire** dans la liste des cibles.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion qui représente l'enveloppe :

Tableau 36. Connexion de l'enveloppe

Source	Cible
Package : Aucun (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA (TOUT)	Package : N/A (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA(TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente la transaction 850 vers le document transformé :

Tableau 37. Connexion de la transaction EDI vers le document ROD

Source	Cible
Package : N/A (N/A) Protocole : X12V5R1Type de document : 850 (TOUT)	Package : Aucun (N/A) Protocole : DEMO850CL_DICTIONARY (TOUT) Type de document : DEMO850CLSUW (TOUT)

Ajout d'attributs
Pourquoi et quand exécuter cette tâche

Définissez les attributs qui autorisent les documents ayant le même ID :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Cliquez sur l'icône **Développer** en regard de **Package : None**.
3. Cliquez sur l'icône **Edition des valeurs d'attribut** en regard de **Protocole : EDI-X12**.
4. Accédez à la section Attributs de contexte du type de documents de la page. Sur la ligne **Autoriser les documents avec des ID en double** de la liste, sélectionnez **Oui**.
5. Cliquez sur **Sauvegarder**.

A ce stade, si TP1 envoie un EDI contenant une transaction 850 au partenaire interne, l'EDI sera désenveloppé et générera une transaction 850. Elle sera alors transformée dans le type de document DEMO850CLSUW et le document résultant sera envoyé à la destination du partenaire interne.

Ajout d'un TA1 à un échange

Dans X12, TA1 est un segment optionnel utilisé pour accusé de réception de l'EDI. L'émetteur peut demander un TA1 au destinataire en définissant l'élément 14 de l'En-tête de contrôle EDI ISA sur **1**. L'attribut Autoriser une requête de WebSphere Partner Gateway peut servir à vérifier si un TA1 est envoyé lorsque l'émetteur le demande.

La mappe &WDI_TA1_ACK est installée en même temps que WebSphere Partner Gateway afin que vous n'ayez pas à l'importer.

Création des associations
Pourquoi et quand exécuter cette tâche

Pour associer la mappe à une définition de documents, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes d'accusé de réception fonctionnel EDI**.

   La mappe &WDI_TA1_ACK s'affiche.
2. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.

   Vous voyez les informations concernant la mappe, ainsi qu'un dossier pour chaque type d'empaquetage disponible sur le système.
3. Créez l'association à la définition de documents en procédant comme suit :
   a. Cochez la case en regard de **Package : None** et développez le dossier.
   b. Cochez la case en regard de **Protocole : EDI-X12 (TOUT)** et développez le dossier.
   c. Cochez la case en regard de **Type de documents : ISA (TOUT)**.
   d. Cliquez sur **Sauvegarder**.

Vous avez créé une association entre la mappe &WDI_TA1_ACK1 et la définition de documents pour l'enveloppe.

Création d'interactions

Pourquoi et quand exécuter cette tâche

Créez une interaction qui représente la transaction TA1.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Sous **Source**, développez **Package : N/A** et **Protocole : &X44TA1** puis sélectionnez **Type de documents : TA1**.
4. Sous **Source**, développez **Package : N/A** et **Protocole : &X44TA1** puis sélectionnez **Type de documents : TA1**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Sauvegarder**.

Créez une interaction dont une source représente l'enveloppe 850 qui contiendra le TA1.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Sous **Source**, développez **Package : N/A** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
4. Sous **Source**, développez **Package : None** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Sauvegarder**.

Activation des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

Ensuite, vous ajoutez les interactions nouvellement créées aux fonctions business-to-business des partenaires.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du partenaire source de cet exemple (**Gestionnaire**).

   Remarque : Gardez en mémoire que le TA1 circule du partenaire qui reçoit le document ROD vers le partenaire qui l'a envoyé. Dans cet exemple, le gestionnaire est la source du TA1 et le partenaire TP1 en est la cible.
3. Cliquez sur **Fonctions B2B**.
4. Activez deux ensembles de fonctions pour le partenaire source.
   a. Tout d'abord, activez la fonction pour le TA1.
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : &X44TA1**.
      4) Développez **Protocole : &X44TA1**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : TA1 (TOUT)**.

b. Ensuite, activez la fonction pour l'enveloppe :
   1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
   2) Développez **Package : N/A**.
   3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : EDI-X12**.
   4) Développez **Protocole : EDI-X12 (TOUT)**.
   5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : ISA (TOUT)**.

5. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du partenaire cible de cet exemple (**TP1**).
7. Cliquez sur **Fonctions B2B**.
8. Activez deux ensembles de fonctions pour le partenaire cible.
   a. Tout d'abord, activez la définition de documents représentant le TAI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : N/A**, afin de l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : &X44TA1 (TOUT)**.
      4) Développez **Protocole : &X44TA1 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : TA1 (TOUT)**.
   b. Ensuite, activez la définition de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : ISA (TOUT)**.

Création du profil d'enveloppe

Pourquoi et quand exécuter cette tâche

Vous créez ensuite le profil de l'enveloppe qui contiendra le TA1 :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Profil d'enveloppe**.
2. Cliquez sur **Créer**.
3. Tapez le nom du profil : **EnvProf1**.
4. Dans la liste EDI Standard, sélectionnez **X12**.
5. Le bouton **Général** est sélectionné par défaut. Tapez les valeurs suivantes pour les attributs généraux de l'enveloppe :
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**

6. Cliquez sur le bouton **Interchange** et indiquez les valeurs suivantes pour les attributs d'échange :
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Cliquez sur **Sauvegarder**.

Activation des connexions de partenaire

Pourquoi et quand exécuter cette tâche

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Sélectionnez **Gestionnaire** dans la liste des sources.
3. Sélectionnez **TP1** dans la liste des cibles.
4. Cliquez sur **Rechercher**.
5. Activez la connexion qui représente le TA1.

Tableau 38. Connexion TA1

Source	Cible
Package : N/A (N/A) Protocole : &X44TA1 (TOUT) Type de document : TA1 (TOUT)	Package : N/A (N/A) Protocole : &X44TA1 (TOUT) Type de document : TA1 (TOUT)

6. Activez la connexion qui représente l'enveloppe :

Tableau 39. Connexion de l'enveloppe

Source	Cible
Package : N/A (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA(TOUT)	Package : Aucun (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA (TOUT)

Configuration des attributs

Pourquoi et quand exécuter cette tâche

Pour préciser les attributs du profil de l'enveloppe :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Sélectionnez **TP1** dans la liste.
3. Cliquez sur **Fonctions B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Package : None**.
5. Cliquez sur l'icône **Edition** en regard de **Protocole : EDI-X12 (TOUT)**.
6. Sur la ligne **Autoriser une requête TA1**, sélectionnez **Oui**.
7. Cliquez sur **Sauvegarder**.
8. Cliquez de nouveau sur **Fonctions B2B**.
9. Cliquez sur l'icône **Développer** en regard de **Package : N/A**.

10. Cliquez sur l'icône **Edition** en regard de **Protocole : &X44TA1 (TOUT)**.
11. Précisez les attributs suivants :
    a. Sur la ligne Profil d'enveloppe, sélectionnez **EnvProf1** dans la liste.
    b. Sur la ligne Qualificatif EDI, tapez **01**.
    c. Sur la ligne Identificateur EDI, tapez **000000001**.
    d. Sur la ligne Indicateur de syntaxe EDI, tapez **T**.
12. Cliquez sur **Sauvegarder**.

Par cette série de tâches, vous avez ajouté un accusé de réception TA1 à l'échange. Une fois l'EDI reçu, WebSphere Partner Gateway renvoie un TA1 à l'émetteur (TP1). Le TA1 est envoyé dans une enveloppe conforme au profil EnvProf1.

Ajout d'une mappe d'accusé de réception fonctionnel

Cette section explique comment ajouter un accusé de réception fonctionnel standard (997) au flux décrit dans « Exemple EDI vers ROD», à la page 351. L'accusé de réception fonctionnel confirme à l'émetteur la bonne réception de la transaction.

Remarque : Cet exemple est similaire à celui de « Ajout d'un TA1 à un échange», à la page 357, mais il n'est pas directement relié. En effet, il est basé sur les tâches que vous avez réalisées dans l'« Exemple EDI vers ROD», à la page 351.

WebSphere Partner Gateway inclut un ensemble de mappes d'accusé de réception fonctionnel préinstallées dont le nom commence par $DT_FA. Il est suivi par le nom du message d'accusé de réception fonctionnel avec sa version et son édition. Par exemple, la Version 2 Edition 4 du message d'accusé de réception fonctionnel 997 est nommée $DT_997V2R4. Consultez la section «Configuration des accusés de réception», à la page 224 pour connaître la liste des mappes fournies avec WebSphere Partner Gateway.

Information associée

Création des associations

Pourquoi et quand exécuter cette tâche

Pour associer la mappe à une définition de documents, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes d'accusé de réception fonctionnel EDI**.
   La mappe &DT_FA997V2R4 s'affiche.
2. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.
   Vous voyez les informations concernant la mappe, ainsi qu'un dossier pour chaque type d'empaquetage disponible sur le système.
3. Créez l'association à la définition de documents en procédant comme suit :
   a. Cochez la case en regard de **Package : N/A** et développez le dossier.
   b. Cochez la case en regard de **Protocole : X12V5R1** et développez le dossier.
   c. Cochez la case en regard de **Type de documents : 850**.
   d. Cliquez sur **Sauvegarder**.

Vous avez associé cette mappe 997 d'accusé de réception fonctionnel au protocole X12.

Création d'interactions

Pourquoi et quand exécuter cette tâche

Créez une interaction qui représente l'accusé de réception 997.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Sous **Source**, développez **Package : N/A** et **Protocole : &DT99724**, puis sélectionnez **Type de documents : 997**.
4. Sous **Cible**, développez **Package : N/A** et **Protocole : &DT99724**, puis sélectionnez **Type de documents : 997**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Sauvegarder**.

Créez une interaction qui représente l'enveloppe.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez **Package : N/A** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
4. Développez **Package : None** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Sauvegarder**.

Activation des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

Ensuite, vous ajoutez les interactions nouvellement créées aux fonctions business-to-business des partenaires.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du partenaire source de cet exemple (**Gestionnaire**).

   Remarque : Gardez en mémoire que l'accusé de réception fonctionnel circule du partenaire qui reçoit le document ROD vers le partenaire qui l'a envoyé. Dans cet exemple, le gestionnaire est la source de l'accusé de réception fonctionnel et le TP1 du partenaire en est la cible.
3. Cliquez sur **Fonctions B2B**.
4. Activez deux ensembles de fonctions pour le partenaire source.
   a. Tout d'abord, activez la fonction pour le FA.
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : &DT99724**.
      4) Développez **Protocole : &DT99724**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : 997 (TOUT)**.

b. Ensuite, activez la fonction pour l'enveloppe :
   1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
   2) Développez **Package : N/A**.
   3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : EDI-X12**.
   4) Développez **Protocole : EDI-X12 (TOUT)**.
   5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : ISA (TOUT)**.

5. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du partenaire cible de cet exemple (**TP1**).
7. Cliquez sur **Fonctions B2B**.
8. Activez deux ensembles de fonctions pour le partenaire cible.
   a. Tout d'abord, activez la définition de documents représentant le 997 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : N/A**, afin de l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : &DT99724 (TOUT)**.
      4) Développez **Protocole : &DT99724 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : 997 (TOUT)**.
   b. Ensuite, activez la définition de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : ISA(TOUT)**.

Création du profil d'enveloppe

Pourquoi et quand exécuter cette tâche

Vous créez ensuite le profil de l'enveloppe qui contiendra l'accusé de réception 997. Un accusé de réception fonctionnel, comme une transaction, doit être enveloppé avant d'être envoyé.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Profil d'enveloppe**.
2. Cliquez sur **Créer**.
3. Tapez le nom du profil : **EnvProf1**.
4. Dans la liste EDI Standard, sélectionnez **X12**.
5. Le bouton **Général** est sélectionné par défaut. Tapez les valeurs suivantes pour les attributs généraux de l'enveloppe :
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**

- TRXCTLLEN: **9**
- MAXDOCS: **1000**

6. Cliquez sur le bouton **Interchange** et indiquez les valeurs suivantes pour les attributs EDI :
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Cliquez sur **Sauvegarder**.

Activation des connexions de partenaire
Pourquoi et quand exécuter cette tâche

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Sélectionnez **Gestionnaire** dans la liste des sources.
3. Sélectionnez **TP1** dans la liste des cibles.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion qui représente l'accusé de réception fonctionnel 997 :

Tableau 40. Connexion de l'accusé de réception fonctionnel

Source	Cible
Package : N/A (N/A) Protocole : &DT99724 (TOUT) Type de document : 997 (TOUT)	Package : N/A (N/A) Protocole : &DT99724 (TOUT) Type de document : 997 (TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente l'enveloppe EDI renvoyée à l'émetteur de l'échange :

Tableau 41. Connexion de l'enveloppe

Source	Cible
Package : N/A (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA(TOUT)	Package : Aucun (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA (TOUT)

Configuration des attributs
Pourquoi et quand exécuter cette tâche

Tout d'abord, précisez la mappe d'accusé de réception fonctionnel à utiliser :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Sélectionnez **TP1** dans la liste.
3. Cliquez sur **Fonctions B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Package : N/A**.
5. Cliquez sur l'icône **Edition** en regard de **Protocole : X12V5R1 (TOUT)**.

6. Sur la ligne Mappe d'accusé de réception fonctionnel, sélectionnez **&DT_FA997V2R4**.
7. Cliquez de nouveau sur **Fonctions B2B**.
8. Cliquez sur l'icône **Développer** en regard de **Package : N/A**.
9. Cliquez sur l'icône **Edition** en regard de **Protocole : &DT99724 (TOUT)**.
10. Précisez les attributs suivants :
    a. Sur la ligne Profil d'enveloppe, sélectionnez **EnvProf1** dans la liste.
    b. Sur la ligne Qualificatif EDI, tapez **01**.
    c. Sur la ligne Identificateur EDI, tapez **000000001**.
    d. Sur la ligne Indicateur de syntaxe EDI, tapez **T**.
11. Cliquez sur **Sauvegarder**.

Dans cette série de tâches, vous avez ajouté un accusé de réception fonctionnel EDI-X12 997 à l'échange, afin que lorsque le partenaire interne reçoit le document, il renvoie le 997 à l'émetteur (TP1). L'accusé de réception 997 est envoyé dans une enveloppe conforme au profil EnvProf1.

Exemple EDI vers XML

Cette section présente un exemple d'envoi de transaction EDI (dans une enveloppe) au concentrateur, qui la transforme en document XML et l'envoie au partenaire interne.

Dans cet exemple, il est supposé que le spécialiste du mappage Data Interchange Services a créé une mappe qui transforme une transaction EDI 879 standard (définie avec le dictionnaire X12V5R1 et correspondant à la version 5010 de X12) en un document XML, qui sera traité par l'application dorsale du partenaire interne. Dans cet exemple, la mappe est nommée S_DT_EDI_TO_XML.eif.

Le spécialiste de mappage Data Interchange Services peut exporter la mappe de transformation directement dans la base de données WebSphere Partner Gateway. Il peut aussi vous envoyer le fichier, auquel cas vous utiliserez bcgDISImport pour l'importer dans WebSphere Partner Gateway. Cette annexe suit ce second scénario.

Importation de la mappe de transformation

Pourquoi et quand exécuter cette tâche

La présente section décrit la procédure permettant d'importer une mappe qui transformera une entrée EDI au format XML. Lors de l'importation de la mappe de transformation, vous importez également la définition de document associée à la mappe.

Avant de pouvoir importer la mappe de transformation, le spécialiste de mappage Data Interchange Services doit vous l'envoyer. Cette procédure suppose que le fichier S_DT_EDI_TO_XML.eif est présent sur votre système.

1. Ouvrez une fenêtre de commande.
2. Entrez la commande ou le script suivant :
   - Sous UNIX :

     ```
     <ProductDir>/bin/bcgDISImport.sh <ID_utilisateur_base_de_données>
      <mot de passe> S_DT_EDI_TO_XML.eif
     ```

   - Sous Windows :

```
<ProductDir>\bin\bcgDISImport.bat <ID utilisateur
base de données>
 <mot de passe> S_DT_EDI_TO_XML.eif
```

où <*ID_utilisateur_base_de_données*> et <*mot_de_passe*> sont les valeurs que vous avez utilisées lors de l'installation de la base de données, dans le cadre de l'installation de WebSphere Partner Gateway.

Vérification de la mappe de transformation et des définitions de documents

Pourquoi et quand exécuter cette tâche

Pour vérifier que les mappes de transformation et définitions de documents importées sont disponibles sur la console de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de transformation**.

   La mappe S_DT_EDI_TO_XML s'affiche.
2. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.

   Les définitions de documents auxquelles cette mappe est associée s'affichent :

Tableau 42. Définition de document associée à la mappe

Source	Cible
Package : N/A Protocole : X12V5R1Type de document : 879 (TOUT)	Package : Aucun Protocole : FVT-XML-TEST (TOUT) Type de document : WWRE_ITEMCREATIONINTERNAL (TOUT)

La mappe S_DT_EDI_TO_XML a été définie pour transformer une transaction X12 879 (conforme au standard X12V5R1) en un protocole personnalisé.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Cette section explique comment créer un récepteur de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs** puis sur **Créer un récepteur**.
2. Dans la zone Nom du récepteur, entrez **RécepteurFichierEDI**.
3. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
4. Dans Chemin principal, entrez **/Data/Manager/editarget**.
5. Cliquez sur **Sauvegarder**.

Le partenaire envoie l'échange de données informatisé à ce récepteur.

Création des interactions

Pourquoi et quand exécuter cette tâche

Créez deux interactions : une pour l'enveloppe EDI et l'autre pour la transaction contenue dans l'enveloppe EDI.

Créez une interaction qui représente l'enveloppe EDI.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.

2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez **Package : None** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
4. Développez **Package : N/A** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Désenveloppement EDI**.

   Remarque : Aucune transformation ne se produit dans cette interaction. Le désenveloppement de l'EDI est effectué, générant la transaction individuelle (879). Vous n'avez donc pas besoin de mappe de transformation pour cette interaction.
6. Cliquez sur **Sauvegarder**.

Créez une interaction dont une source représente la transaction 879 et une cible le document transformé.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez **Package : N/A** et **Protocole : X12V5R1** puis sélectionnez **Type de documents : 879**.
4. Développez **Package : None** et **Protocole : FVT-XML-TEST** puis sélectionnez **Type de documents: WWRE_ITEMCREATIONINTERNAL**.
5. Dans la liste des mappes de transformation, sélectionnez **S_DT_EDI_TO_XML**.
6. Dans la liste des actions, sélectionnez **Validation et translation EDI**.
7. Cliquez sur **Sauvegarder**.

Cette interaction représente la transformation d'une transaction EDI X12 879 standard dans un autre format. Vous devez par conséquent sélectionner une mappe de transformation.

Création des partenaires

Pourquoi et quand exécuter cette tâche

Dans cet exemple, vous disposez de deux partenaires : le partenaire interne (gestionnaire) et un partenaire externe (TP1).

Créez le profil du partenaire interne :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du partenaire, tapez **Gestionnaire**
4. Pour le Type de partenaire, sélectionnez **Partenaire interne**.
5. Cliquez sur **Nouveau** pour ID entreprise et tapez `000000000` pour ID de forme libre.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour ID entreprise et tapez `01-000000000` pour ID de forme libre.
7. Cliquez sur **Sauvegarder**.

Créez le second partenaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.

2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du partenaire, tapez **TP1**
4. Pour le Type de partenaire, sélectionnez **Partenaire externe**.
5. Cliquez sur **Nouveau** pour ID entreprise et tapez `000000001` pour ID de forme libre.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour ID entreprise et tapez `01-000000001` pour ID de forme libre.
7. Cliquez sur **Sauvegarder**.

Création des destinations

Pourquoi et quand exécuter cette tâche

Créez des destinations fichier-répertoire pour les deux partenaires de l'exemple. Créez d'abord une destination pour le gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.
   a. Dans Nom, tapez **DestinationFichierGestionnaire**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file://Data/Manager/filedestination**
   d. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les destinations du partenaire interne.
6. Cliquez sur **Afficher les destinations par défaut**.
7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4.
8. Cliquez sur **Sauvegarder**.

Ensuite, créez une destination pour le partenaire.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Sélectionnez l'autre partenaire créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **DestinationFichierTP1**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file://Data/TP1/filedestination**
   d. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Liste** pour dresser la liste de toutes les destinations configurées pour le partenaire.
6. Cliquez sur **Afficher les destinations par défaut**.

7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4, à la page 368.
8. Cliquez sur **Sauvegarder**.

Configuration des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

Activez les fonctions business-to-business des deux partenaires de cet échange. Dans cet exemple, l'échange EDI est émis par le partenaire externe (TP1) et sera transmis au partenaire interne.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du partenaire source de cet exemple (**TP1**).
3. Cliquez sur **Fonctions B2B**.
4. Activez deux ensembles de fonctions pour le partenaire source.
   a. Tout d'abord, activez la définition de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : ISA (TOUT)**.
   b. Ensuite, activez la définition de documents représentant la transaction :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : X12V5R1**.
      4) Développez **Protocole X12V5R1 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : 879**.
5. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du partenaire cible de cet exemple (**Gestionnaire**).
7. Cliquez sur **Fonctions B2B**.
8. Activez deux ensembles de fonctions pour le partenaire cible.
   a. Tout d'abord, activez la définition de documents :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : N/A**, afin de l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.

5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : ISA (TOUT)**.

b. Ensuite, activez la définition de documents représentant le document transformé :

1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.

2) Développez **Package : None**.

3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : FVT-XML-TEST (TOUT)**.

4) Développez **Protocole : FVT-XML-TEST (TOUT)**.

5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents :WWRE_ITEMCREATIONINTERNAL (TOUT)**.

Activation des connexions

Pourquoi et quand exécuter cette tâche

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Sélectionnez **TP1** dans la liste des sources.
3. Sélectionnez **Gestionnaire** dans la liste des cibles.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion qui représente l'enveloppe :

Tableau 43. Connexion de l'enveloppe

Source	Cible
Package : Aucun (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA (TOUT)	Package : N/A (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA(TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente la transaction 879 vers le document transformé :

Tableau 44. Connexion de la transaction EDI vers le document XML

Source	Cible
Package : N/A (N/A) Protocole : X12V5R1 (TOUT) Type de document : 879 (TOUT)	Package : Aucun (N/A) Protocole : FVT-XML-TEST (TOUT) Type de document : WWRE_ITEMCREATIONINTERNAL (TOUT)

A ce stade, si TP1 a envoyé un EDI contenant une transaction 879 au partenaire interne, l'EDI sera désenveloppé et générera une transaction 879. Elle sera alors transformée et le document résultant sera envoyé à la destination du partenaire interne.

Exemple XML vers EDI

Cette section fournit un exemple d'envoi de document XML par le partenaire interne au concentrateur, qui le transforme en transaction EDI enveloppée dans un EDI et l'envoie à un partenaire.

Dans cet exemple, il est supposé que le spécialiste du mappage Data Interchange Services a créé une mappe de transformation qui transforme un document XML en

transaction EDI 850 standard (définie avec le dictionnaire MX12V3R1) qui sera traitée par le partenaire. Dans cet exemple, la mappe est nommée S_DT_XML_TO_EDI.eif.

Le spécialiste de mappage Data Interchange Services peut exporter la mappe de transformation directement dans la base de données WebSphere Partner Gateway. Il peut aussi vous envoyer le fichier, auquel cas vous utiliserez bcgDISImport pour l'importer dans WebSphere Partner Gateway. Cette annexe suit ce second scénario.

Importation de la mappe de transformation

Pourquoi et quand exécuter cette tâche

La présente section décrit la procédure permettant d'importer une mappe de transformation qui transformera une entrée XML en transaction EDI. Lors de l'importation de la mappe de transformation, vous importez également la définition de document associée à la mappe.

Avant de pouvoir importer la mappe de transformation, le spécialiste de mappage Data Interchange Services doit vous l'envoyer. Cette procédure suppose que le fichier S_DT_XML_TO_EDI.eif est présent sur votre système.

1. Ouvrez une fenêtre de commande.
2. Entrez la commande ou le script suivant :
   - Sous UNIX :

     ```
     <ProductDir>/bin/bcgDISImport.sh <ID_utilisateur_base_de_données>
      <mot de passe> S_DT_XML_TO_EDI.eif
     ```

   - Sous Windows :

     ```
     <ProductDir>\bin\bcgDISImport.bat <ID utilisateur
     base de données>
      <mot de passe> S_DT_XML_TO_EDI.eif
     ```

     où <*ID_utilisateur_base_de_données*> et <*mot_de_passe*> sont les valeurs que vous avez utilisées lors de l'installation de la base de données, dans le cadre de l'installation de WebSphere Partner Gateway.

Vérification de la mappe de transformation et des définitions de documents

Pourquoi et quand exécuter cette tâche

Pour vérifier que les mappes de transformation et définitions de documents importées sont disponibles sur la console de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de transformation**.

   La mappe S_DT_XML_TO_EDI s'affiche.
2. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.

   Les définitions de documents auxquelles cette mappe est associée s'affichent :

Tableau 45. Définitions de documents associées à la mappe

Source	Cible
Package : Aucun) Protocole : FVT-XML-TEST (TOUT) Type de document : ICGCPO (TOUT)	Package : N/A Protocole : MX12V3R1(TOUT) Type de document : 850 (TOUT)

La mappe S_DT_XML_TO_EDI a été définie pour transformer un document XML en transaction EDI.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Cette section explique comment créer un récepteur de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs** puis sur **Créer un récepteur**.
2. Dans la zone Nom du récepteur, entrez **RécepteurFichierXML**.
3. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
4. Dans Chemin principal, entrez **/Data/Manager/xmltarget**.
5. Dans la liste des points de configuration, sélectionnez **Preprocess**.
6. Sélectionnez **com.ibm.bcg.edi.receiver.preprocesshandler.XMLSplitterHandler** dans la liste des gestionnaires disponibles et cliquez sur **Ajouter** pour le déplacer dans la liste des gestionnaires configurés.
7. Cliquez sur **Sauvegarder**.

Le partenaire interne envoie le document XML à ce récepteur.

Création des interactions

Pourquoi et quand exécuter cette tâche

Créez deux interactions : une pour l'enveloppe XML-to-EDI et l'autre pour la transaction contenue dans l'enveloppe EDI.

Créez une interaction dont la source représente le document XML et la cible la transaction 850 transformée.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez **Package : None** et **Protocole : FVT-XML-TEST** puis sélectionnez **Type de documents : ICGCPO**.
4. Développez **Package : N/A** et **Protocole : MX12V3R1**, puis sélectionnez **Type de documents : 850**.
5. Dans la liste Mappe de transformation, sélectionnez **S_DT_XML_TO_EDI**.
6. Dans la liste des actions, sélectionnez **Traduction XML et validation EDI**.
7. Cliquez sur **Sauvegarder**.

Cette interaction représente la transformation d'un document XML en transaction EDI. Par conséquent vous devez sélectionner une mappe de transformation.

Créez une interaction qui représente l'enveloppe EDI.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez **Package : N/A** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.

4. Développez **Package : None** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Passe-système**.

   Remarque : Aucune transformation ne se produit dans cette interaction.
6. Cliquez sur **Sauvegarder**.

Création des partenaires

Pourquoi et quand exécuter cette tâche

Dans cet exemple, vous disposez de deux partenaires : le partenaire interne (gestionnaire) et un partenaire externe (TP1).

Créez le profil du partenaire interne :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du partenaire, tapez **Gestionnaire**
4. Pour le Type de partenaire, sélectionnez **Partenaire interne**.
5. Cliquez sur **Nouveau** pour ID entreprise et tapez `000000000` pour ID de forme libre.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour créer un ID entreprise et tapez `01-000000000` pour ID de forme libre. Lorsque vous cliquez sur Nouveau, la zone de saisie ID messagerie est également affichée et activée pour que vous puissiez créer un ID messagerie.
7. Cliquez sur **Nouveau** pour créer un nouvel ID messagerie et saisissez votre ID messagerie dans la zone Identificateur de messagerie. Vous pouvez aussi cliquer sur Nouveau pour créer plusieurs ID messagerie.
8. Cliquez sur **Sauvegarder**.

Créez le second partenaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du partenaire, tapez **TP1**
4. Pour le Type de partenaire, sélectionnez **Partenaire externe**.
5. Cliquez sur **Nouveau** pour créer un ID entreprise et tapez `01-000000000` pour ID de forme libre. Lorsque vous cliquez sur Nouveau, la zone de saisie ID messagerie est également affichée et activée pour que vous puissiez créer un ID messagerie.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour créer un nouvel ID messagerie et saisissez votre ID messagerie dans la zone Identificateur de messagerie. Vous pouvez aussi cliquer sur Nouveau pour créer plusieurs ID messagerie.
7. Cliquez sur **Sauvegarder**.

Création des destinations

Pourquoi et quand exécuter cette tâche

Créez des destinations fichier-répertoire pour les deux partenaires de l'exemple. Créez d'abord une destination pour le gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.
   a. Dans Nom, tapez **DestinationFichierGestionnaire**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file://Data/Manager/filedestination**
   d. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les destinations du partenaire interne.
6. Cliquez sur **Afficher les destinations par défaut**.
7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4.
8. Cliquez sur **Sauvegarder**.

Ensuite, créez une destination pour le partenaire.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Sélectionnez l'autre partenaire créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **DestinationFichierTP1**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file://Data/TP1/filedestination**
   d. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Liste** pour dresser la liste de toutes les destinations configurées pour le partenaire.
6. Cliquez sur **Afficher les destinations par défaut**.
7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4.
8. Cliquez sur **Sauvegarder**.

Configuration des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

Activez les fonctions business-to-business des deux partenaires de cet échange. Dans cet exemple, le document XML est émis par le partenaire interne et sera transmis au partenaire externe.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.

2. Cliquez sur l'icône **Afficher les détails** du partenaire source de cet exemple (**ComMan**).
3. Cliquez sur **Fonctions B2B**.
4. Activez trois ensembles de fonctions pour le partenaire source.
   a. Activez la définition de documents représentant le document XML :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : FVT-XML-TEST (TOUT)**.
      4) Développez **Protocole : FVT-XML-TEST (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : ICGCPO (TOUT)**.
   b. Ensuite, activez la définition de documents représentant le document transformé :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : MX12V3R1 (TOUT)**.
      4) Développez **Protocole : MX12V3R1 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : 850**.
   c. Ensuite, activez la définition de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : ISA (TOUT)**.
5. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du partenaire cible de cet exemple (**TP1**).
7. Cliquez sur **Fonctions B2B**.
8. Activez deux ensembles de fonctions pour le partenaire cible.
   a. Tout d'abord, activez la définition de documents représentant la transaction EDI 850 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : N/A**, afin de l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : MX12V3R1 (TOUT)**.
      4) Développez **Protocole : MX12V3R1 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : 850 (TOUT)**.

b. Ensuite, activez la définition de documents :
   1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.
   2) Développez **Package : None**.
   3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
   4) Développez **Protocole : EDI-X12 (TOUT)**.
   5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : ISA(TOUT)**.

Création du profil d'enveloppe

Pourquoi et quand exécuter cette tâche

Vous créez ensuite le profil de l'enveloppe qui contiendra la transaction 850 transformée :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Profil d'enveloppe**.
2. Cliquez sur **Créer**.
3. Tapez le nom du profil : **EnvProf1**.
4. Dans la liste EDI Standard, sélectionnez **X12**.
5. Le bouton **Général** est sélectionné par défaut. Tapez les valeurs suivantes pour les attributs généraux de l'enveloppe :
   - INTCTLLEN: **9**
   - GRPCTLLEN: **9**
   - TRXCTLLEN: **9**
   - MAXDOCS: **1000**
6. Cliquez sur le bouton **Interchange** et indiquez les valeurs suivantes pour les attributs d'échange :
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. Cliquez sur **Sauvegarder**.

Création du format XML

Pourquoi et quand exécuter cette tâche

Cette section explique comment créer le format XML personnalisé.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Formats XML**.
2. Cliquez sur **Création du format XML**.
3. Dans Format d'acheminement, sélectionnez **FVT-XML-TEST ALL**.
4. Dans Type de fichier, sélectionnez **XML**.
5. Dans Type d'identificateur, sélectionnez **Balise racine** et tapez **MMDoc**.
6. Dans ID Métier source, sélectionnez **Constante** et tapez **000000000**.

7. Dans ID Métier cible, sélectionnez **Constante** et tapez **000000001**.
8. Dans Type de documents source, sélectionnez **Constante** et tapez **ICGCPO**.
9. Dans Version du Type de documents source, sélectionnez **Constante** et tapez **TOUT**.
10. Cliquez sur **Sauvegarder**.

Activation des connexions

Pourquoi et quand exécuter cette tâche

Activez les connexions du partenaire :

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Sélectionnez **Gestionnaire** dans la liste des sources.
3. Sélectionnez **TP1** dans la liste des cibles.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion suivante :

Tableau 46. Connexion de transaction de document XML vers EDI

Source	Cible
Package : Aucun (N/A) Protocole : FVT-XML-TEST (TOUT) Type de document : ICGCPO (TOUT)	Package : N/A (N/A) Protocole : MX12V3R1 (TOUT) Type de document : 850 (TOUT)

6. Cliquez sur **Activer** pour la connexion qui représente l'enveloppe EDI :

Tableau 47. Connexion de l'enveloppe EDI

Source	Cible
Package : N/A (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA(TOUT)	Package : Aucun (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA (TOUT)

Configuration des attributs

Pourquoi et quand exécuter cette tâche

Configurez les attributs Fonctions B2B du partenaire cible (TP1) et du partenaire source (Gestionnaire) :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur **Afficher les détails** en regard de **TPI** pour le sélectionner.
3. Cliquez sur **Fonctions B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Package : N/A**.
5. Cliquez sur l'icône **Edition** en regard de **Protocole : MX12V3R1**.
6. Précisez les attributs suivants :
   a. Sur la ligne Profil d'enveloppe, sélectionnez **EnvProf1** dans la liste.
   b. Sur la ligne Qualificatif EDI, tapez **01**.
   c. Sur la ligne Identificateur EDI, tapez **000000001**.
   d. Sur la ligne Indicateur de syntaxe EDI, tapez **T**.
7. Cliquez sur **Sauvegarder**.
8. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.

9. Cliquez sur Afficher les détails en regard de **Gestionnaire** pour le sélectionner.
10. Cliquez sur **Fonctions B2B**.
11. Cliquez sur l'icône **Développer** en regard de **Package : N/A**.
12. Cliquez sur l'icône **Edition** en regard de **Protocole : MX12V3R1 (TOUT)**.
13. Précisez les attributs suivants :
    a. Sur la ligne Qualificatif EDI, tapez **01**.
    b. Sur la ligne Identificateur EDI, tapez **000000000**.
    c. Sur la ligne Indicateur de syntaxe EDI, tapez **T**.
14. Cliquez sur **Sauvegarder**.

A ce stade, si le partenaire source (le partenaire interne) a envoyé un document XML au partenaire, ce document sera transformé (au niveau du concentrateur) en transaction EDI, puis enveloppé et envoyé à la destination du partenaire.

Exemple ROD vers EDI

Cette section fournit un exemple d'envoi de document ROD par le partenaire interne au concentrateur, qui le transforme en transaction EDI enveloppée dans un EDI et l'envoie à un partenaire.

Dans cet exemple, il est supposé que le spécialiste du mappage Data Interchange Services a créé une mappe qui transforme un document ROD en transaction EDI 850 standard (définie avec le dictionnaire X12V5R1 correspondant à la version 5010 de X12), qui sera traitée par le partenaire. Dans cet exemple, la mappe est nommée S_DT_ROD_TO_EDI.eif.

Le spécialiste de mappage Data Interchange Services peut exporter la mappe de transformation directement dans la base de données WebSphere Partner Gateway. Il peut aussi vous envoyer le fichier, auquel cas vous utiliserez bcgDISImport pour l'importer dans WebSphere Partner Gateway. Cette annexe suit ce second scénario.

Importation de la mappe de transformation

Pourquoi et quand exécuter cette tâche

La présente section décrit la procédure permettant d'importer une mappe de transformation qui transformera une entrée ROD en transaction X12. Lors de l'importation de la mappe de transformation, vous importez également la définition de document associée à la mappe.

Avant de pouvoir importer la mappe de transformation, le spécialiste de mappage Data Interchange Services doit vous l'envoyer. Cette procédure suppose que le fichier S_DT_ROD_TO_EDI.eif est présent sur votre système.

1. Ouvrez une fenêtre de commande.
2. Entrez la commande ou le script suivant :
   - Sous UNIX :

     ```
     <ProductDir>/bin/bcgDISImport.sh <ID_utilisateur_base_de_données>
      <mot de passe> S_DT_ROD_TO_EDI.eif
     ```

   - Sous Windows :

     ```
     <ProductDir>\bin\bcgDISImport.bat <ID utilisateur
     base de données>
      <mot de passe> S_DT_ROD_TO_EDI.eif
     ```

où <*ID_utilisateur_base_de_données*> et <*mot_de_passe*> sont les valeurs que vous avez utilisées lors de l'installation de la base de données, dans le cadre de l'installation de WebSphere Partner Gateway.

Vérification de la mappe de transformation et des définitions de documents

Pourquoi et quand exécuter cette tâche

Pour vérifier que les mappes de transformation et définitions de documents importées sont disponibles sur la console de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Mappes > Mappes de transformation**.

   La mappe S_DT_ROD_TO_EDI s'affiche.
2. Cliquez sur l'icône **Afficher les détails** en regard de la mappe.

   Les définitions de documents auxquelles cette mappe est associée s'affichent :

Tableau 48. Définitions de documents associées à la mappe

Source	Cible
Package : Aucun Protocole : ROD-TO-EDI_DICT (TOUT) Type de document : DTROD-TO-EDI_ROD (TOUT)	Package : N/A Protocole : X12V5R1(TOUT) Type de document : 850 (TOUT)

La mappe S_DT_ROD_TO_EDI a été définie pour transformer un document ROD associé au dictionnaire ROD-TO-EDI_DICT en transaction 850 X12, conforme au standard X12V5R1.

Configuration du récepteur

Pourquoi et quand exécuter cette tâche

Cette section explique comment créer un récepteur de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récepteurs** puis sur **Créer un récepteur**.
2. Dans la zone Nom du récepteur, entrez **RécepteurFichierROD**.
3. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
4. Dans Chemin principal, entrez **/Data/Manager/rodtarget**.
5. Dans la liste des points de configuration, sélectionnez **Preprocess**.
6. Sélectionnez **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** dans la liste des gestionnaires disponibles et cliquez sur **Ajouter** pour le déplacer dans la liste des gestionnaires configurés.
7. Sélectionnez **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** dans la liste des gestionnaires configurés et cliquez sur **Configurer**.
8. Ajoutez les valeurs de la table ci-dessous :

Tableau 49. Attributs gestionnaire du processus de fractionnement ROD

Zone	Valeur
Nom de l'empaquetage d'origine	None
Version du package d'origine	N/D

Tableau 49. Attributs gestionnaire du processus de fractionnement ROD (suite)

Zone	Valeur
Nom du protocole d'origine	ROD-TO-EDI_DICT
Version du protocole d'origine	TOUT
Code du processus d'origine	DTROD-TO-EDI_ROD
Version du processus d'origine	TOUT
METADICTIONARY	ROD-TO-EDI_DICT
METADOCUMENT	DTROD-TO-EDI_ROD
METASYNTAX	rod
ENCODING	ascii
BCG_BATCHDOCS	ON

9. Cliquez sur **Définir valeurs**.
10. Cliquez sur **Sauvegarder**.

Le partenaire interne envoie le document ROD à cette cible.

Création des interactions

Pourquoi et quand exécuter cette tâche

Créez deux interactions : une pour l'enveloppe EDI qui sera envoyée à partir du concentrateur et une pour la transformation du document ROD en EDI.

Créez une interaction dont la source représente la document ROD et la cible le document X12.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez **Package : None** et **Protocole : ROD-TO-EDI_DICT** puis sélectionnez **DTROD-TO-EDI_ROD**.
4. Développez **Package : N/A** et **Protocole : X12V5R1** puis sélectionnez **Type de documents : 850**.
5. Dans la liste Mappe de transformation, sélectionnez **S_DT_ROD_TO_EDI**.
6. Dans la liste des actions, sélectionnez **Validation ROD et validation EDI**.
7. Cliquez sur **Sauvegarder**.

Cette interaction représente la transformation d'un document ROD en transaction X12 standard et par conséquent vous devez sélectionner une mappe de transformation.

Créez une interaction qui représente l'enveloppe EDI.

1. Cliquez sur le **lien Administrateur du concentrateur > Configuration du concentrateur > Définition de document > Gérer des interactions**.
2. Dans l'écran **Gérer les interactions**, cliquez sur le **lien Créer une interaction**.
3. Développez **Package : N/A** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
4. Développez **Package : None** et **Protocole : EDI-X12** puis sélectionnez **Type de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Passe-système**.

Remarque : Aucune transformation ne se produit dans cette interaction. Son but est d'envelopper l'EDI.

6. Cliquez sur **Sauvegarder**.

Création des partenaires

Pourquoi et quand exécuter cette tâche

Dans cet exemple, vous disposez de deux partenaires : le partenaire interne (gestionnaire) et un partenaire externe (TP1).

Créez le profil du partenaire interne :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du partenaire, tapez **Gestionnaire**
4. Pour le Type de partenaire, sélectionnez **Partenaire interne**.
5. Cliquez sur **Nouveau** pour ID entreprise et tapez `000000000` pour ID de forme libre.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour ID entreprise et tapez `01-000000000` pour ID de forme libre.
7. Cliquez sur **Sauvegarder**.

Créez le second partenaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du partenaire, tapez **TP1**
4. Pour le Type de partenaire, sélectionnez **Partenaire externe**.
5. Cliquez sur **Nouveau** pour ID entreprise et tapez `000000001` pour ID de forme libre.

   Remarque : Veillez à sélectionner ID de forme libre et non DUNS.
6. Cliquez sur **Nouveau** pour ID entreprise et tapez `01-000000001` pour ID de forme libre.
7. Cliquez sur **Sauvegarder**.

Création des destinations

Pourquoi et quand exécuter cette tâche

Créez des destinations fichier-répertoire pour les deux partenaires de l'exemple. Créez d'abord une destination pour le gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.
   a. Dans Nom, tapez **DestinationFichierGestionnaire**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.

c. Dans Adresse, tapez : **file://Data/Manager/filedestination**
d. Cliquez sur **Sauvegarder**.

5. Cliquez sur **Liste** pour afficher la liste de toutes les destinations du partenaire interne.
6. Cliquez sur **Afficher les destinations par défaut**.
7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4, à la page 381
8. Cliquez sur **Sauvegarder**.

Ensuite, créez une destination pour le partenaire.

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Sélectionnez l'autre partenaire créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Destinations** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la destination. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **DestinationFichierTP1**.
   b. Dans la liste Transport, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file://Data/TP1/filedestination**
   d. Cliquez sur **Sauvegarder**.
5. Cliquez sur **Liste** pour dresser la liste de toutes les destinations configurées pour le partenaire.
6. Cliquez sur **Afficher les destinations par défaut**.
7. Dans la liste **Production**, sélectionnez la destination créée à l'étape 4.
8. Cliquez sur **Sauvegarder**.

Configuration des fonctions business-to-business

Pourquoi et quand exécuter cette tâche

Activez les fonctions business-to-business des deux partenaires de cet échange. Dans cet exemple, le document ROD est émis par le partenaire interne et sera transmis au partenaire externe (TP1).

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du partenaire source de cet exemple (**Gestionnaire**).
3. Cliquez sur **Fonctions B2B**.
4. Activez deux ensembles de fonctions pour le partenaire source.
   a. Tout d'abord, activez la définition de documents représentant le document ROD :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : ROD-TO-EDI_DICT (TOUT)**.
      4) Développez **Protocole : ROD-TO-EDI_DICT (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : DTROD-TO-EDI_ROD (TOUT)**.

b. Ensuite, activez la définition de documents représentant l'enveloppe EDI :
   1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Package : N/A**, pour l'activer.
   2) Développez **Package : N/A**.
   3) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
   4) Développez **Protocole EDI-X12 (TOUT)**.
   5) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Type de documents : ISA (TOUT)**.

5. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du partenaire cible de cet exemple (**TP1**).
7. Cliquez sur **Fonctions B2B**.
8. Activez deux ensembles de fonctions pour le partenaire cible.
   a. Tout d'abord, activez la définition de documents représentant la transaction EDI 850 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : N/A**, afin de l'activer.
      2) Développez **Package : N/A**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : X12V5R1 (TOUT)**.
      4) Développez **Protocole X12V5R1 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : 850 (TOUT)**.
   b. Ensuite, activez la définition de documents représentant l'enveloppe :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Package : None** pour l'activer.
      2) Développez **Package : None**.
      3) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Type de documents : ISA (TOUT)**.

Création du profil d'enveloppe

Pourquoi et quand exécuter cette tâche

Vous créez ensuite le profil de l'enveloppe qui contiendra la transaction 850 transformée :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > EDI > Profil d'enveloppe**.
2. Cliquez sur **Créer**.
3. Tapez le nom du profil : **EnvProf1**.
4. Dans la liste EDI Standard, sélectionnez **X12**.
5. Le bouton **Général** est sélectionné par défaut. Tapez les valeurs suivantes pour les attributs généraux de l'enveloppe :
   - INTCTLLEN: **9**

- GRPCTLLEN: **9**
- TRXCTLLEN: **9**
- MAXDOCS: **1000**

6. Cliquez sur le bouton **Interchange** et indiquez les valeurs suivantes pour les attributs EDI :
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Cliquez sur **Sauvegarder**.

Activation des connexions

Pourquoi et quand exécuter cette tâche

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions**.
2. Sélectionnez **Gestionnaire** dans la liste des sources.
3. Sélectionnez **TP1** dans la liste des cibles.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion qui représente la transaction du document ROD vers EDI :

Tableau 50. Connexion ROD vers EDI

Source	Cible
Package : N/A (N/A) Protocole : ROD-TO-EDI_DICT (TOUT) Type de document : DTROD-TO-EDI_ROD (TOUT)	Package : Aucun (N/A) Protocole : X12V5R1 (TOUT) Type de document : 850

6. Cliquez sur **Activation** pour la connexion qui représente l'enveloppe :

Tableau 51. Connexion de l'enveloppe

Source	Cible
Package : Aucun (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA (TOUT)	Package : N/A (N/A) Protocole : EDI-X12 (TOUT) Type de document : ISA(TOUT)

Configuration des attributs

Pourquoi et quand exécuter cette tâche

Pour préciser les attributs du profil de l'enveloppe :

1. Cliquez sur **Administrateur de compte > Profils > Partenaire** puis sur **Rechercher**.
2. Sélectionnez **TP1** dans la liste.
3. Cliquez sur **Fonctions B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Package : N/A**.
5. Cliquez sur l'icône **Edition** en regard de **Protocole : X12V5R1**.

6. Précisez les attributs suivants :
   a. Sur la ligne Profil d'enveloppe, sélectionnez **EnvProf1** dans la liste.
   b. Sur la ligne Qualificatif EDI, tapez **01**.
   c. Sur la ligne Identificateur EDI, tapez **000000001**.
   d. Sur la ligne Indicateur de syntaxe EDI, tapez **T**.
7. Cliquez sur **Sauvegarder**.

A ce stade, si le partenaire interne envoie un document ROD au concentrateur, le document sera transformé en transaction 850, qui sera ensuite enveloppée et envoyée à la destination du partenaire.

Chapitre 21. Informations complémentaires sur RosettaNet

La présente annexe apporte des informations complémentaires sur la prise en charge RosettaNet. Il contient les rubriques suivantes :

- «Désactivation des PIP»
- « Notification d'échec»
- «Création de packages de définition de documents PIP», à la page 389
- «Packages de définition de documents PIP», à la page 401

Désactivation des PIP

Pourquoi et quand exécuter cette tâche

Une fois qu'un package PIP a été téléchargé dans WebSphere Partner Gateway, il est impossible de le supprimer. Vous pouvez cependant le désactiver afin qu'il ne soit plus utilisé.

Pour désactiver un PIP pour toutes les communications avec des partenaires, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition de documents**.
2. Développez les définitions de document pour connaître le type de document du PIP que vous souhaitez désactiver.
3. Dans la colonne Etat du package, cliquez sur **Activé**. La colonne Etat affiche maintenant **Désactivé** et WebSphere Partner Gateway ne peut pas utiliser la définition de document pour le PIP.

Pour désactiver une communication PIP avec un partenaire donné, désactivez la connexion au partenaire défini pour le processus PIP.

Notification d'échec

0A1 - Processus PIP

Si un incident se produit au cours du traitement d'un message PIP, WebSphere Partner Gateway utilise le processus PIP 0A1 pour signaler l'incident au partenaire ou au système dorsal ayant envoyé le message. Par exemple, supposons qu'un système dorsal lance un processus PIP 3A4. WebSphere Partner Gateway traite le message RNSC et envoie un message RosettaNet à un partenaire. WebSphere Partner Gateway attend la réponse au message RosettaNet jusqu'à ce que la limite du délai d'attente soit atteinte. A ce stade, WebSphere Partner Gateway crée un processus PIP 0A1 et l'envoie au partenaire. Le processus PIP 0A1 identifie la condition d'exception afin de permettre au partenaire de compenser l'échec du processus PIP 3A4.

Pour assurer la notification d'incident, téléchargez un package 0A1 et servez-vous en pour créer une connexion PIP au partenaire.

Mise à jour des informations de contact

Pour modifier les informations de contact avec le processus PIP 0A1, vous devez éditer le fichier BCG.Properties, situé dans le répertoire <*ProductDir*>/router/lib/config.

Ces zones complètent les informations de contact dans le processus PIP 0A1. Le numéro de télécopie est facultatif (sa valeur peut rester vide), mais les autres zones sont obligatoires.

- **bcg.0A1.fromContactName**
- **bcg.0A1.fromEMailAddr**
- **bcg.0A1.fromPhoneNbr**
- **bcg.0A1.fromFaxNbr**

Les numéros de téléphone sont limités à 30 octets. Les autres zones sont de longueur illimitée. Une fois les valeurs modifiées, le gestionnaire de documents doit être redémarré.

Edition des valeurs d'attribut RosettaNet

Pourquoi et quand exécuter cette tâche

Pour la prise en charge de RosettaNet, une définition de document de type action possède un jeu d'attributs particulier. Ces attributs fournissent des informations servant à valider le message PIP, à définir les rôles et services utilisés dans le processus PIP et à définir la réponse à l'action. Les packages PIP fournis par WebSphere Partner Gateway définissent automatiquement des valeurs pour ces attributs, que vous n'avez généralement pas à modifier.

Pour modifier les attributs RosettaNet d'une définition de document d'action, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du document**.
2. Cliquez sur les icônes **Développer** pour développer un noeud jusqu'au niveau de définition de document approprié, ou sélectionnez **Tout** pour développer l'intégralité de l'arborescence.
3. La colonne Actions de chaque action contient une icône **Editer les valeurs d'attribut RosettaNet**. Cliquez sur cette icône pour éditer les attributs RosettaNet de l'action. La console de communauté affiche une liste des attributs définis sous Attributs RosettaNet.
4. Complétez les paramètres suivants sous Attributs RosettaNet (ces attributs sont définis automatiquement lorsqu'un processus PIP est téléchargé dans le système).

Tableau 52. attributs RosettaNet

Attribut RosettaNet	Description
Nom de la DTD	Identifie le nom de l'action du processus PIP dans la DTD fournie par RosettaNet
Du service	Contient le nom du service de composant réseau du partenaire ou système dorsal qui envoie le message
Vers le service	Contient le nom du service de composant réseau du partenaire ou système dorsal qui reçoit le message

Tableau 52. attributs RosettaNet (suite)

Attribut RosettaNet	Description
A partir du rôle	Contient le nom de rôle du partenaire ou système dorsal qui envoie le message
Vers le rôle	Contient le nom de rôle du partenaire ou système dorsal qui reçoit le message
Balise racine	Contient le nom de l'élément racine dans le document XML du message PIP
Réponse à partir du nom d'action	Identifie l'action suivante à effectuer dans le processus PIP

Remarque : Si la console affiche le message `Aucun attribut n'a été trouvé`, c'est que les attributs n'ont pas été définis.

5. Si la console affiche ce message pour une définition de niveau inférieur, il se peut que la définition fonctionne quand même, car elle hérite des attributs de la définition de niveau supérieur. Les attributs ajoutés et leurs valeurs remplacent les attributs hérités, ce qui modifie la fonctionnalité de la définition de document.
6. Cliquez sur **Sauvegarder**.

Création de packages de définition de documents PIP

Pourquoi et quand exécuter cette tâche

RosettaNet ajoutant des processus PIP de temps en temps, il peut s'avérer nécessaire de créer vos propres packages PIP pour prendre en charge ces nouveaux processus ou les mises à niveau des processus existants. Sauf indication contraire, les procédures de cette section indiquent comment créer le package de définition de documents PIP pour PIP 5C4 V01.03.00. WebSphere Partner Gateway fournit un package de définition de documents PIP pour le PIP 5C4 V01.02.00. Par conséquent, les procédures décrivent en réalité la procédure de mise à niveau. Cependant, la création d'un package de définition de documents PIP est similaire et les procédures identifient les éventuelles étapes supplémentaires.

Avant de commencer, téléchargez les spécifications PIP à partir de www.rosettanet.org pour la nouvelle version et, si vous procédez à une mise à niveau, l'ancienne version. Par exemple, si vous effectuez la mise à niveau décrite dans les procédures, téléchargez 5C4_DistributeRegistrationStatus_V01_03_00.zip et 5C4_DistributeRegistrationStatus_V01_02_00.zip. La spécification comprend les types de fichier suivants :

- Instructions pour les messages XML RosettaNet - fichiers HTML tels que 5C4_MG_V01_03_00_RegistrationStatusNotification.htm qui définissent la cardinalité, le vocabulaire, la structure et les valeurs et types de valeurs admis pour les éléments de données du processus PIP.
- Schéma de message XML RosettaNet - fichiers DTD tels que 5C4_MS_V01_03_RegistrationStatusNotification.dtd qui définissent l'ordre ou la séquence, les noms d'élément, la composition et les attributs du processus PIP.
- Spécification PIP - fichier DOC tel que 5C4_Spec_V01_03_00.doc qui fournit les commandes de performances métier du processus PIP.
- Notes d'édition PIP - fichier DOC tel que 5C4_V01_03_00_ReleaseNotes.doc qui décrit la différence entre cette version et la précédente.

La création ou la mise à niveau d'un package de définition de documents PIP comprend les procédures suivantes :

- Création des fichiers XSD
- Création du fichier XML
- Création des packages

Création de fichiers XSD

Pourquoi et quand exécuter cette tâche

Un package de définition de documents PIP contient des fichiers de schéma XML qui définissent les formats de message et les valeurs acceptables pour les éléments. La procédure suivante indique comment créer ces fichiers à partir du contenu du fichier de spécification PIP.

Vous créez au moins un fichier XSD pour chaque fichier DTD dans le fichier de spécification PIP. Dans l'exemple de mise à niveau vers PIP 5C4 V01.03.00, comme le format des messages a changé, la procédure décrit la création du fichier BCG_5C4RegistrationStatusNotification_V01.03.xsd, à titre d'exemple. Pour plus d'informations sur les fichiers XSD, voir «A propos de la validation», à la page 399.

Pour créer les fichiers XSD pour le package de définition de documents PIP, procédez comme suit :

1. Importez ou chargez le fichier DTD dans un éditeur XML tel que WebSphere Studio Application Developer. Par exemple, chargez le fichier 5C4_MS_V01_03_RegistrationStatusNotification.dtd.
2. A l'aide de l'éditeur XML, convertissez la DTD en schéma XML. La procédure suivante indique comment le faire en utilisant Application Developer :
   a. Dans la sous-fenêtre de navigation de la perspective XML, ouvrez le projet contenant le fichier DTD importé.
   b. Cliquez avec le bouton droit sur le fichier DTD et sélectionnez **Generate > XML Schema**.
   c. Dans le panneau Generate, tapez ou sélectionnez l'emplacement où vous souhaitez sauvegarder le nouveau fichier XSD. Dans la zone File name, entrez le nom du nouveau fichier XSD. Dans le cas de cet exemple, vous devez entrer un nom du type BCG_5C4RegistrationStatusNotification_V01.03.xsd.
   d. Cliquez sur **Terminer**.
3. Pour tenir compte des éléments qui possèdent plusieurs valeurs de cardinalité dans les recommandations XML RosettaNet XML, ajoutez des spécifications au nouveau fichier XSD. Les recommandations représentent les éléments du message sous la forme d'une arborescence, en affichant la cardinalité de chaque élément à gauche de celui-ci.

   En général, les éléments dans les recommandations correspondent aux définitions des éléments dans le fichier DTD. Cependant, les recommandations peuvent contenir certains éléments qui portent les mêmes noms mais ont des cardinalités différentes. Comme la DTD ne peut pas fournir la cardinalité dans ce cas, vous devez modifier la XSD. Par exemple, le fichier de recommandations 5C4_MG_V01_03_00_RegistrationStatusNotification.htm comporte une définition de ContactInformation en ligne 15 qui contient cinq éléments enfants dotés des cardinalités suivantes :

   1 contactName

   0..1 EmailAddress

0..1 facsimileNumber

0..1 PhysicalLocation

0..1 telephoneNumber

La définition de ContactInformation à la ligne 150 comporte quatre éléments enfants dotés des cardinalités suivantes :

1 contactName

1 EmailAddress

0..1 facsimileNumber

1 telephoneNumber

Dans le fichier XSD, cependant, chaque enfant de ContactInformation possède une cardinalité conforme aux deux définitions :

```
<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 vous mettez à jour le package de définition de documents PIP basé sur une autre version du package et que vous souhaitiez réutiliser une définition de l'autre version, procédez comme suit pour chacune de ces définitions :

a. Supprimez la définition de l'élément. Par exemple, supprimez l'élément ContactInformation.

b. Ouvrez le package de définition de documents PIP de la version remplacée. Par exemple, ouvrez le fichier BCG_Package_RNIFV02.00_5C4V01.02.zip.

c. Recherchez la définition que vous souhaitez réutiliser. Par exemple, la définition ContactInformation_type7 dans le fichier BCG_ContactInformation_Types.xsd correspond à la définition qu'il vous faut pour la ligne 15 des recommandations.

```
<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. Dans le nouveau fichier XSD que vous créez pour le package de définition de documents PIP mis à jour, créez une référence au fichier XSD contenant la définition que vous souhaitez réutiliser. Par exemple, créez une référence à BCG_ContactInformation_Types.xsd dans le fichier BCG_5C4RegistrationStatusNotification_V01.03.xsd, comme suit :

```
<xsd:include schemaLocation="BCG_ContactInformation_Types.xsd"/>
```

e. Dans le nouveau fichier XSD, supprimez l'attribut ref des éléments faisant référence à l'élément que vous avez supprimé. Ajoutez un attribut type faisant référence à la définition que vous réutilisez. Par exemple, dans

l'élément productProviderFieldApplicationEngineer, supprimez *ref="Contact Information"* et ajoutez l'attribut suivant :

```
name="ContactInformation"
 type="ContactInformation_type7"
```

Si vous créez un package de définition de documents PIP, ou si vous en mettez un à niveau mais que la définition dont vous avez besoin n'existe pas dans l'autre version, procédez comme suit pour chaque instance de l'élément que vous avez trouvée dans les recommandations :

a. Supprimez la définition de l'élément. Par exemple, supprimez l'élément ContactInformation.

b. Créez la définition de remplacement. Par exemple, créez la définition ContactInformation_localType1 afin qu'elle corresponde à la définition de la ligne 15 des recommandations.

```
<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. Pour les éléments faisant référence à l'élément que vous avez supprimé, supprimez l'attribut ref et ajoutez un attribut type faisant référence au type complexe approprié défini à l'étape précédente. Par exemple, dans l'élément productProviderFieldApplicationEngineer, supprimez *ref="Contact Information"* et ajoutez l'attribut suivant :

```
name="ContactInformation"
type="ContactInformation_localType1"
```

La figure 35 affiche l'élément productProviderFieldApplicationEngineer avant modification.

```
<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="ContactInformation"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figure 35. Elément productProviderFieldApplicationEngineer avant modification

La figure 36 affiche l'élément productProviderFieldApplicationEngineer après modification.

```
<xsd:element name="productProviderFieldApplicationEngineer">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="ContactInformation"
          type="ContactInformation_localType1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figure 36. Elément productProviderFieldApplicationEngineer après modification

4. Spécifiez les valeurs d'énumération des éléments qui ne peuvent avoir que des valeurs données. Les recommandations définissent les valeurs d'énumération dans les tables de la section relative aux recommandations.

   Par exemple, dans un message PIP 5C4 V01.03.00, l'élément GlobalRegistrationComplexityLevelCode ne peut prendre que les valeurs Above average, Average, Maximum, Minimum, None et Some.

   Si vous mettez à jour le package de définition de documents PIP sur la base d'une autre version du package et si vous souhaitez réutiliser un jeu de valeurs d'énumération provenant de l'autre version, procédez comme suit pour chaque ensemble :

   a. Supprimez la définition de l'élément. Par exemple, supprimez l'élément GlobalRegistrationComplexityLevelCode :
   b. Ouvrez le package de définition de documents PIP de la version remplacée. Par exemple, ouvrez le fichier BCG_Package_RNIFV02.00_5C4V01.02.zip.
   c. Recherchez la définition contenant les valeurs d'énumération que vous souhaitez réutiliser. Par exemple, la définition _GlobalRegistrationComplexityLevelCode dans le fichier BCG_GlobalRegistrationComplexityLevelCode.xsd contient les définitions de valeur d'énumération définies par le table des instances de l'entité.

      ```
      <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. Dans le nouveau fichier XSD que vous créez pour le package de définition de documents PIP mis à jour, créez une référence au fichier XSD contenant la définition que vous souhaitez réutiliser. Par exemple, créez une référence à BCG_GlobalRegistrationComplexityLevelCode.xsd dans le fichier BCG_5C4RegistrationStatusNotification_V01.03.xsd, comme suit :

      ```
      <xsd:include schemaLocation=
          "BCG_GlobalRegistrationComplexityLevelCode_Types.xsd" />
      ```

   e. Dans le nouveau fichier XSD, supprimez l'attribut ref des éléments faisant référence à l'élément que vous avez supprimé. Ajoutez un attribut type faisant référence à la définition que vous réutilisez. Par exemple, dans l'élément DesignAssemblyInformation, supprimez *ref*=”GlobalRegistrationComplexityLevelCode” et ajoutez les informations suivantes :

      ```
      name="GlobalRegistrationComplexityLevelCode"
      type="_GlobalRegistrationComplexityLevelCode"
      ```

   Si vous créez un package de définition de documents PIP, ou si vous en mettez un à niveau mais que les définitions de valeur d'énumération dont vous avez besoin n'existent pas dans l'autre version, procédez comme suit pour tout élément comportant des valeurs énumérées dans les recommandations :

   a. Supprimez la définition de l'élément. Par exemple, supprimez l'élément GlobalRegistrationComplexityLevelCode.
   b. Créez la définition de remplacement. Par exemple, créez la définition GlobalRegistrationComplexityLevelCode_localType et incluez les définitions de valeur d'énumération décrites par le tableau.

```
<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. Pour les éléments faisant référence à l'élément que vous avez supprimé, supprimez l'attribut ref et ajoutez un attribut type faisant référence au type complexe approprié défini à l'étape précédente. Par exemple, supprimez *ref="GlobalRegistrationComplexityLevelCode"* et ajoutez les informations suivantes :

```
name="GlobalRegistrationComplexityLevelCode"
type="GlobalRegistrationComplexityLevelCode_localType"
```

La figure 37 affiche l'élément DesignAssemblyInformation avant modification.

```
<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>
```

Figure 37. Elément DesignAssemblyInformation avant modification

La figure 38, à la page 395 affiche l'élément DesignAssemblyInformation avant modification.

```
<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>
```

Figure 38. Elément DesignAssemblyInformation après modification

5. Définissez le type de données, la longueur minimale, la longueur maximale et la représentation des entités de données. Les instructions pour les messages XML RosettaNet fournissent ces informations dans la table des entités de données métier fondamentales.

   Si vous mettez à jour le package de définition de documents PIP sur la base d'une autre version du package et si vous souhaitez réutiliser une définition d'entité de données provenant de l'autre version, procédez comme suit pour chaque ensemble :

   a. Supprimez la définition de l'élément d'entité de données. Par exemple, supprimez l'élément DateStamp.

   b. Ouvrez le package de définition de documents PIP de la version remplacée. Par exemple, ouvrez le fichier BCG_Package_RNIFV02.00_5C4V01.02.zip.

   c. Recherchez la définition que vous souhaitez réutiliser. Par exemple, la définition _common_DateStamp_R dans le fichier BCG_common.xsd contient la définition suivante, qui est conforme aux informations données dans les recommandations.

      ```
      <xsd:simpleType name="_common_DateStamp_R">
        <xsd:restriction base="xsd:string">
          <xsd:pattern value="[0-9]{8}Z" />
        </xsd:restriction>
      </xsd:simpleType>
      ```

   d. Dans le nouveau fichier XSD que vous créez pour le package de définition de documents PIP mis à jour, créez une référence au fichier XSD contenant la définition que vous souhaitez réutiliser. Par exemple, créez une référence à BCG_common.xsd dans le fichier BCG_5C4RegistrationStatusNotification_V01.03.xsd, comme suit :

      ```
      <xsd:include schemaLocation="BCG_common.xsd" />
      ```

   e. Dans le nouveau fichier XSD, supprimez l'attribut ref des éléments faisant référence à l'élément que vous avez supprimé. Ajoutez un attribut type faisant référence à la définition que vous réutilisez. Par exemple, dans l'élément DesignAssemblyInformation, supprimez *ref*=″DateStamp″ et ajoutez l'attribut suivant :

      ```
      name="DateStamp" type="_common_DateStamp_R"
      ```

Si vous créez un package de définition de documents PIP, ou si vous en mettez un à niveau mais que la définition d'entité de données dont vous avez besoin n'existe pas dans l'autre version, procédez comme suit pour chaque élément d'entité de données :

a. Supprimez la définition de l'élément. Par exemple, supprimez l'élément DateStamp.

b. Créez la définition de remplacement. Par exemple, utilisez le type de données, la longueur minimale, la longueur maximale et la représentation pour créer la définition DateStamp_localType.

```
<xsd:simpleType name="DateStamp_localType">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{8}Z" />
  </xsd:restriction>
</xsd:simpleType>
```

c. Pour les éléments faisant référence à l'élément que vous avez supprimé, supprimez l'attribut ref et ajoutez un attribut type faisant référence au type complexe approprié défini à l'étape précédente. Par exemple, supprimez *ref="DateStamp"* et ajoutez les informations suivantes :

```
name="DateStamp" type="DateStamp_localType"
```

La figure 39 affiche l'élément beginDate avant modification.

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element ref="DateStamp"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figure 39. Elément beginDate avant modification

La figure 40 affiche l'élément beginDate après modification.

```
<xsd:element name="beginDate">
  <xsd:complexType">
    <xsd:sequence>
      <xsd:element name="DateStamp" type="DateStamp_localType"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Figure 40. Elément beginDate après modification

Création du fichier XML

Pourquoi et quand exécuter cette tâche

Après avoir créé les fichiers XSD pour votre package de définition de documents PIP, vous pouvez créer le fichier XML du package RNIF et le fichier XML du package Backend Integration. Par exemple, ces packages s'appellent respectivement BCG_Package_RNIFV02.00_5C4V01.03.zip et BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.03.zip. La procédure suivante décrit la création du fichier XML pour le package RNIF :

1. Extrayez le fichier XML d'un fichier de package de définition de documents PIP RNIF. Si vous effectuez une mise à niveau, extrayez le fichier de la version précédente du package (par exemple, BCG_Package_RNIFV02.00_5C4V01.02.zip). Si vous créez un nouveau package, extrayez le fichier à partir d'un package de définition de documents PIP semblable à celui que vous créez. Par exemple, si vous créez un package pour

prendre en charge un processus PIP à deux actions, copiez le fichier XML à partir d'un autre package PIP à deux actions.

2. Copiez le fichier et renommez-le de façon appropriée, par exemple RNIFV02.00_5C4V01.03.xml.
3. Dans le nouveau fichier, mettez à jour les éléments qui contiennent des informations sur le processus PIP. Par exemple, le tableau suivant répertorie les informations nécessaires pour la mise à jour dans l'exemple de processus PIP 5C4. Notez que ces informations peuvent figurer plusieurs fois dans le fichier. Veillez à mettre à jour toutes les instances.

Tableau 53. Informations de mise à jour PIP 5C4

Informations à modifier	**Ancienne valeur**	**Nouvelle valeur**
ID du processus PIP	5C4	5C4
Version du processus PIP	V01.02	V01.03
Nom du fichier DTD du message de demande sans extension	5C4_MS_V01_02_ RegistrationStatusNotification	5C4_MS_V01_03_ RegistrationStatusNotification
Nom du fichier DTD du message de confirmation sans extension (pour processus PIP à deux actions seulement)	N/D	N/D
Nom du fichier XSD du message de demande sans extension	BCG_5C4RegistrationStatus Notification_V01.02	BCG_5C4RegistrationStatus Notification_V01.03
Nom du fichier XSD du message de confirmation sans extension (pour processus PIP à deux actions seulement)	N/D	N/D
Nom de l'élément racine dans le fichier XSD du message de demande	Pip5C4RegistrationStatus Notification	Pip5C4RegistrationStatus Notification
Nom de l'élément racine dans le fichier XSD du message de confirmation (processus PIP à deux actions seulement)	N/D	N/D

4. Ouvrez le document de spécification PIP et servez-vous en pour mettre à jour les informations répertoriées dans le tableau suivant. Si vous effectuez une mise à jour, comparez les spécifications des différentes versions parce qu'il n'est peut-être pas nécessaire de mettre à jour ces valeurs.

Tableau 54. Informations de mise à jour PIP 5C4 à partir de la spécification PIP

Informations à mettre à jour	Description	Valeur dans le package 5C4
Nom de l'activité	Spécifié au tableau 3-2	Distribute Registration Status
Nom de rôle de l'initiateur	Spécifié au tableau 3-1	Product Provider
Nom de rôle du répondeur	Spécifié au tableau 3-1	Demand Creator
Nom de l'action de demande	Spécifié au tableau 4-2	Registration Status Notification
Nom de l'action de confirmation	Spécifié au tableau 4-2 (pour processus PIP à deux actions seulement)	N/D

5. Mettez à jour les valeurs d'attribut du package. Si vous effectuez une mise à jour, comparez les spécifications des différentes versions parce qu'il n'est peut-être pas nécessaire de mettre à jour ces valeurs.

   Remarque : Si vous créez un package Backend Integration, passez directement à l'étape 6, à la page 399.

Tableau 55. Mises à jour d'attributs PIP 5C4

Informations à mettre à jour	Description	Valeur dans le package 5C4	Chemin d'accès à l'élément dans le fichier XML
NonRepudiation Required	Spécifié au tableau 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOf Receipt	Spécifié au tableau 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
DigitalSignature Required	Spécifié au tableau 5-1	O	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
TimeToAcknowledge	Spécifié au tableau 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is TimeToAcknowledge) ns1:AttributeValue ATTRVALUE
TimeToPerform	Spécifié au tableau 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is TimeToPerform) ns1:AttributeValue ATTRVALUE

Tableau 55. Mises à jour d'attributs PIP 5C4 (suite)

Informations à mettre à jour	Description	Valeur dans le package 5C4	Chemin d'accès à l'élément dans le fichier XML
RetryCount	Spécifié au tableau 3-3	3	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (Its ATTRIBUTEKEY is RetryCount) ns1:AttributeValue ATTRVALUE

6. Modifiez les éléments ns1:Package/ns1:Protocol/GuidelineMap pour supprimer les fichiers XSD inutilisés et ajouter les fichiers XSD que vous avez créés ou référencés.

Pour créer le package Backend Integration, répétez les étapes 1, à la page 396 à 6, avec les différences suivantes :

- A l'étape 1, à la page 396, extrayez le fichier XML à partir du package Backend Integration (par exemple BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip).
- N'effectuez pas l'étape 5, à la page 398.

Après avoir créé les fichiers XML et XSD, vous pouvez créer les packages de flux de documentation PIP.

Création du package

Pourquoi et quand exécuter cette tâche

Pour créer un package RNIF, procédez comme suit :

1. Créez un répertoire GuidelineMaps et copiez-y les fichiers XSD du package.
2. Créez un répertoire Packages et copiez-y le fichier XML RNIF.
3. Allez dans le répertoire parent et créez un package de définition de documents PIP (fichier ZIP) contenant les répertoires GuidelineMaps et Packages. Vous devez conserver l'arborescence des répertoires dans le fichier ZIP.

Pour créer le package Backend Integration, suivez les étapes 1 à 3, mais utilisez le fichier XML Backend Integration au lieu du fichier RNIF.

Après avoir créé le package PIP, vous pouvez le télécharger en suivant la procédure de la section «Packages RNIF et PIP», à la page 119.

A propos de la validation

WebSphere Partner Gateway valide le contenu de service d'un message RosettaNet à l'aide de mappes de validation. Ces mappes définissent la structure d'un message valide, ainsi que la cardinalité, le format et les valeurs valides (énumération) des éléments contenus dans le message. Dans chaque package de définition de documents PIP, WebSphere Partner Gateway fournit les mappes de validation sous forme de fichiers XSD dans le répertoire GuidelineMaps.

Etant donné que RosettaNet spécifie le format d'un message PIP, il ne sera en principe pas nécessaire de personnaliser les mappes de validation. Dans le cas contraire, voir «Création de packages de définition de documents PIP», à la page 389 pour plus d'informations sur les étapes nécessaires pour mettre à niveau les fichiers XSD servant à valider les messages et sur la création d'un package de définition de documents PIP.

Cardinalité

La cardinalité détermine combien de fois un élément particulier peut ou doit figurer dans un message. Dans les mappes de validation, les attributs minOccurs et maxOccurs déterminent la cardinalité de l'attribut, comme l'illustre l'exemple suivant tiré de BCG_5C4RegistrationStatusNotification_V01.02.xsd :

```
<xsd:element name="GeographicRegion" type="GeographicRegionType"
    minOccurs="0"/>
```

Si WebSphere Partner Gateway n'a pas besoin de vérifier la cardinalité d'un élément, les valeurs des attributs minOccurs et maxOccurs de cet élément dans la mappe de validation sont "0" et "unbounded", comme indiqué dans l'exemple suivant :

```
<xsd:element name="DesignRegistrationIdentification"
    type="DesignRegistrationIdentificationType2"
    minOccurs="0" maxOccurs="unbounded"/>
```

Format

Le format détermine la disposition ou l'organisation des données pour le type d'un élément. Dans les mappes de validation, le type comporte une ou plusieurs restrictions, comme indiqué dans les exemples suivants :

Exemple 1

```
<xsd:simpleType name="_common_LineNumber_R">
  <xsd:restriction base="xsd:string">
    <xsd:minLength value="1" />
    <xsd:maxLength value="6" />
  </xsd:restriction>
</xsd:simpleType>
```

Tous les éléments de type _common_LineNumber_R dans un message doivent être des chaînes de 1 à 6 caractères.

Exemple 2

```
<xsd:simpleType name="_GlobalLocationIdentifier">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[0-9]{9}.{1,4}" />
  </xsd:restriction>
</xsd:simpleType>
```

Tous les éléments de type _GlobalLocationIdentifier dans un message doivent être des chaînes de neuf caractères de données numériques, suivis de un à quatre caractères de données alphanumériques. La longueur est donc de 10 à 13 caractères.

Exemple 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>
```

Tous les éléments de type _DayofMonth d'un message doivent être des entiers positifs (PositiveInteger), comporter un ou deux caractères et faire partie de l'intervalle 1 à 31, bornes incluses.

Enumération

L'énumération détermine les valeurs valides pour un élément. Dans les mappes de validation, le type de l'élément comporte une ou plusieurs restrictions d'énumération, comme indiqué dans l'exemple suivant :

```
<xsd:simpleType name="_local_GlobalDesignRegistrationNotificationCode">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Initial" />
    <xsd:enumeration value="Update" />
  </xsd:restriction>
</xsd:simpleType>
```

Les éléments de type _local_GlobalDesignRegistrationNotificationCode d'un message ne peuvent prendre que les valeurs "Initial" ou "Update".

Packages de définition de documents PIP

Les sections suivantes décrivent les Packages de définition de documents PIP fournis par WebSphere Partner Gateway pour chaque PIP. Chaque package contient un fichier XML inclus dans un répertoire Packages et plusieurs fichiers XSD dans un répertoire GuidelineMaps, qui sont communs à tous les packages de définition de documents PIP du processus PIP.

0A1 Notification of Failure V1.0

La section suivante présente le contenu du PIP 0A1 Notification of Failure V1.0.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 0A1 Notification of Failure V1.0. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 56. Fichiers ZIP et XML du PIP 0A1 Notification of Failure V1.0

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 0A1 Notification of Failure 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 Notification of Failure V02.00

La section suivante présente le contenu du PIP 0A1 Notification of Failure V02.00.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 0A1 Notification of Failure V02.00. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 57. Fichiers ZIP et XML du PIP 0A1 Notification of Failure V02.00

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 0A1 Notification of Failure 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 Distribute New Product Information

La section suivante présente le contenu du PIP 2A1 Distribute New Product Information.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 2A1 Distribute New Product Information. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 58. Fichiers ZIP et XML de 2A1 Distribute New Product Information

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 2A1 Distribute New Product Information :

- 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 Distribute Product Master

La section suivante présente le contenu du PIP 2A12 Distribute Product Master.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 2A12 Distribute Product Master. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 59. Fichiers ZIP et XML de 2A12 Distribute Product Master

Nom du fichier ZIP	Nom du fichier XML
BCG_Package_RNIF1.1_2A12V01.03.zip	BCG_RNIF1.1_2A12V01.03.xml

Tableau 59. Fichiers ZIP et XML de 2A12 Distribute Product Master (suite)

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 2A12 Distribute Product Master :

- 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 Request Quote

La section suivante présente le contenu du PIP 3A1 Request Quote.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A1 Request Quote. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 60. Fichiers ZIP et XML du PIP 3A1 Request Quote

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A1 Request Quote :

- 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 Request Price and Availability

La section suivante présente le contenu du PIP 3A2 Request Price and Availability.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A2 Request Price and Availability. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 61. Fichiers ZIP et XML de 3A2 Request Price and Availability

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A2 Request Price and Availability :

- 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 Request Purchase Order V02.00

La section suivante présente le contenu du PIP 3A4 Request Purchase OrderV02.00.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A4 Request Purchase Order. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 62. Fichiers ZIP et XML du PIP 3A4 Request Purchase Order

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A4 Request Purchase Order :

- 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 Request Purchase Order V02.02

La section suivante présente le contenu du PIP 3A4 Request Purchase OrderV02.02.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A4 Request Purchase Order. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 63. Fichiers ZIP et XML du PIP 3A4 Request Purchase Order

Nom du fichier ZIP	Nom du fichier XML
BCG_Package_RNIF1.1_3A4V02.02.zip	BCG_RNIF1.1_3A4V02.02.xml

Tableau 63. Fichiers ZIP et XML du PIP 3A4 Request Purchase Order (suite)

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A4 Request Purchase Order :

- 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 Query Order Status

La section suivante présente le contenu du PIP 3A5 Query Order Status.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A5 Query Order Status. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 64. Fichiers ZIP et XML du PIP 3A5 Query Order Status

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A5 Query Order Status :

- 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 Distribute Order Status

La section suivante présente le contenu du PIP 3A6 Distribute Order Status.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A6 Distribute Order Status. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 65. Fichiers ZIP et XML du PIP 3A6 Distribute Order Status

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A6 Distribute Order Status :

- 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 Notify of Purchase Order Update

La section suivante présente le contenu du PIP 3A7 Notify of Purchase Order Update.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A7 Notify Purchase Order Update. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 66. Fichiers ZIP et XML de 3A7 Notify of Purchase Order Update

Nom du fichier ZIP	Nom du fichier 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
BCG_Package_RNSC1.0_RNIFV02.00_3A7V02.02.zip	BCG_RNSC1.0_RNIFV02.00_3A7V02.02.xml

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A7 Notify of Purchase Order Update :

- 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 Request Purchase Order Change V01.02

La section suivante présente le contenu du PIP 3A8 Request Purchase Order Change V01.02.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A8 Request Purchase Order Change. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 67. Fichiers ZIP et XML du PIP 3A8 Request Purchase Order

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A8 Request Purchase Order Change :

- 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 Request Purchase Order Change V01.03

La section suivante présente le contenu du PIP 3A8 Request Purchase Order Change V01.03.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A8 Request Purchase Order Change. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 68. Fichiers ZIP et XML du PIP 3A8 Request Purchase Order

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A8 Request Purchase Order Change :

- 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 Request Purchase Order Cancellation

La section suivante présente le contenu du PIP 3A9 Request Purchase Order Cancellation.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3A9 Request Purchase Order Cancellation. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 69. Fichiers ZIP et XML du PIP 3A9 Request Purchase Order Cancellation

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3A9 Request Purchase Order Cancellation :

- 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 Notify of Advance Shipment

La section suivante présente le contenu du PIP 3B2 Notify of Advance Shipment.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3B2 Notify of Advance Shipment. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 70. Fichiers ZIP et XML de 3B2 Notify of Advance Shipment

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3B2 Notify of Advance Shipment :

- 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 Distribute Shipment Status

La section suivante présente le contenu du PIP 3B3 Distribute Shipment Status.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3B3 Distribute Shipment Status. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 71. Fichiers ZIP et XML du PIP 3B3 Distribute Shipment Status

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3B3 Distribute Shipment Status :

- 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 Notify of Shipping Order

La section suivante présente le contenu du PIP 3B11 Notify of Shipping Order.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3B11 Notify Shipping Order. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 72. Fichiers ZIP et XML de 3B11 Notify of Shipping Order

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3B11 Notify of Shipping Order :

- 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 Request Shipping Order

La section suivante présente le contenu du PIP 3B12 Request Shipping Order.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3B12 Request Shipping Order. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 73. Fichiers ZIP et XML du PIP 3B12 Request Shipping Order

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3B12 Request Shipping Order :

- 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 Notify of Shipping Order Confirmation

La section suivante présente le contenu du PIP 3B13 Notify of Shipping Order Confirmation.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3B13 Notify Shipping Order Confirmation. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 74. Fichiers ZIP et XML de 3B13 Notify of Shipping Order Confirmation

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3B13 Notify of Shipping Order Confirmation :

- 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 Request Shipping Order Cancellation

La section suivante présente le contenu du PIP 3B14 Request Shipping Order Cancellation.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3B14 Request Shipping Order Cancellation. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 75. Fichiers ZIP et XML du PIP 3B14 Request Shipping Order Cancellation

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3B14 Request Shipping Order Cancellation :

- 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 Notify of Shipping Documentation

La section suivante présente le contenu du PIP 3B18 Notify of Shipping Documentation.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3B18 Notify Shipping Documentation. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 76. Fichiers ZIP et XML de 3B18 Notify of Shipping Documentation

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3B18 Notify of Shipping Documentation :

- 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 Return Product

La section suivante présente le contenu du PIP 3C1 Return Product.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3C1 Return Product. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 77. Fichiers ZIP et XML de 3C1 Return Product

Nom du fichier ZIP	Nom du fichier 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

Tableau 77. Fichiers ZIP et XML de 3C1 Return Product (suite)

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3C1 Return Product :

- 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 Notify of Invoice

La section suivante présente le contenu du PIP 3C3 Notify of Invoice.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3C3 Notify of Invoice. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 78. Fichiers ZIP et XML de 3C3 Notify of Invoice

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3C3 Notify of Invoice :

- 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 Notify of Invoice Reject

La section suivante présente le contenu du PIP 3C4 Notify of Invoice Reject.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3C4 Notify of Invoice Reject. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 79. Fichiers ZIP et XML de 3C4 Notify of Invoice Reject

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3C4 Notify of Invoice :

- 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 Notify of Remittance Advice

La section suivante présente le contenu du PIP 3C6 Notify of Remittance Advice.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3C6 Notify of Remittance Advice. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 80. Fichiers ZIP et XML de 3C6 Notify of Remittance

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3C6 Notify of Remittance Advice :

- 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 Notify of Self-Billing Invoice

La section suivante présente le contenu du PIP 3C7 Notify of Self-Billing Invoice.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3C7 Notify of Self-Billing Invoice. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 81. Fichiers ZIP et XML de 3C7 Notify of Self-Billing Invoice

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3C7 Notify of Self-Billing Invoice :

- 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 Distribute Work in Process

La section suivante présente le contenu du PIP 3D8 Distribute Work in Process.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 3D8 Distribute Work in Process. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 82. Fichiers ZIP et XML de 3D8 Distribute Work in Process

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 3D8 Distribute Work in Process :

- 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 Notify of Strategic Forecast

La section suivante présente le contenu du PIP 4A1 Notify of Strategic Forecast.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4A1 Notify of Strategic Forecast. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 83. Fichiers ZIP et XML de 4A1 Notify of Strategic Forecast

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4A1 Notify of Strategic Forecast :

- 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 Notify of Threshold Release Forecast

La section suivante présente le contenu du PIP 4A3 Notify of Threshold Release Forecast.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4A3 Notify of Threshold Release Forecast. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 84. 4A3 Notify of Threshold Release Forecast

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4A3 Notify of Threshold Release Forecast :

- 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 Notify of Planning Release Forecast

La section suivante présente le contenu du PIP 4A4 Notify of Planning Release Forecast.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4A4 Notify of Planning Release Forecast . Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 85. 4A4 Notify of Planning Release Forecast

Nom du fichier ZIP	Nom du fichier 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

Tableau 85. 4A4 Notify of Planning Release Forecast (suite)

Nom du fichier ZIP	Nom du fichier XML
BCG_Package_RNSC1.0_RNIFV02.00_4A4R02.00A.zip	BCG_RNSC1.0_RNIFV02.00_4A4R02.00A.xml

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4A4 Notify of Planning Release Forecast :

- 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 Notify of Forecast Reply

La section suivante présente le contenu du PIP 4A5 Notify of Forecast Reply.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4A5 Notify of Forecast Reply. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 86. Fichiers ZIP et XML de 4A5 Notify of Forecast Reply

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4A5 Notify of Forecast Reply :

- 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 Notify of Shipment Receipt

La section suivante présente le contenu du PIP 4B2 Notify of Shipment Receipt.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4B2 Notify of Shipment Receipt. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 87. Fichiers ZIP et XML de 4B2 Notify of Shipment Receipt

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4B2 Notify of Shipment Receipt :

- 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 Notify of Consumption

La section suivante présente le contenu du PIP 4B3 Notify of Consumption.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4B3 Notify of Consumption. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 88. Fichiers ZIP et XML de 4B3 Notify of Consumption

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4B3 Notify of Consumption :

- 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 Distribute Inventory Report V02.01

La section suivante présente le contenu du PIP 4C1 Distribute Inventory Report V02.01PIP.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4C1 Distribute Inventory Report. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 89. Fichiers ZIP et XML de 4C1 Distribute Inventory Report

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4C1 Distribute Inventory Report :

- 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 Distribute Inventory Report V02.03

La section suivante présente le contenu du PIP 4C1 Distribute Inventory Report V02.03.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 4C1 Distribute Inventory Report. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante :

Tableau 90. Fichiers ZIP et XML de 4C1 Distribute Inventory Report

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 4C1 Distribute Inventory Report :

- 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 Distribute Product List

La section suivante présente le contenu du PIP 5C1 Distribute Product List.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 5C1 Distribute Product List. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 91. Fichiers ZIP et XML de 5C1 Distribute Product List

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 5C1 Distribute Product List :

- 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 Request Design Registration

La section suivante présente le contenu du PIP 5C2 Request Design Registration.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 5C2 Request Design Registration. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 92. Fichiers ZIP et XML du PIP 5C2 Request Design Registration

Nom du fichier ZIP	Nom du fichier 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
BCG_Package_RNSC1.0_RNIFV02.00_5C2V01.00.zip	BCG_RNSC1.0_RNIFV02.00_5C2V01.00.xml

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 5C2 Request Design Registration :

- 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 Distribute Registration Status

La section suivante présente le contenu du PIP 5C4 Distribute Registration Status.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 5C4 Distribute Registration Status. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 93. Fichiers ZIP et XML du PIP 5C4 Distribute Registration Status

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 5C4 Distribute Registration Status :

- 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 Request Ship From Stock And Debit Authorization

La section suivante présente le contenu du PIP 5D1 Request Ship From Stock And Debit Authorization.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 5D1 Request Ship From Stock and Debit Authorization. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 94. Fichiers ZIP et XML de 5D1 Request Ship from Stock and Debit Authorization

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

La section suivante présente le contenu du PIP 5D1 Request Ship From Stock And Debit Authorization.

- 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 Query Service Entitlement

La section suivante présente le contenu du PIP 6C1 Query Service Entitlement.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 6C1 Query Service Entitlement. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 95. Fichiers ZIP et XML du PIP 6C1 Query Service Entitlement

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 6C1 Query Service Entitlement :

- 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 Request Warranty Claim

La section suivante présente le contenu du PIP 6C2 Request Warranty Claim.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 6C2 Request Warranty Claim. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 96. Fichiers ZIP et XML du PIP 6C2 Request Warranty Claim

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 6C2 Request Warranty Claim :

- 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 Distribute Work in Process

La section suivante présente le contenu du PIP 7B1 Distribute Work in Process.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 7B1 Distribute Work in Process. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 97. Fichiers ZIP et XML de 7B1 Distribute Work in Process

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 7B1 Distribute Work in Process :

- 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 Notify Of Manufacturing Work Order

La section suivante présente le contenu du PIP 7B5 Notify Of Manufacturing Work Order.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 7B5 Notify of Manufacturing Work Order. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 98. Fichiers ZIP et XML de 7B5 Notify of Manufacturing Work Order

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 7B5 Notify Of Manufacturing Work Order :

- 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 Notify Of Manufacturing Work Order Reply

La section suivante présente le contenu du PIP 7B6 Notify Of Manufacturing Work Order Reply.

Contenu du fichier du package

Le tableau suivant indique les fichiers ZIP et fichiers XML correspondants du PIP 7B6 Notify of Manufacturing Work Order Reply. Les mappes d'instructions, communes à toutes les versions, sont indiquées dans la section suivante.

Tableau 99. Fichiers ZIP et XML de 7B6 Notify of Manufacturing Work Order Reply

Nom du fichier ZIP	Nom du fichier 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

Contenu de la mappe d'instructions

Cette section présente le contenu des mappes d'instructions de 7B6 Notify Of Manufacturing Work Order Reply :

- 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

Chapitre 22. Informations complémentaires sur CIDX

La présente annexe apporte des informations complémentaires sur la prise en charge CIDX. Il contient les rubriques suivantes :

Référence associée

«Prise en charge de l'intégration du processus CIDX»

«Création de packages de définition de document CIDX»

Prise en charge de l'intégration du processus CIDX

CIDX offre les deux mécanismes suivants pour l'intégration de processus :

- Intégration **basée sur le message :** la liaison de document se base sur <RequestingDocumentIdentifier> et <ThisDocumentIdentifier>
- **Intégration basée sur le framework :** la liaison de document est basée sur la sémantique d'en-tête de service RNIF 1.1

Pour l'intégration basée sur le message, des packages PIP 1-action pour les transaction ChemXML sont nécessaires. Tandis que pour l'intégration basée sur le framework, des packages PIP 2-action pour transactions ChemXML sont nécessaires. WebSphere Partner Gateway prend en charge l'intégration du processus forms et process. WebSphere Partner Gateway fournit des packages PIP 1-action pour "E41 Création de commande" et "E42 Réponse à une commande".

Création de packages de définition de document CIDX

Vous pouvez avoir besoin de créer vos propres packages CIDX pour prendre en charge les autres messages CIDX. La procédure de création des nouveaux packages de définition de document CIDX est identique à celle pour RosettaNet.

Pour des informations supplémentaires sur RosettaNet, voir Chapitre 21, «Informations complémentaires sur RosettaNet», à la page 387

Chapitre 23. Attributs

Cette annexe décrit les attributs que vous pouvez définir depuis la console de communauté. Il concerne les attributs suivants :

Attributs EDI

Cette section décrit les attributs EDI disponibles lors de la définition des échanges de données informatisé EDI. Certains de ces attributs sont prédéfinis dans la chaîne de contrôle représentant la mappe de transformation associée au document EDI. Les valeurs définies dans la chaîne de contrôle (sur le client Data Interchange Services) supplantent celles que vous avez saisies sur la console de communauté.

attributs de profil d'enveloppe

Vous pouvez définir plusieurs attributs pour un profil d'enveloppe EDI. Les attributs disponibles dépendent du type d'EDI. En général, les attributs correspondent à un standard d'EDI et les valeurs attribuables dépendent du standard d'EDI représenté par le profil d'enveloppe.

Aucun des attributs n'exige de valeur. Pour certains des attributs, une valeur par défaut est utilisée si vous n'en indiquez aucune. Les tables de la présente section indiquent quels attributs ont des valeurs par défaut et quelles sont ces valeurs.

Remarque : Les propriétés de profil d'enveloppe non répertoriées n'ont pas de valeur par défaut. La valeur texte que vous précisez est utilisée si elle n'est pas supplantée par des propriétés d'enveloppe génériques ou spécifiques définies dans la mappe ou dans une connexion.

attributs X12

Les tableaux de la présente section indiquent les attributs X12 pour lesquels des valeurs par défaut sont fournies.

attributs généraux

Le tableau 100, à la page 446 indique les attributs généraux pour lesquels des valeurs par défaut sont fournies.

Tableau 100. attributs généraux

Nom de zone	Obligatoire ?	Description	Valeur par défaut
INTCTLLEN (Longueur du numéro de contrôle EDI)	Non	Détermine la longueur du numéro de contrôle EDI. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
GRPCTLLEN (Longueur du numéro de contrôle de groupe)	Non	Définit la longueur du numéro de contrôle de groupe. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
TRXCTLLEN (Longueur du numéro de contrôle de transaction)	Non	Détermine la longueur du numéro de contrôle de transaction. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
ENVTYPE (Type d'enveloppe)	Non	Cet attribut n'est pas défini par l'utilisateur mais est dérivé du type de profil d'enveloppe en cours de création.	X12
MAXDOCS (Nombre maximum de transactions)	Non	Nombre maximum de transactions d'une enveloppe. Vous devez saisir un nombre entier.	Aucune valeur maximum
CTLNUMFLAG (Numéros de contrôle par ID de transaction)	Non	Oui indique que des ensembles séparés de numéros de contrôle sont conservés en fonction du type de transaction EDI. Non indique qu'un ensemble commun de numéros de contrôle doit être utilisé pour tous les types de transactions EDI.	Non

attributs EDI

Aucun attribut EDI X12 n'est exigé et les attributs n'ont pas de valeur par défaut.

Tableau 101. attributs des groupes

Nom de zone	Obligatoire ?	Description	Valeur par défaut
GS01 (ID de groupe fonctionnel)	Non	L'identificateur du groupe.	La valeur par défaut est extraite de l'en-tête de chaîne de contrôle. Vous pouvez visualiser cette valeur sur le client Data Interchange Services, en consultant la colonne Groupe fonctionnel de la page Définitions de document EDI.
GS08 (Versions du groupe)	Non	La version du groupe.	La valeur par défaut correspond au standard.

attributs des groupes

Le tableau 101 indique les attributs de groupe pour lesquels des valeurs par défaut sont fournies.

attributs de transaction

Aucun attribut de transaction n'est exigé. Les attributs n'ont pas de valeur par défaut.

attributs UCS

Cette section indique si les valeurs par défaut s'appliquent à un groupe, une transaction ou un EDI UCS.

attributs généraux

Le tableau 102 indique les attributs généraux pour lesquels des valeurs par défaut sont fournies.

Tableau 102. attributs généraux

Nom de zone	Obligatoire ?	Description	Valeur par défaut
INTCTLLEN (Longueur du numéro de contrôle EDI)	Non	Détermine la longueur du numéro de contrôle EDI. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	5
GRPCTLLEN (Longueur du numéro de contrôle de groupe)	Non	Définit la longueur du numéro de contrôle de groupe. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
TRXCTLLEN (Longueur du numéro de contrôle de transaction)	Non	Détermine la longueur du numéro de contrôle de transaction. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
ENVTYPE (Type d'enveloppe)	Non	Cet attribut n'est pas défini par l'administrateur du concentrateur mais est dérivé du type de profil d'enveloppe en cours de création.	UCS
MAXDOCS (Nombre maximum de transactions)	Non	Nombre maximum de transactions d'une enveloppe. Vous devez saisir un nombre entier.	Aucune valeur maximum
CTLNUMFLAG (Numéros de contrôle par ID de transaction)	Non	Oui indique que des ensembles séparés de numéros de contrôle sont conservés en fonction du type de transaction EDI. Non indique qu'un ensemble commun de numéros de contrôle doit être utilisé pour tous les types de transactions EDI.	Non

attributs EDI

Aucun attribut EDI n'est exigé. Les attributs n'ont pas de valeur par défaut.

attributs des groupes

Le tableau 103, à la page 448 indique les attributs de groupe pour lesquels des valeurs par défaut sont fournies.

Tableau 103. attributs des groupes

Nom de zone	Obligatoire ?	Description	Valeur par défaut
GS01 (ID de groupe fonctionnel)	Non	L'identificateur du groupe.	La valeur par défaut est extraite de l'en-tête de chaîne de contrôle. Vous pouvez visualiser cette valeur sur le client Data Interchange Services, en consultant la colonne Groupe fonctionnel de la page Définitions de document EDI.
GS08 (Versions du groupe)	Non	La version du groupe.	La valeur par défaut correspond au standard.

attributs de transaction

Aucun attribut de transaction n'est exigé. Les attributs n'ont pas de valeur par défaut.

attributs EDIFACT

Cette section indique si les valeurs par défaut s'appliquent à un groupe, un message ou un EDI EDIFACT.

attributs généraux

Le tableau 104 indique les attributs généraux pour lesquels des valeurs par défaut sont fournies.

Tableau 104. attributs généraux

Nom de zone	Obligatoire ?	Description	Valeur par défaut
INTCTLLEN (Longueur du numéro de contrôle EDI)	Non	Détermine la longueur du numéro de contrôle EDI. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
GRPCTLLEN (Longueur du numéro de contrôle de groupe)	Non	Définit la longueur du numéro de contrôle de groupe. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
TRXCTLLEN (Longueur du numéro de contrôle de transaction)	Non	Détermine la longueur du numéro de contrôle de transaction. Vous devez saisir un nombre entier. Si aucune valeur n'est saisie, la longueur par défaut est utilisée.	9
ENVTYPE (Type d'enveloppe)	Non	Cet attribut n'est pas défini par l'administrateur du concentrateur mais est dérivé du type de profil d'enveloppe en cours de création.	EDIFACT
EDIFACTGRP (Création de groupes pour EDI)	Non	Cette valeur n'est valable que pour les enveloppes de type EDIFACT (le niveau groupe a été désapprouvé dans EDIFACT). Oui indique que des groupes fonctionnels (segments (UNG/UNE) doivent être créés pour EDIFACT DATA. Non indique qu'il est inutile d'en créer.	Non

Tableau 104. attributs généraux (suite)

Nom de zone	Obligatoire ?	Description	Valeur par défaut
MAXDOCS (Nombre maximum de transactions)	Non	Nombre maximum de transactions d'une enveloppe. Vous devez saisir un nombre entier.	Aucune valeur maximum
CTLNUMFLAG (Numéros de contrôle par ID de transaction)	Non	Oui indique que des ensembles séparés de numéros de contrôle sont conservés en fonction du type de transaction EDI. Non indique qu'un ensemble commun de numéros de contrôle doit être utilisé pour tous les types de transactions EDI.	Non

attributs EDI

Aucun attribut EDI n'est exigé. Les attributs n'ont pas de valeur par défaut.

attributs des groupes

Le tableau 105 indique les attributs de groupe pour lesquels des valeurs par défaut sont fournies.

Tableau 105. attributs des groupes

Nom de zone	Obligatoire ?	Description	Valeur par défaut
UNG01 (ID de groupe fonctionnel)	Non	L'identificateur du groupe.	La valeur par défaut est extraite de l'en-tête de chaîne de contrôle. Vous pouvez visualiser cette valeur sur le client Data Interchange Services, en consultant la colonne Groupe fonctionnel de la page Définitions de document EDI.

Attributs de messages

Le tableau 106 indique les attributs de messages pour lesquels des valeurs par défaut sont fournies.

Tableau 106. Attributs de messages

Nom de zone	Obligatoire ?	Description	Valeur par défaut
UNH0201 (Type de message)	Non	Le type de message.	La valeur par défaut est extraite de l'en-tête de chaîne de contrôle. Vous pouvez visualiser cette valeur sur le client Data Interchange Services, en consultant la page Définitions de document EDI.
UNH0202 (Version de message)	Non	La version du message.	D
UNH0203 (Version de message)	Non	La version du message.	D'après le standard
UNH0204 (Agence de contrôle)	Non	Le code identifiant une agence de contrôle.	UN

Attributs de définition et de connexion de document

Cette section décrit les attributs de définition de document pour l'enveloppe. Certains de ces attributs ne peuvent être définis qu'au niveau du protocole ou de la connexion, comme indiqué.

Attributs de séparateur et de délimiteur

Cette section indique les caractères utilisés en tant que délimiteurs ou séparateurs dans un EDI. Le tableau 107 indique la façon dont l'attribut apparaît sur la console de communauté, le terme correspondant dans X12 et EDIFACT (ISO 9735 Version 4, Edition 1), si l'attribut est obligatoire et fournit une description de l'attribut. Après le tableau, un exemple indique de quelle façon ces caractères apparaissent dans un document EDI.

Descriptions des attributs

Les attributs des séparateurs et délimiteurs sont indiqués dans le tableau 107.

Remarque : Certains caractères (indiqués) peuvent être en hexadécimal. Il peut s'agir de valeurs Unicode provenant d'autres types de codages. Pour Unicode, utilisez le format \unnnn. Pour les autres codages, utilisez le format 0xnn.

Tableau 107. Attributs du profil de l'enveloppe

Attribut	Terme X12	Terme EDIFACT	Description
Délimiteur de segment	marque de fin de segment	marque de fin de segment	Caractère unique placé à la fin d'un segment. Il peut s'agir d'une valeur hexadécimale. La valeur par défaut dépend du type d'EDI. **X12** ~ (tilde) **EDIFACT** ' (guillemet simple) **UCS** ~ (tilde)
Délimiteur d'élément de données	séparateur d'élément de données	séparateur d'élément de données	Caractère unique qui sépare les éléments de données d'un segment. Il peut s'agir d'une valeur hexadécimale. La valeur par défaut dépend du type d'EDI. **X12** * (astérisque) **EDIFACT** + (signe plus) **UCS** * (astérisque)
Délimiteur d'élément secondaire	séparateur d'élément de composant	séparateur d'élément de données de composant	Caractère unique qui sépare les éléments individuels d'un élément de données composite. Il peut s'agir d'une valeur hexadécimale. La valeur par défaut dépend du type d'EDI. **X12** \ (barre oblique inversée) **EDIFACT** : (deux points) **UCS** \ (barre oblique inversée)

Tableau 107. Attributs du profil de l'enveloppe (suite)

Attribut	Terme X12	Terme EDIFACT	Description
caractère de déblocage		caractère de déblocage	Caractère unique qui modifie la signification du caractère suivant, permettant à un caractère séparateur d'apparaître dans un élément de données. Il peut s'agir d'une valeur hexadécimale. Ceci ne s'applique qu'à EDIFACT. **EDIFACT** ? (point d'interrogation)
Séparateur d'élément de données à répétition	séparateur de répétition	séparateur de répétition	Caractère unique qui sépare les instances d'un élément de données de répétition. Il peut s'agir d'une valeur hexadécimale. La valeur par défaut dépend du type d'EDI pour X12 ou EDIFACT. **X12** ^ (accent circonflexe) **EDIFACT** * (astérisque)
Notation décimale		notation décimale (désapprouvée)	Cet attribut était utilisé pour le formatage décimal ou l'analyse syntaxique. Il est désormais désapprouvé. Il s'agit d'un point ou d'une virgule. La valeur par défaut est le point.

Exemple de structure EDI

Cette section décrit un EDI simple et comment s'utilisent dans un EDI les attributs décrits au tableau 107, à la page 450.

Un message EDI est composé de plusieurs segments disposés dans un ordre particulier. Une segment est composé d'une série d'éléments. Il peut s'agir d' éléments de données simples contenant une seule information. Il peut également s'agir d' éléments de données composites, constitués de plusieurs éléments de données simples. Ces éléments simples sont appelés des éléments de données de composant.

Les éléments de données composites ne sont pas imbriqués. Un élément composite ne peut contenir que des éléments de données simples, pas d'autres éléments composites. Même si le cas n'est pas présenté dans ce document, un élément de données de composant peut également être défini en tant qu'élément de données à répétition.

Prenons l'exemple suivant :

```
ABC*123*AA\BB\CC*001^002^003*star?*power~
```

Dans cet exemple :

- "ABC" est le nom du segment (nommé "étiquette du segment" par EDIFACT) ; il est appelé "segment ABC"
- "*" (astérisque) est le séparateur d'élément de données.

  Le nom d'attribut correspondant sur la console de communauté est Délimiteur de segment.
- "123" est le premier élément de données, simple (parfois nommé ABC01 dans certains contextes)

- "AA\BB\CC" est le second élément de données (ABC02), un élément composite constitué d' éléments de données de composant
  - "\ " (barre oblique inversée) est le séparateur d'élément de données de composant

    Le nom d'attribut correspondant sur la console de communauté est le délimiteur d'élément de données
  - "AA" est le premier élément de données de composant de ABC02 (également désigné par ABC0201)
  - "BB" est le deuxième élément de données de composant de ABC02 (ABC0202)
  - "CC" est le troisième élément de données de composant de ABC02 (ABC0203)
- "001^002^003" est le troisième élément de données (ABC03), un élément de données à répétition
  - "^" (accent circonflexe) est un séparateur de répétition

    Le nom d'attribut correspondant sur la console de communauté est le caractère d'élément de données à répétition
  - "001","002" et "003" sont les répétitions (toutes également désignées par ABC03)
- "star?*power" est le quatrième élément de données (ABC04)
  - "?" (point d'interrogation) est le caractère de déblocage : l'astérisque qui suit n'est pas traité comme un séparateur d'élément de données
  - "star*power" est la valeur qui résulte de ABC04
- "~" (tilde) marque la fin du segment.

  Le nom d'attribut correspondant sur la console de communauté est Délimiteur de segment.

Autres attributs d'EDI

Cette section indique les attributs d'EDI supplémentaires que vous pouvez définir au niveau de la définition du document ou de la connexion.

Tableau 108. Autres attributs d'EDI

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Sortie de segment	Non	Utilisé pour la transformation EDI/XML, indique si un saut de ligne doit être inséré après chaque segment EDI ou élément XML. **Important :** 1. Utilisez toujours un seul délimiteur de caractères. 2. Si vous utilisez la combinaison de délimiteurs de caractères "/r/n" et que le délimiteur de caractères "/r" se trouve en position de délimiteur de segment de l'en-tête d'échange, le délimiteur de caractères "/n" sera ignoré. 3. Modifiez l'arborescence des types en conséquence.	Limité au protocole ou à la connexion	Oui

Tableau 108. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Autorise les documents avec ID en double	Non	Oui indique que les ID de documents en double (numéros de contrôle EDI) sont autorisés. Non indique que les numéros de contrôle EDI en double doivent être traités comme une erreur.	Limité au protocole ou à la connexion	Non
Niveau d'erreur max lors de la transformation	Non	Indique le nombre maximum d'erreurs autorisées au cours d'une transformation avant qu'elle n'échoue. Les valeurs valides sont 0, 1 et 2. Si la mappe de transformation contient une commande Erreur pour indiquer une erreur spécifique à l'utilisateur et si le niveau de la commande Erreur est supérieur à cette valeur, la transformation échoue.	Limité au protocole ou à la connexion	0
Mappe d'accusé de réception fonctionnel	Non	Fournit la mappe utilisée pour convertir l'accusé de réception générique interne en accusé de réception spécifique. **Remarque :** Vous sélectionnez cet attribut dans une liste de mappes FA (mappes d'accusé de réception fonctionnel, de type “K”).	Limité au protocole ou à la connexion	
Profil de l'enveloppe	Oui	Le nom du profil d'enveloppe EDI à utiliser pour l'enveloppement. Tous les profils d'enveloppe définis figurent dans la liste.		
actif XMLNS	Non	Procède au traitement de l'espace de nom pour le document XML en entrée. Cet attribut est utilisé par l'étape de transformation XML. Les valeurs valides sont Oui et Non.		Schéma : Oui DTD : Non
Niveau d'erreur de validation max	Non	Le niveau maximum d'erreur de validation acceptable (gravité de l'erreur acceptée avant de considérer la transaction comme "échouée"). Les valeurs valides sont 0, 1 et 2. **0** N'autoriser la validation qu'en l'absence d'erreurs. **1** Accepter les documents qui n'ont que des erreurs de validation d'élément simple. **2** Accepter les documents qui ont des erreurs de validation d'élément ou de segment		0

Tableau 108. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
niveau de validation	Non	Indique le niveau de contrôle à effectuer au niveau de la transaction. Le niveau 2 utilise les valeurs définies dans la table de validation alphanumérique et la table de validation des jeux de caractères. Cet attribut s'applique également à l'attribut Validation détaillée des segments, si cet attribut est défini sur Oui. Les valeurs valides sont 0, 1 et 2. **0** Procéder uniquement à une validation de base, telle que le contrôle des éléments ou segments manquants et des longueurs minimum et maximum. Ne pas valider les valeurs d'éléments par rapport aux listes de codes ou types de données précisés dans la définition de transaction. **1** Procéder à une validation de niveau 0 et valider les valeurs des éléments par rapport aux listes de codes précisées pour l'élément de données. **2** Procéder à une validation de niveau 1 et vérifiez la validité de la valeur de l'élément par rapport au type de données de l'élément.		0
table de validation de jeu de caractère	Non	Indique la table à utiliser pour valider le jeu de caractères. Cette table n'est utilisée que lorsque l'attribut du Niveau de validation est 2. Cet attribut concerne la table des listes de codes virtuels. L'utilisateur peut créer de nouvelles listes de codes dans l'onglet Listes de codes de la zone Mapping du client Data Interchange Services. Cette zone contient également les listes de codes utilisées dans d'autres contextes, par exemple la validation de certains éléments EDI.		CHARSET
table de validation alphanumérique	Non	Indique la table à utiliser pour la validation alphanumérique. Cette table n'est utilisée que lorsque l'attribut du Niveau de validation est 2. Cet attribut concerne les tables des listes de codes virtuels. L'utilisateur peut créer de nouvelles listes de codes dans l'onglet Listes de codes de la zone Mapping du client Data Interchange Services. Cette zone contient également les listes de codes utilisées dans d'autres contextes, par exemple la validation de certains éléments EDI.		ALPHANUM

Tableau 108. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
générer des informations de niveau de groupe uniquement dans l'Accusé de réception fonctionnel	Non	Cet attribut s'applique à EDI-X12. Les valeurs sont Oui ou Non. **Oui** Ne générer les informations de niveau de groupe que pour l'accusé de réception fonctionnel. **Non** Générer les informations détaillées complètes sur l'accusé de réception fonctionnel (pour chaque transaction individuelle et les segments et éléments d'une transaction).	Limité au protocole ou à la connexion	Non
année de contrôle du siècle	Non	Intervient pour la conversion sur quatre chiffres des dates sur deux chiffres. Si la date sur deux chiffres est supérieure à cette valeur, le quantième du siècle est “19”. Si la date sur deux chiffres est inférieure ou égale à cette valeur, le quantième du siècle est “20”. La plage valide est 0-99.	Limité au protocole ou à la connexion	10
Validation détaillée des segment	Non	Cet attribut s'applique aux en-têtes et éléments de fin de segment suivants : • X12 – ISA, IEA – GS, GE – ST, SE • EDIFACT – UNA – UNB, UNZ – UNG, UNE – UNH, UNT • UNTUCS – BG, EG – GS, GE – ST, SE Les valeurs valides sont Oui et Non. **Oui** Procéder à un validation détaillée des segments d'enveloppe. La précision du contrôle est définie par l'attribut Niveau de validation. **Non** Ne pas procéder à une validation détaillée des segments d'enveloppe.	Limité au protocole ou à la connexion	Non
Annulation TA1	Non	Autoriser la génération d'une requête TA1 si indiqué dans le segment d'enveloppe EDI. S'applique uniquement à EDI-X12. Si Oui, un TA1 est généré s'il est précisé dans le segment d'enveloppe EDI. Si non, aucun TA1 n'est généré même s'il est précisé dans le segment d'enveloppe EDI.	Limité au protocole ou à la connexion	Oui

Tableau 108. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Supprimer une erreur	Non	Cet attribut est utilisé dans le traitement polymorphe. Dans le cas d'un traitement par lot résultant d'un désenveloppement, cet attribut indique s'il faut supprimer tout le traitement par lot si l'une des transactions échoue. Les valeurs valides sont Oui et Non.	Limité au protocole ou à la connexion	Non
Qualificatif 1 de profil de connexion	Non	Cet attribut est utilisé par l'enveloppeur pour déterminer le profil à utiliser pour une connexion EDI. Les transactions sont placées dans différents EDI selon la valeur de cet attribut.		
Qualificatif de l'EDI	Non	Le code qui sert à identifier le format de l'identificateur de l'émetteur ou du destinataire de l'EDI.		
Identificateur de l'EDI	Non	Identifie l'émetteur ou le destinataire du document. Le type de donnée entrée est défini par l'attribut Qualificatif de l'EDI.		
Indicateur de syntaxe EDI	Non	Indique si les documents sources en cours de traduction sont de type Production, Test ou Information. Les valeurs valides sont P, T et I.		
Identificateur d'émetteur d'application de groupe	Non	Identifie l'émetteur de la transaction. Une fois convenu par les partenaires d'échanges, cet attribut facilite l'adressage au sein d'une entreprise.		
Identificateur de récepteur d'application de groupe	Non	Identifie le destinataire de la transaction. Une fois convenu par les partenaires d'échanges, cet attribut facilite l'adressage au sein d'une entreprise.		
Routage EDI inverse	Non	Indique l'adresse où doit être envoyée toute réponse.		
Adresse de routage EDI	Non	Le code de sous-adresse pour le routage intermédiaire.		
Qualificatif d'émetteur d'application de groupe	Non	Le code qui sert à identifier le format de l'identificateur de l'émetteur d'application de groupe.		
Identificateur de récepteur d'application de groupe	Non	Le code qui sert à identifier le format de l'identificateur du récepteur d'application de groupe.		
Mot de passe d'application de groupe	Non	Cet attribut définit les informations de sécurité.		
Limite de temps FA requise		Nombre de minutes après lequel une transaction est envoyée et dans laquelle une FA doit être renvoyée. Si la valeur est vierge, aucune FA n'est requise.		

Propriétés du client Data Interchange Services

Cette section décrit les propriétés qui peuvent être définies dans le cadre d'une mappe de transformation, dans le client Data Interchange Services et les attributs WebSphere Partner Gateway correspondants.

Tableau 109. Propriétés de mappages et attributs correspondants

Propriété du client Data Interchange Services	Supplante l'attribut WebSphere Partner Gateway
AckReq	Accusé de réception requis
Alphanum	table de validation alphanumérique
Charset	table de validation de jeu de caractère
CtlNumFlag	Numéros de contrôle par Id de transaction
EdiDecNot (notation décimale)	Notation décimale
EdiDeDlm (séparateur d'élément de données)	Délimiteur d'élément de données
EdiDeSep (séparateur d'élément de données à répétition)	Séparateur d'élément de données à répétition
EdifactGrp	Création de groupes pour EDI
EdiRlsChar (caractère de déblocage)	caractère de déblocage
EdiSeDlm (séparateur d'élément de données de composant)	Délimiteur d'élément secondaire
EdiSegDlm (marque de fin de segment)	Délimiteur de segment
EnvProfName	Profil d'enveloppe
EnvType	Type d'enveloppe
MaxDocs	nombre maximum de transactions
Reroute	Routage EDI inverse
SegOutput	Sortie de segment
ValLevel	niveau de validation
ValErrLevel	Niveau d'erreur de validation max
ValMap	Mappe de validation

Le tableau 110 répertorie d'autres propriétés du client Data Interchange Services et les attributs WebSphere Partner Gateway qui leur sont associés.

Tableau 110. Propriétés de client Data Interchange Services et attributs associés

Propriété du client Data Interchange Services	Supplante l'attribut WebSphere Partner Gateway
IchgCtlNum	Numéro de contrôle EDI.
IchgSndrQl	Qualificatif de l'émetteur EDI
IchgSndrId	ID de l'émetteur EDI
IchgRcvrQl	Qualificatif du récepteur de l'EDI
IchgRcvrId	ID du récepteur de l'EDI
IchgDate	Date de l'EDI
IchgTime	Heure de l'EDI
IchgPswd	Mot de passe de l'EDI

Tableau 110. Propriétés de client Data Interchange Services et attributs associés (suite)

Propriété du client Data Interchange Services	Supplante l'attribut WebSphere Partner Gateway
IchgUsgInd	Indicateur de syntaxe EDI
IchgAppRef	Référence de l'application EDI.
IchgVerRel	Version et édition de l'EDI.
IchgGrpCnt	Nombre de groupes de l'EDI.
IchgCtlTotal	Contrôle de total du segment de fin de l'EDI.
IchgTrxCnt	Nombre de documents dans l'EDI.
GrpCtlNum	Numéro de contrôle de groupe
GrpFuncGrpId	ID du groupe fonctionnel
GrpAppSndrId	ID d'émetteur de l'application de groupe
GrpAppRcvrId	ID du récepteur de l'application de groupe
GrpDate	Date du groupe
GrpTime	Heure du groupe
GrpPswd	Mot de passe de groupe
GrpVer Version du groupe.	Version du groupe
GrpRel Edition du groupe.	Edition du groupe
GrpTrxCnt	Nombre de documents dans le groupe
TrxCtlNum	Numéro de contrôle de transaction
TrxCode	Code de transaction
TrxVer	Version de transaction
TrxRel	Edition de transaction
TrxSegCnt	Nombre de segments EDI dans le document.

attributs AS

Cette section apporte des informations sur les attributs AS.

Tableau 111. attributs AS

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Heure d'accusé de réception en minutes	Non	La durée d'attente d'un accusé de réception MDN avant de renvoyer la demande initiale. Cet attribut est associé au Nombre de relances. Il est indiqué en minutes.	Limité au protocole ou à la connexion	30
Nombre de relances	Non	Le nombre de fois que la demande sera renvoyée si une MDN n'est pas reçue. Cet attribut est associé à l'attribut Heure d'accusé de réception. Par exemple, la valeur 3 indique que la demande pourra être envoyée au maximum quatre fois (une fois pour la demande initiale et trois tentatives supplémentaires).	Limité au protocole ou à la connexion	3

Tableau 111. attributs AS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Compression AS avant signature	Non	Indique si la compression AS doit être appliquée aux données utiles et à la signature, ou seulement aux données utiles. Si vous sélectionnez Oui, les données utiles sont compressées avant que le message ne soit signé. Cet attribut est associé à l'attribut Compression AS.	Limité au protocole ou à la connexion	Oui
Compression AS	Non	Compression des données. Cet attribut est associé à l'attribut Compression AS avant signature.	Limité au protocole ou à la connexion	Non
Chiffrement AS	Non	Cet attribut s'applique à AS2 et sert à indiquer l'URL où un partenaire doit envoyer une MDN asynchrone. Cet attribut fonctionne en conjonction avec l'attribut AS MDN asynchrone, mais une valeur est requise même pour les MDN synchrones.	Limité au protocole ou à la connexion	Non
AS MDN Http Url	Oui si l'attribut "AS MDN asynchrone" est défini sur Oui et que vous utilisez AS2.	Cet attribut s'applique à AS2 et sert à indiquer l'URL où un partenaire doit envoyer une MDN asynchrone. Cet attribut fonctionne en conjonction avec l'attribut AS MDN asynchrone, mais une valeur est requise même pour les MDN synchrones.	Limité au protocole ou à la connexion	
Adresse électronique MDN de l'AS	Oui si l'attribut "AS MDN asynchrone" est défini sur Oui et que vous utilisez AS1.	Indique l'adresse e-mail que le partenaire utilisera pour envoyer une MDN asynchrone. Cet attribut est utilisé en association avec l'attribut AS MDN demandé. La valeur de l'attribut Adresse électronique MDN de l'AS sert pour la zone “Disposition-notification-to”. Pour AS1, cet attribut fonctionne en conjonction avec l'attribut AS MDN asynchrone au format mailto:xxx@company.com. Pour AS2, cet attribut exige toujours une valeur bien que l'adresse e-mail elle-même ne soit pas utilisée.	Limité au protocole ou à la connexion	

Tableau 111. attributs AS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
AS MDN asynchrone	Non	Indique si la MDN doit être retournée de manière synchrone ou asynchrone. Selon la valeur de cet attribut, c'est l'attribut AS MDN HTTP URL ou Adresse électronique de l'AS qui est utilisé. Les valeurs valides sont Oui et Non. **Oui** Asynchrone **Non** Synchrone Si l'attribut est défini sur Oui, la zone "receipt-delivery-option" est renseignée selon l'attribut AS MDN HTTP URL (pour AS2) ou l'attribut Adresse électronique de l'AS (pour AS1).	Limité au protocole ou à la connexion	Oui
AS MDN demandé	Non	Indique si une réponse MDN est obligatoire. Si l'attribut est défini sur Oui, l'en-tête “transport Disposition-notification-to” sera renseigné avec la valeur de l'attribut Adresse électronique MDN de l'AS. Les valeurs valides sont Oui et Non. **Oui** Exige une MDN. **Non** Une MDN n'est pas obligatoire.	Limité au protocole ou à la connexion	Oui
Algorithme de la synthèse de message AS	Non	L'algorithme de synthèse de message à utiliser lors de la signature. Cet attribut est utilisé en association avec les attributs AS signé et AS MDN signé. Pour les MDN signées, la valeur sert à renseigner l'en-tête “Disposition-notification-options: signed-receipt-micalg”.	Limité au protocole ou à la connexion	sha1
AS MDN signée	Non	Indique si la demande exige le retour d'une MDN signée. Cet attribut est utilisé en association avec l'attribut AS MDN demandé. Si la valeur est Oui, la zone “Disposition-notification-options: signed-receipt-protocol” est renseignée. Les valeurs valides sont Oui et Non. **Oui** Une MDN signée est exigée. **Non** Une MDN signée n'est pas exigée. Si cet attribut est défini sur Oui, la MDN envoyée par le partenaire doit être signée. Si cet attribut est défini sur Non, la MDN peut être signée ou non.	Limité au protocole ou à la connexion	Non

Tableau 111. attributs AS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
AS signé	Non	Indique s'il faut ou non signer le document. Pour le côté VERS de l'échange (lorsque vous envoyez des documents à un partenaire), cet attribut indique s'il faut signer le document. Pour le côté DEPUIS de l'échange (lorsque vous recevez des documents d'un partenaire), si l'attribut est défini sur Oui, une demande AS envoyée par le partenaire doit être signée. Si l'attribut est défini sur Non, le document du partenaire peut être signé ou non. **Oui** Signer le document **Non** Il n'est pas obligatoire de signer le document	Limité au protocole ou à la connexion	Non
Irréfutabilité requise	Non	Indique si ce document doit ou non être sauvegardé dans le magasin d'irréfutabilité. S'appliquera au document à la fois en tant que source ou cible. Oui – Sauvegarde le document dans le magasin d'irréfutabilité. Non – Ne sauvegarde pas le document dans le magasin d'irréfutabilité.	Limité au protocole ou à la connexion	Oui
Emplacement de stockage des messages requis	Non	Indique si ce document doit ou non être sauvegardé dans l'emplacement de stockage des messages. S'appliquera aux documents source et cible. Oui – Sauvegarde le document dans l'emplacement de stockage des messages. Non – Ne sauvegarde pas le document dans l'emplacement de stockage des messages.	Limité au protocole ou à la connexion	Oui
ID entreprise de l'AS	Non	L'ID entreprise de l'AS à utiliser dans l'en-tête “AS2-To” ou “AS3-To”. En l'absence de valeur, WebSphere Partner Gateway utilise l'ID entreprise du récepteur qui a servi dans le document source. **Remarque :** L'en-tête “AS2-From” ou “AS3-From” sera défini à partir de l'attribut “ID entreprise de l'AS” provenant de la définition du document source ou, s'il n'est pas défini, du document source original qui est arrivé dans WebSphere Partner Gateway et qui est envoyé en tant qu'AS.	Limité au protocole ou à la connexion	

Tableau 111. attributs AS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Adresse AS MDN FTP	Oui pour AS3 lorsque l'attribut "AS MDN Requested" est Oui	L'adresse AS MDN FTP à utiliser lorsque l'on demande une MDN. Cet attribut est utilisé en conjonction avec l'attribut "AS MDN Requested". La valeur de l'adresse AS MDN FTP est utilisée dans la zone “Disposition-notification-to”. Elle doit être au format : `ftp://username:pwd@host.com:port/folder-name.`	Limité au protocole ou à la connexion	Non
Algorithme de signature	Oui si "Signature numérique obligatoire" est sur Oui	Algorithme utilisé pour signer le document. Cet attribut n'est utilisé que si la valeur d'attribut “Signature numérique obligatoire” est définie sur “Oui.”		dsa-sha1
Algorithme de chiffrement	Oui lorsque la valeur d'attribut “Chiffrement obligatoire” est définie sur “Oui.”	L'algorithme est utilisé pour chiffrer les charges. Cette valeur fonctionne en conjonction avec l'attribut "Protocole de chiffrement". Cet attribut n'est utilisé que si la valeur d'attribut “Chiffrement obligatoire” est définie sur “Oui.”		AES-128
Protocole de chiffrement	Non	Protocole utilisé pour chiffrer les charges. Les valeurs possibles sont ChiffrementXML et SMIME. Cet attribut n'est utilisé que si la valeur d'attribut "Chiffrement obligatoire" est définie sur "Oui." Si Chiffrement obligatoire est défini sur "oui" et qu'aucune valeur n'est fournie pour cet attribut, le document échouera.		ChiffrementXML

attributs RosettaNet

Cette section apporte des informations sur les attributs RosettaNet.

Tableau 112. attributs RosettaNet

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Heure d'accusé de réception	Oui	La durée d'attente d'un accusé de réception avant de renvoyer la demande initiale. Cet attribut est associé au Nombre de relances. Il est indiqué en minutes. La valeur par défaut est obtenue du document de spécification PIP RosettaNet.	Limité au protocole ou à la connexion	120
Durée d'exécution	Oui	La durée d'attente d'une réponse à une demande, avant d'envoyer un message de notification d'échec.	Limité au protocole ou à la connexion	

Tableau 112. attributs RosettaNet (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Nombre de relances	Oui	Le nombre de fois que la demande sera renvoyée si un accusé de réception n'est pas reçu. Cet attribut est associé à l'attribut Heure d'accusé de réception. Par exemple, la valeur 3 indique que la demande pourra être envoyée au maximum quatre fois (une fois pour la demande initiale et trois tentatives supplémentaires). La valeur par défaut est obtenue du document de spécification PIP RosettaNet.	Limité au protocole ou à la connexion	3
Signature numérique requise	Non	Indique si le message PIP doit avoir une signature numérique. La valeur par défaut est obtenue du document de spécification PIP RosettaNet.	Limité au protocole ou à la connexion	Oui
Irréfutabilité requise	Non	Indique si ce document doit ou non être sauvegardé dans le magasin d'irréfutabilité. S'appliquera au document à la fois en tant que source ou cible. Oui – Sauvegarde le document dans le magasin d'irréfutabilité. Non – Ne sauvegarde pas le document dans le magasin d'irréfutabilité.	Limité au protocole ou à la connexion	Oui
Emplacement de stockage des messages requis	Non	Indique si ce document doit ou non être sauvegardé dans l'emplacement de stockage des messages. S'appliquera aux documents source et cible. Oui – Sauvegarde le document dans l'emplacement de stockage des messages. Non – Ne sauvegarde pas le document dans l'emplacement de stockage des messages.	Limité au protocole ou à la connexion	Oui
Irréfutabilité de l'avis de réception requise	Non	Indique si le document Accusé de réception doit être conservé dans le magasin d'irréfutabilité. La valeur par défaut est obtenue du document de spécification PIP RosettaNet.	Limité au protocole ou à la connexion	Oui
Synchronisation prise en charge		Indique si le PIP prend en charge les communications synchrones. La valeur par défaut dépend de la spécification du PIP.	Limité au protocole ou à la connexion Cet attribut n'est disponible que pour RNIF 2.0.	

Tableau 112. attributs RosettaNet (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Accusé de réception de synchronisation requise		Indique si le PIP exige un Accusé de réception synchrone. La valeur par défaut dépend de la spécification du PIP.	Limité au protocole ou à la connexion Cet attribut n'est disponible que pour RNIF 2.0.	
Code de la chaîne d'approvisionnement globale	Obligatoire pour RNIF 1.1	Il s'agit du code identifiant la chaîne d'approvisionnement de la fonction du partenaire. Les valeurs autorisées sont : • Composants électroniques • Technologie d'informations • Technologie de semiconducteurs	Limité au protocole ou à la connexion	
Chiffrement		Cet attribut indique s'il faut appliquer un chiffrement. **Remarque :** Il ne s'agit pas du chiffrement SSL. Pour le côté VERS de l'échange (lorsque vous envoyez des documents à un partenaire), cet attribut indique qu'il faut chiffrer le document. Pour le côté DEPUIS de l'échange (lorsque vous recevez des documents d'un partenaire), si l'attribut est défini sur Oui, une demande RNIF envoyée par le partenaire doit être chiffrée. Si l'attribut est défini sur Non, le document du partenaire peut être chiffré ou non. Les valeurs autorisées sont : **None** Le chiffrement n'est pas obligatoire. **Charge** Le chiffrement ne portera que sur le contenu du service RosettaNet. **Données utiles et Conteneur** Le chiffrement portera sur le contenu et sur l'en-tête du service RosettaNet.	Limité au protocole ou à la connexion Cet attribut n'est disponible que pour RNIF 2.0.	None
Texte de message standard	Non	Il s'agit de la norme à laquelle le contenu du service doit être conforme. Cela doit être défini si, et uniquement s'il s'agit d'un Message de contenu de service spécifié non RosettaNet.		Pas de valeur par défaut.
Version de message standard	Non	Il s'agit de la version de la norme à laquelle le contenu du service doit être conforme. Cela doit être défini si, et uniquement s'il s'agit d'un Message de contenu de service spécifié non RosettaNet.		Pas de valeur par défaut.

Tableau 112. attributs RosettaNet (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Identificateur de liaison de charge PIP	Non	Il s'agit d'un identificateur de liaison PIP défini par le partenaire, qui est unique entre les partenaires commerciaux. Cet attribut n'est défini que dans le cas d'un contenu de service non RosettaNet.		Pas de valeur par défaut.
FromGlobalPartner ClassificationCode	Oui pour les schémas RNIF 1.1	Il s'agit du code identifiant la fonction d'un partenaire dans la chaîne d'approvisionnement. Requis uniquement lorsque l'on utilise RNIF 1.1 pour les PIP basés sur un schéma. Cette valeur doit être spécifiée également pour 0A1 pip, lorsque sont utilisés les PIP basés sur un schéma.		Pas de valeur par défaut.
ToGlobalPartner ClassificationCode	Oui pour les schémas RNIF 1.1	Il s'agit du code identifiant la fonction d'un partenaire dans la chaîne d'approvisionnement. Requis uniquement lorsque l'on utilise RNIF 1.1 pour les PIP basés sur un schéma. Cette valeur doit être spécifiée également pour 0A1 pip, lorsque sont utilisés les PIP basés sur un schéma.		Pas de valeur par défaut.
Algorithme de résumé de message RN	Non	Cet attribut n'est utilisé que lorsque l'attribut “Signature numérique obligatoire” est défini sur Oui. Détermine l'algorithme de synthèse à utiliser pour la signature numérique. Les valeurs autorisées sont SHA1 et MD5.		SHA1
Algorithme de chiffrement RN	Non	Cet attribut n'est utilisé que lorsque l'attribut “Chiffrement” est défini sur “Charge” ou “Charge et conteneur”. Les valeurs autorisées sont “Triple DES” et “RC2-40”.		Norme Triple DES

Attribut Backend Integration

Cette section apporte des informations sur l'attribut associé à l'empaquetage Backend Integration.

Tableau 113. Attribut Backend Integration

Attribut	Description	Valeur par défaut
Indicateur d'enveloppe	Cet attribut indique s'il faut intégrer le document dans une enveloppe XML. Les valeurs valides sont Oui et Non.	Non

Attributs ebMS

Cette section décrit les attributs ebMS.

Tableau 114. Attributs ebMS

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Heure d'accusé de réception en minutes	Non	La durée d'attente d'un accusé de réception avant de renvoyer la demande initiale. Cet attribut est associé au Nombre de relances. Il est indiqué en minutes.	Limité au protocole ou à la connexion	30
Nombre de relances	Non	Le nombre de fois que la demande sera renvoyée si un accusé de réception n'est pas reçu. Cet attribut est associé à l'attribut Heure d'accusé de réception. Par exemple, la valeur 3 indique que la demande pourra être envoyée au maximum quatre fois (une fois pour la demande initiale et trois tentatives supplémentaires).	Limité au protocole ou à la connexion	3
Irréfutabilité requise	Non	Indique si ce document doit ou non être sauvegardé dans le magasin d'irréfutabilité. S'appliquera au document à la fois en tant que source ou cible. Oui – Sauvegarde le document dans le magasin d'irréfutabilité. Non – Ne sauvegarde pas le document dans le magasin d'irréfutabilité.	Limité au protocole ou à la connexion	Oui
Emplacement de stockage des messages requis	Non	Indique si ce document doit ou non être sauvegardé dans l'emplacement de stockage des messages. S'appliquera aux documents source et cible. Oui – Sauvegarde le document dans l'emplacement de stockage des messages. Non – Ne sauvegarde pas le document dans l'emplacement de stockage des messages.	Limité au protocole ou à la connexion	Oui
Irréfutabilité de l'avis de réception requise	Non	Indique si le document Accusé de réception doit être conservé dans le magasin d'irréfutabilité.	Limité au protocole ou à la connexion	Oui

Tableau 114. Attributs ebMS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Accusé de réception demandé	Non	Les valeurs possibles sont toujours, parMessage, et jamais. S'il est défini sur “toujours,” alors, lors de l'envoi d'un document ebMS, une demande d'accusé de réception sera faite en plaçant un élément acknowledgmentRequested dans le document ebMS SOAP. Pour l'expéditeur, "parMessage" et "jamais" signifie "Non." Lors de la réception d'un document ebMS, si la valeur est définie sur "toujours", le document entrant doit demander un accusé de réception, sinon il échoue. Si la valeur est définie sur “parMessage” sur le concentrateur du récepteur, il n'y aura pas d'échec du document, que celui-ci demande un accusé de réception ou non. Si la valeur est définie sur “jamais”, le message entrant ne doit alors jamais demander d'accusé de réception.		jamais
Signature d'accusé de réception demandée	Non	Les valeurs possibles sont toujours, parMessage, et jamais. “toujours” désigne une demande d'accusé de réception signé. "parMessage" et "jamais" signifie qu'il peut y avoir une demande d'accusé de réception non signé. Cet attribut fonctionne conjointement avec l'attribut “AccuséderéceptionDemandé”. Si la valeur de l'attribut AccuséderéceptionDemandé est défini sur “parMessage” ou “jamais”, alors ce dernier ne sera pas pris en compte. . S'il n'y a pas de valeur, alors “jamais” sera utilisé. Cet attribut n'est utilisé que pour l'envoi de document. Cet attribut n'est pas utilisé pour un document reçu.		jamais
Acteur	Non	Cet attribut n'a pas besoin d'être défini dans l'implémentation d'ebMS 2.0. L'attribut acteur est nécessaire lorsqu'un accusé de réception sync est nécessaire. l est placé dans le document ebMS SOAP. La spécification ebMS 2.0 suggère une valeur constante http://schemas.xmlsoap.org/soap/actor/next pour cet attribut (par défaut). Il est pris en compte et l'utilisateur n'a pas à définir cette valeur d'attribut. Il est laissé pour être utilisé dans une future implémentation.		http://schemas.xmlsoap.org/soap/actor/next

Tableau 114. Attributs ebMS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Compression obligatoire	Non	Les valeurs possibles sont “Oui” et “Non.” Si les charges ebMS doivent être compressées, la valeur doit être définie sur “Oui.” Si la compression n'est pas nécessaire, ne définissez rien ou spécifiez la valeur “Non.”		Non
Elimination de doublon	Non	Lors de l'envoi d'un message ebMS, si cette valeur d'attribut est définie sur "toujours," cela placera un élément DuplicateElimination dans le document ebMS SOAP. Cet élément DuplicateElimination dans le document ebMS SOAP indique que le concentrateur de réception ne doit pas transmettre les charges ebMS vers le système dorsal si le document ebMS est un double. **Remarque :** Pour un document SOAP, les valeurs "parMessage" et "jamais"ne seront pas placées dans l'élément DuplicateElimination. Lors de la réception d'un document ebMS, si la valeur est définie sur "toujours," alors, l'élément DuplicateElimination doit être dans le document ebMS SOAP, sinon cela provoquera un échec du document. Si la valeur définie est "parMessage" et que l'élément duplicateElimination est défini dans le document reçu, la double vérification doit être effectuée. Pour un document ebMS reçu, si la valeur d'attribut est "toujours" et si l'élément DuplicateElimination est présent, le document sera vérifié pour voir s'il s'agit d'un double. Si le document est un double, il échouera. Pour la valeur "jamais", si l'élément DuplicateElimination figure dans le document SOAP, le document échouera. S'il n'y a pas de valeur, alors “jamais” sera utilisé.		jamais
Constituant de chiffrement	Non	La valeur de cet attribut doit être une liste dont le type de contenu est séparé par un point virgule pour les charges, par exemple application/xml;text/xml; application/binary:application/edi provoquera le chiffrement des charges avec ce type de contenu. Cet attribut n'est utilisé que si la valeur d'attribut “Chiffrement obligatoire” est définie sur “Oui.”		application/ xml;text/xml; application/ EDI-X12; application/ EDI-CONSENT; application/ EDIFACT; application/ binary; application/ octet-stream

Tableau 114. Attributs ebMS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Paramètre Mime de chiffrement	Non	Un attribut facultatif utilisé pour placer des paramètres supplémentaires en tant qu'en-têtes MimeMultipart dans le document chiffré. S'appliquera à chaque charge chiffrée. Exemple de valeur : smime-type="enveloped-data" ou type="text/xml" version="1.0." Cet attribut n'est utilisé que si la valeur d'attribut "Chiffrement obligatoire" est définie sur "Oui."		Pas de valeur par défaut. **Remarque :** Cette variable n'est pas utilisée dans l'implémentation actuelle. Sa définition n'a pas d'effet lors de l'exécution.
Type Mime de chiffrement	Non	Non utilisé dans l'implémentation en cours.		Pas de valeur par défaut.
Chiffrement obligatoire	Non	Les valeurs possibles sont "Oui" et "Non." Si la valeur sélectionnée est "Oui", les charges seront chiffrées. Cet attribut est associé au "Constituant de chiffrement.". **Remarque :** Si la valeur d'attribut "Chiffrement requis" est définie sur "Oui" et qu'aucun type de contenu n'est configuré pour le "Constituant de chiffrement,", alors rien ne sera chiffré.		
Transformation de chiffrement	Non	Non utilisé dans l'implémentation en cours.		Pas de valeur par défaut. **Remarque :** Cette variable n'est pas utilisée dans l'implémentation actuelle. Sa définition n'a pas d'effet lors de l'exécution.
Exclure de la Signature	Non	La valeur de cet attribut doit être une liste dont le types de contenu est séparé par un point virgule, par exemple `application/binary;application/octet-stream`. Les charges ayant ce type de contenu ne seront pas incluses dans la signature. Cet attribut n'est utilisé que si la valeur d'attribut "Signature numérique obligatoire" est définie sur "Oui."		Sans entrée, la signature s'appliquera à toutes les charges.
Fonction de hachage	Non	L'algorithme de hachage qui doit être utilisé dans la signature XML lors du hachage des charges pendant la signature. Cet attribut n'est utilisé que si la valeur d'attribut "Signature numérique obligatoire" est définie sur "Oui." Seul SHA1 est pris en charge comme algorithme de hachage pour ebMS. Même si un autre algorithme de hachage est défini dans la connexion pour les documents ebMS, c'est SHA1 qui est utilisé comme algorithme de hachage.		SHA1

Tableau 114. Attributs ebMS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Sémantique de commande de message	Non	Les valeurs possibles sont “Garanti” et “NonGaranti”. Lors de l'envoi d'un document, si la valeur est définie sur “Garanti” alors un élément de Commande de message sera placé dans le document SOAP. Le concentrateur de réception en identifiant cet élément dans le document SOAP, s'assurera que les charges sont livrées au système dorsal dans l'ordre. Pour un document reçu, si cet attribut est défini sur “Garanti” alors le document ebMS entrant doit contenir un élément MessageOrder et s'il est manquant, le document échouera et un message d'erreur avec le CodeErreur “Incohérent” sera envoyé au partenaire.		NonGaranti
Rôle	Non	Lors de l'envoi d'un document ebMS, cette valeur d'attribut existe en tant que valeur d'élément de rôle dans le document SOAP ebMS. Lors de la réception d'un ebMS, cette valeur d'attribut est comparée à la valeur d'élément de rôle dans le document SOAP ebMS et si les valeurs ne correspondent pas (même si la valeur d'attribut est vide), alors le document échouera et un message d'erreur avec le CodeErreur “Incohérent” est envoyé au partenaire.		Pas de valeur par défaut.
Durée de conservation	Non	La durée en minutes pendant laquelle le document doit être conservé, par exemple 1440 pendant 24 heures. Lors de l'envoi d'un document, la Durée de conservation est utilisée pour calculer la Durée de vie à l'aide de la formule : Durée de vie = Durée de conservation + (no. de relances* IntervalleRelances). Lors de la réception d'un document, la Durée de conservation est utilisée pour effectuer l'élimination des doubles. Si un document avec un ID de Message Double est reçu, on vérifie si la Durée de conservation pour le document précédent est écoulée ou non. Si la durée de conservation n'est pas écoulée, le document est marqué comme double, sinon le document n'est pas marqué comme double. S'il n'y a aucune entrée, alors la valeur par défaut est 0.		0

Tableau 114. Attributs ebMS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Constituant d'empaquetage	Non	Non utilisé dans l'implémentation en cours.		Pas de valeur par défaut. **Remarque :** Cette variable n'est pas utilisée dans l'implémentation actuelle. Sa définition n'a pas d'effet lors de l'exécution.
Paramètre Mime d'empaquetage	Non	Non utilisé dans l'implémentation en cours.		Pas de valeur par défaut. **Remarque :** Cette variable n'est pas utilisée dans l'implémentation actuelle. Sa définition n'a pas d'effet lors de l'exécution.
Algorithme de chiffrement	Oui lorsque la valeur d'attribut “Chiffrement obligatoire” est définie sur “Oui.”	L'algorithme est utilisé pour chiffrer les charges. Cette valeur fonctionne en conjonction avec l'attribut "Protocole de chiffrement". Cet attribut n'est utilisé que si la valeur d'attribut “Chiffrement obligatoire” est définie sur “Oui.”		AES-128
Protocole de chiffrement	Non	Protocole utilisé pour chiffrer les charges. Les valeurs possibles sont ChiffrementXML et SMIME. Cet attribut n'est utilisé que si la valeur d'attribut "Chiffrement obligatoire" est définie sur "Oui." Si Chiffrement obligatoire est défini sur "oui" et qu'aucune valeur n'est fournie pour cet attribut, le document échouera.		ChiffrementXML
Intervalle de relance	Non	Pour un document envoyé, il s'agit de l'intervalle de temps en minutes pour un accusé de réception avant le renvoi d'un document ebMS. Les documents ebMS ne sont renvoyés que lorsqu'un accusé de réception est requis mais qu'il n'a pas été reçu du partenaire dans l'intervalle de relance. Une valeur de 0 indique qu'il n'y a pas de relances. Cet attribut fonctionne en conjonction avec l'attribut “Nombre de relances”.		270

Tableau 114. Attributs ebMS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Algorithme de signature	Oui si "Signature numérique obligatoire" est sur Oui	Algorithme utilisé pour signer le document. Cet attribut n'est utilisé que si la valeur d'attribut “Signature numérique obligatoire” est définie sur “Oui.” **Remarque :** Dans ebMS, hmac-sha1 n'est pas pris en charge.		dsa-sha1
Transformation de signature	Non	Il s'agit de l'algorithme de transformation utilisé pour transformer les charges avant de créer la signature XML. Cet attribut n'est utilisé que si la valeur d'attribut “Signature numérique obligatoire” est définie sur “Oui.”		Pas de valeur par défaut.
Mode de Réponse synchronisé	Non	Il s'agit du type de réponse synchrone obligatoire pour le document qui est envoyé. Si la valeur est définie en tant que : • **MSHSignalsOnly** - Seuls l'accusé de réception MSH / documents d'erreur seront envoyés sur une connexion synchrone. La réponse commerciale et les documents de signal commercial seront renvoyés de manière asynchrone. • **signalsOnly** – Seuls les documents de signal commercial et les documents MSH seront envoyés sur une connexion synchrone. La réponse commerciale sera renvoyée de manière asynchrone. • **responseOnly** – Seules les réponses commerciales et les documents MSH seront envoyés sur une connexion synchrone. Les documents de signal commercial ne seront pas renvoyés. • **signalsAndResponse** - Les réponses commerciales et documents de signaux commerciaux seront envoyés sur une connexion synchrone. • **Aucun** – Aucun document de réponse synchrone provenant du récepteur.		Néant
Vérification intelligible obligatoire	Non	La valeur de cet attribut est envoyée au système dorsal en tant que valeur d'en-tête “x-aux-IntelligibleCheckRequired”. Les valeurs possibles sont “oui” et “non.” L'objectif est d'indiquer au système dorsal que l'AccusédeRéception ne doit être envoyé que si le document ebXML avec les charges ne contient pas d'erreur. C'est au système dorsal d'interpréter cette valeur.		Non
Méthode de Canonicalisation	Non	Algorithme de Canonicalisation utilisé avant de réaliser une signature XML. Cet attribut n'est utilisé que si la valeur d'attribut “Signature numérique obligatoire” est définie sur “Oui.”		COMMENTAIRES _INCLUS

Tableau 114. Attributs ebMS (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Constituant de compression	Non	Liste des types de contenu de charges séparés par un point-virgule qui doivent être compressés. Par exemple, si les charges avec le TypeContenu “text/xml” et “application/edi” doivent être compressées, alors la valeur de cet attribut sera “text/xml;application/edi”. Aucune entrée signifie qu'aucune charge ne sera compressée, même lorsque “Compression obligatoire” est définie sur “Oui.” Cet attribut n'est utilisé que si la valeur d'attribut “Compression obligatoire” est définie sur “Oui.”		application/xml; text/xml;application/EDI-X12; application/EDI-CONSENT; application/EDIFACT
Type de service	Oui si la valeur de l'élément Service (Type de document) n'est pas un URI	Pendant l'envoi d'un document ebMS, la valeur d'élément ebMSService dans le message SOAP ebMS doit être soit un URI, soit une chaîne. S'il s'agit d'une chaîne, ce type d'attribut est obligatoire. Si la valeur Service (Type de document) n'est pas un URI, alors cette valeur d'attribut Type de service est utilisée comme valeur de type d'attribut dans le document ebMS.		Pas de valeur par défaut.

attributs généraux

Cette section apporte des informations sur les attributs généraux.

Tableau 115. attributs généraux

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Mappe de validation	Non	Il s'agit de la mappe de validation utilisée pour valider ce document. L'action qui est utilisée pendant l'exécution doit avoir une étape de validation qui utilise cet attribut. Seules les mappes de validation qui ont été téléchargées et associées à ce type de document pourront être sélectionnées.	Limité au protocole ou à la connexion	Pas de valeur par défaut.
Attribut utilisateur 1	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User01 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.
Attribut utilisateur 2	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User02 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.

Tableau 115. attributs généraux (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Attribut utilisateur 3	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User03 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.
Attribut utilisateur 4	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User04 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.
Attribut utilisateur 5	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User05 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.
Attribut utilisateur 6	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User06 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.
Attribut utilisateur 7	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User07 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.
Attribut utilisateur 8	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User08 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.

Tableau 115. attributs généraux (suite)

Attribut	Obligatoire	Description	Restrictions	Valeur par défaut
Attribut utilisateur 9	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User09 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.
Attribut utilisateur 10	Non	S'utilise dans les sorties définies par l'utilisateur. La valeur est déterminée par le créateur de la sortie définie par l'utilisateur. Elles seront définies dans l'Objet Document Commercial ayant l'attribut bcg.ro.user.User10 soit en tant que préfixe d'Origine (document source) ou de Destination (Document cible).		Pas de valeur par défaut.

Attributs OpenPGP

Après avoir créé une connexion entre des partenaires externe et interne, définissez les attributs de connexion comme décrit dans cette rubrique.

Dans la page **Gérer les connexions**, après avoir activé une connexion, cliquez sur **Attributs** du côté cible des fonctions business-to-business pour définir les valeurs des attributs de connexion spécifiques à OpenPGP.

Les différents attributs de connexion OpenPGP sont les suivants :

Tableau 116. Attributs OpenPGP

Attribut	Obligatoire	Description	Valeur par défaut
Utiliser le format OpenPGP	Oui	Définissez le côté cible des fonctions business-to-business dans la page Gérer les connexions sur "Oui" pour utiliser le format OpenPGP.	Pas de valeur par défaut.
Chiffrement obligatoire	Facultatif	Vous pouvez utiliser cet attribut pour chiffrer les charges. Pour chiffrer les charges, définissez la valeur sur "Oui".	Pas de valeur par défaut.
Préférence d'algorithme symétrique	Obligatoire	Cet attribut est l'algorithme de clé à utiliser de préférence pour le chiffrement OpenPGP. Dans la liste déroulante, sélectionnez la préférence pour l'algorithme symétrique. Lorsque l'attribut **Chiffrement obligatoire** est défini sur vrai, il est obligatoire de définir cet attribut.	Pas de valeur par défaut.
Détection des modifications	Facultatif et sélectionné uniquement avec le chiffrement	Si vous voulez imposer un contrôle d'intégrité des messages, définissez cet attribut sur vrai. Ce paramètre vérifie si le message a été ou non altéré pendant la transmission.	Pas de valeur par défaut.
Compression obligatoire	Facultatif	Vous pouvez utiliser cet attribut pour compresser les charges. Définissez cet attribut sur Oui pour qu'il y ait compression.	Pas de valeur par défaut.

Tableau 116. Attributs OpenPGP (suite)

Attribut	Obligatoire	Description	Valeur par défaut
Préférence pour l'algorithme de compression	Obligatoire	Cet attribut est l'algorithme de compression préféré pour OpenPGP. Dans la liste déroulante, sélectionnez l'algorithme de compression préféré. Lorsque l'attribut **Compression obligatoire** est défini sur vrai, il est obligatoire de définir cet attribut.	Pas de valeur par défaut.
Armor	Facultatif	OpenPGP code les données en ASCII Armor. Des en-têtes spécifiques sont placés autour des données encodées avec Radix-64, de façon à ce qu'OpenPGP puisse reconstruire les données par la suite. ASCII Armor est aussi utilisé pour protéger des données binaires brutes lorsqu'elles sont transférées à travers la connexion. Si vous définissez ce paramètre sur vrai du côté cible de la connexion, la conversion en Armor est réalisée lors de l'empaquetage du document. La définition d'une valeur pour cet attribut est facultative.	Pas de valeur par défaut.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

IBM® World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032
Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales :LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE, EXPLICITE OU IMPLICITE, IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Burlingame Laboratory Director
IBM Burlingame Laboratory
577 Airport Blvd., Suite 800
Burlingame, CA 94010
Etats-Unis

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

COPYRIGHT

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Documentation sur l'interface de programmation

Les informations relatives aux interfaces de programmation, lorsqu'elles sont disponibles, ont pour objet de vous aider à créer des applications à l'aide de ce programme. Les interfaces de programmation génériques vous permettent de créer des logiciels d'application qui obtiennent les services des outils de ce programme. Toutefois, ces informations peuvent également contenir des informations relatives aux diagnostics, aux modifications et à l'optimisation efectués. Ces informations sont mises à votre disposition pour vous permettre de résoudre les incidents liés à vos applications.

Avertissement : N'utilisez pas les informations relatives aux diagnostics, aux modifications et à l'optimisation comme une interface de programmation dans la mesure où elles sont susceptibles d'être modifiées.

Marques commerciales et marques de service

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

IBM	DB2	IMS	MQIntegrator	Tivoli
le logo 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 et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

MMX, Pentium et ProShare sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays.

Solaris, Java et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans d'autres pays.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

WebSphere Partner Gateway Enterprise Edition et Advanced Edition incluent un logiciel développé par le projet Eclipse (www.eclipse.org)

Index

Nombres

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z