IBM WebSphere Partner Gateway Enterprise et Advanced Editions

Guide de configuration du concentrateur

Version 6.0

IBM WebSphere Partner Gateway Enterprise et Advanced Editions

Guide de configuration du concentrateur

Version 6.0

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant dans l'Annexe E, «Remarques», à la page 313.

juin 2005

Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50

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.

A propos de ce manuel

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

A qui s'adresse ce manuel

Ce document s'adresse à la personne chargée de configurer le serveur WebSphere Partner Gateway, également appelé concentrateur. Pour pouvoir configurer le concentrateur, vous devez en être l'administrateur. L'administrateur du concentrateur est habilité à utiliser l'ensemble des fonctions de la Console de communauté de WebSphere Partner Gateway pour configurer et exploiter le concentrateur.

Conventions typographiques

Ce document obéit aux conventions ci-dessous.

Tableau 1. Conventions typographiques

Convention	Description
`Police de caractères à espacement unique`	Cette police désigne un texte à saisir, des valeurs d'arguments ou des options de commande, des exemples et exemples de codes, ou des informations affichées à l'écran (messages textuels ou invites).
gras	La mise en gras désigne des éléments d'interfaces tels que noms de boutons, noms de menus ou options de menus, ainsi que les en-têtes de colonnes des tableaux et textes.
italique	L'italique désigne des éléments sur lesquels on souhaite attirer l'attention, les titres de manuels, des termes nouveaux ou qui seront définis par la suite, des noms de variables ou des lettres de l'alphabet utilisées en tant que lettres.
`Police en italique à espace simple`	Une police en italique et à espace simple est utilisée pour les noms des variables dans un texte écrit dans une police à espace simple.
ProductDir	*ProductDir* représente le répertoire d'installation du produit. Tous les noms de chemins du produit IBM WebSphere Partner Gateway sont relatifs au répertoire dans lequel IBM WebSphere Partner Gateway est installé sur le système.
`%texte%` et *`$texte`*	Le texte placé entre des signes de pourcentage (%) indique la valeur de la variable système ou utilisateur `text` de Windows. La notation équivalente dans un environnement UNIX est $ *texte* , ce qui indique la valeur de la variable d'environnement *texte* d'UNIX.
Texte en couleur souligné	Un texte en couleur souligné indique une référence croisée. Cliquez sur le texte pour consulter l'objet de la référence.
Texte encadré en bleu	(Documents PDF uniquement) Un cadre autour d'un texte désigne une référence croisée. Cliquez sur le texte encadré pour accéder à l'objet de la référence. Cette convention est l'équivalent pour fichiers PDF du "Texte en couleur souligné" également indiqué dans ce tableau.

Tableau 1. Conventions typographiques (suite)

Convention	Description
“ “ (guillemets)	(Fichiers PDF uniquement) Des guillemets entourent les références croisées vers d’autres sections du document.
{ }	Dans une ligne de syntaxe, des accolades entourent un ensemble d’options parmi lesquelles vous ne devez en choisir qu’une seule.
[ ]	Dans une ligne de syntaxe, des crochets encadrent les paramètres facultatifs.
< >	Des crochets en chevron entourent les éléments variables d’un nom pour les distinguer les uns des autres. Par exemple, <*nom_serveur*><*nom_connecteur*>tmp.log.
/, \	Des barres obliques inverses (\) servent de séparateurs dans les chemins d’accès aux répertoires, dans les installations Windows. Pour les installations UNIX, les barres obliques normales (/) remplacent les barres obliques inverses.

Documents connexes

La documentation fournie avec ce produit comporte des informations détaillées sur l’installation, la configuration, l’administration et l’utilisation de WebSphere Partner Gateway Enterprise et Advanced Edition.

Vous pouvez télécharger la documentation ou la lire directement à partir du site http://www.ibm.com/software/integration/wspartnergateway/library/infocenter

Remarque : Des informations importantes relatives à ce produit peuvent être également disponibles dans les notes techniques et les flashs du support technique, diffusés après la publication de ce document. Celles-ci sont disponibles sur le site Web WebSphere Business Integration Support, à l’adresse http://www.ibm.com/software/integration/wspartnergateway/support/. Sélectionnez la zone qui vous intéresse et explorez les sections Technotes et Flashes.

Nouveautés de cette version

Nouveautés de l'édition 6.0

Les nouveautés de WebSphere Partner Gateway (appelé WebSphere Business Integration Connect dans les précédentes éditions) sont les suivantes :

- Capacité de désenvelopper des transactions EDI, de les valider et de les transformer dans ces enveloppes
- Capacité d'envelopper des transactions EDI séparées avant de les livrer
- Capacité de recevoir dans un même fichier plusieurs documents ROD (record-oriented-data oriented data) et XML, ou des EDI, et de les séparer en documents ou EDI individuels
- Capacité de réaliser des conversions entre toute combinaison de documents ROD, XML et EDI
- Introduction d'un nouveau transfert (script FTP) pouvant être utilisé à la fois pour des cibles et des passerelles, afin de communiquer avec les réseaux VAN (Value Added Networks) ainsi que d'autres serveurs FTP
- Capacité de prendre en charge plus d'un certificat pour certaines fonctions, afin qu'en cas d'expiration du certificat principal, le certificat secondaire puisse être utilisé
- Capacité d'envoyer des documents depuis une passerelle HTTP ou HTTPS à des participants, via un serveur proxy

Il convient de noter que WebSphere Partner Gateway version 6.0 ne prend pas en charge l'algorithme RC5.

Nouveautés de la version 4.2.2

La version 4.2.2 est la première du *Guide de configuration du concentrateur*.

Chapitre 1. Introduction

Après avoir installé WebSphere Partner Gateway et pour permettre l'échange de documents entre le Gestionnaire de communauté et les participants, vous devez configurer le serveur WebSphere Partner Gateway (c'est-à-dire le concentrateur).

Ce chapitre contient les rubriques suivantes :

Vue d'ensemble

Le but de cette opération est de permettre au Gestionnaire de communauté d'échanger un ou plusieurs documents (par voie électronique) avec un participant. 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 le participant sont généralement dans un format standard, et représentent une interaction métier spécifique. Par exemple, le participant peut envoyer un bon de commande sous forme d'un PIP RosettaNet 3A4, 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 Gestionnaire de communauté. De la même façon, une application dorsale du Gestionnaire de communauté peut envoyer une réponse au bon de commande dans son propre format personnalisé, qui sera transformé dans un format standard. Le document transformé est ensuite envoyé au participant.

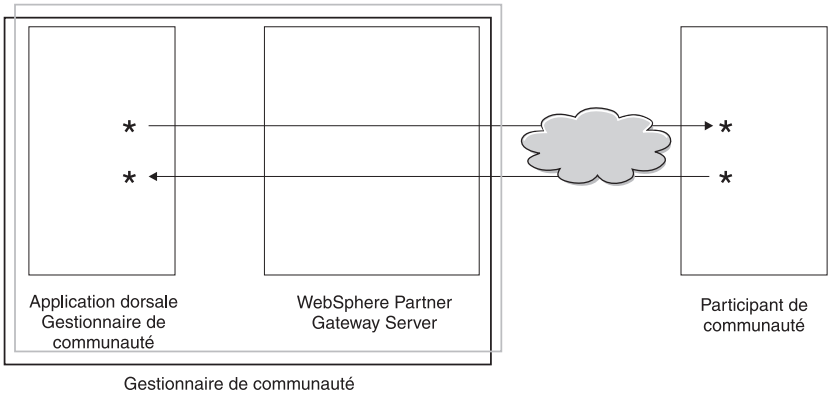

Figure 1. Circulation des documents via le concentrateur

Dans ce guide, vous découvrirez comment configurer le concentrateur et les participants. Vous apprendrez également comment configurer les paramètres de sécurité pour le concentrateur.

Notez sur la figure 1, à la page 1 que le serveur WebSphere Partner Gateway et l'application dorsale du Gestionnaire de communauté appartiennent au Gestionnaire de communauté. Le Gestionnaire de communauté est la société qui possède le concentrateur, mais il en est également l'un des participants. Comme vous le verrez dans les chapitres suivants, la méthode de définition d'un profil est la même pour le Gestionnaire de communauté que pour les participants.

Remarque : Ce document vous apprend à créer les connexions qui circulent de l'application dorsale du Gestionnaire de communauté vers la passerelle d'un participant et d'un participant vers la passerelle du Gestionnaire de communauté. Une fois les documents arrivés à la passerelle du Gestionnaire de communauté, 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 d'entreprise*.

Informations nécessaires à la configuration du concentrateur

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

- Quels types de documents (par exemple, EDI-X12 ou XML personnalisé) le Gestionnaire de communauté et ses participants enverront via le concentrateur ?
- Quels types de transfert (par exemple, HTTP ou FTP) le Gestionnaire de communauté et ses participants 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 ?
- 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 participants 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 Gestionnaire de communauté comme un type spécial de participant du concentrateur.

Vue d'ensemble des transferts

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

Remarque : Lors de l'utilisation d'un fichier-répertoire entre un participant 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 transferts. Les plus répandus entre le concentrateur et les applications dorsales sont HTTP, HTTPS, JMS et fichier-répertoire.

La figure 2 indique les différents transferts utilisables.

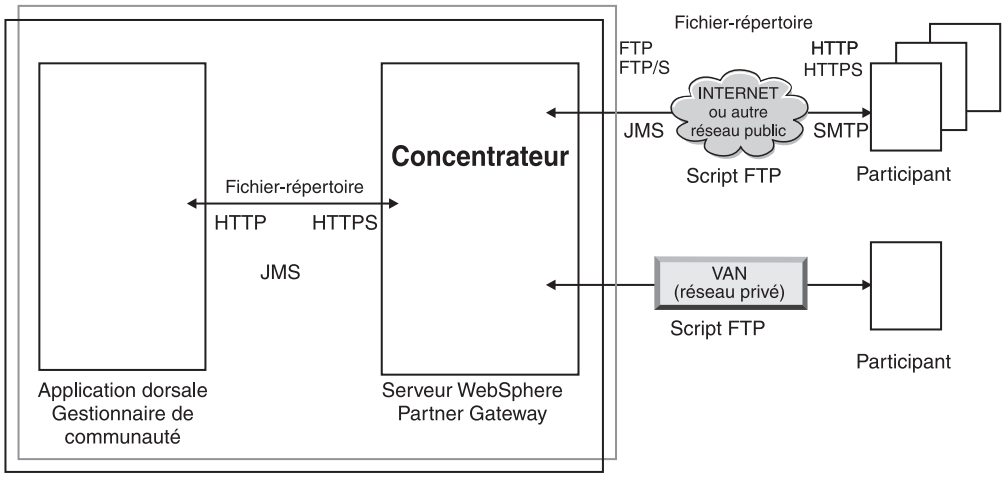

Figure 2. Transferts pris en charge par WebSphere Partner Gateway

Le type de transfert utilisé pour envoyer et recevoir des documents a des répercussions sur la définition des cibles et passerelles. Une cible est un point d'entrée dans le concentrateur, l'emplacement qui reçoit les documents envoyés par les participants ou les applications dorsales. Une passerelle est un point d'entrée dans l'ordinateur du participant ou le système dorsal, l'emplacement où le concentrateur envoie des documents. Avant d'utiliser les transferts FTP, FTPS, script FTP, JMS et fichier-répertoire, vous devez procéder à certains paramétrages décrits au Chapitre 2, «Etapes préalables à la configuration du concentrateur», à la page 19.

Vue d'ensemble des définitions de flot de documents

Lorsque vous définissez l'échange de documents entre les participants et le Gestionnaire de communauté, vous devez apporter quelques précisions concernant le document :

- Le *regroupement* qui entoure le document
- Le *protocole* métier qui définit le document
- Le type de *flot de documents*

Le regroupement et le protocole du document ainsi que le flot de documents constituent la *définition du flot de document*. La définition du flot de documents apporte des informations sur la façon de traiter le document. Prenons par exemple la définition de flot de documents suivante, fournie avec le système :

- Regroupement : AS
- Protocole : EDI-X12
- Flot de documents : ISA

Le concentrateur extrait les informations de l'en-tête AS (qui l'aident à identifier la source et la destination du document). Il sait rechercher dans le document des

informations, en fonction de leur position. Des attributs sont affectés aux trois parties de la définition du flot de processus. Vous pouvez modifier les attributs fournis par le système ou en ajouter.

Regroupement

Le regroupement fournit des informations concernant la transmission du document. Comme indiqué dans la précédente section, si le regroupement 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 participant envoie un PIP RosettaNet au Gestionnaire de communauté, le PIP est regroupé en tant que RNIF.

La figure 3 présente les types de regroupements pouvant être définis pour les documents échangés entre le concentrateur et un participant de la communauté, et entre le concentrateur et une application dorsale.

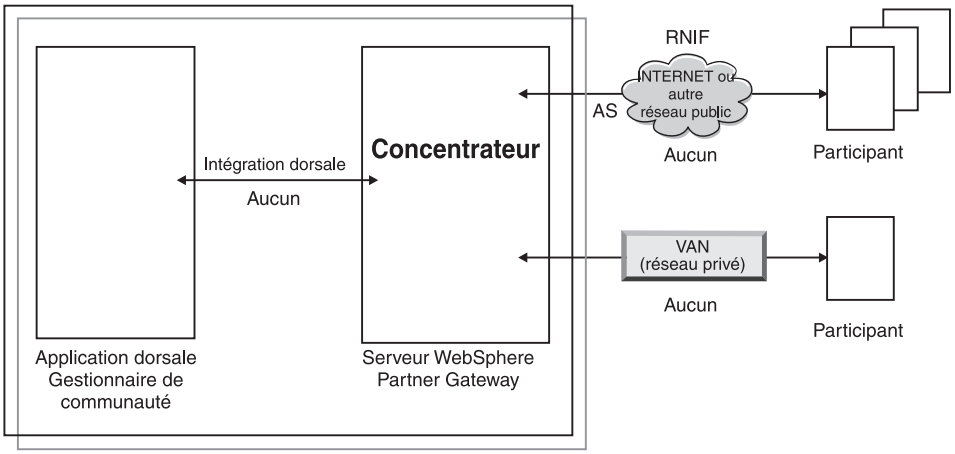

Figure 3. Types de regroupements de documents

Des regroupements sont associés à des protocole spécifiques. Par exemple, un participant doit préciser un regroupement 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 regroupement Intégration dorsale, 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 regroupement Intégration dorsale, elle doit ajouter des informations d'en-tête. Le regroupement d'Intégration dorsale et les conditions requises pour les informations d'en-tête sont décrites dans le *Guide d'intégration d'entreprise*.

AS : Le regroupement AS n'est disponible qu'entre les participants et le concentrateur. Le regroupement AS peut être utilisé pour les documents conformes aux standards AS1 ou AS2. 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. Les documents envoyés par un participant avec un regroupement AS sont accompagnés d'informations d'en-tête AS1 ou AS2. Les documents envoyés à un participant attendant des en-têtes AS1 ou AS2 doivent être regroupés (au niveau du concentrateur) en tant que AS.

Aucun : Le regroupement Aucun peut servir à échanger des documents entre le concentrateur et les participants, et entre le concentrateur et l'application dorsale. Aucune information d'en-tête n'est ajoutée (ou attendue) pour ce mode de regroupement.

Module RNIF : Le regroupement RNIF est fourni sur le support d'installation. Téléchargez le regroupement RNIF (ainsi que les PIP qui doivent être échangés) en appliquant la procédure décrite dans la section «Documents RosettaNet», à la page 68. Le regroupement RNIF sert à envoyer des documents RosettaNet du participant au concentrateur ou du concentrateur au participant.

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

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

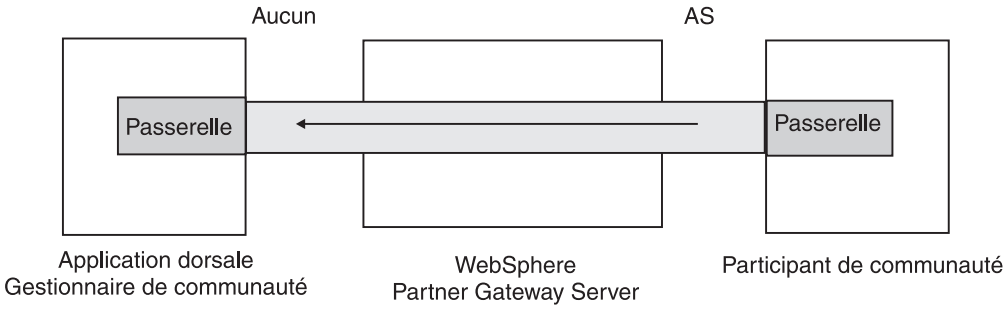

Figure 4. Connexion unidirectionnelle type

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 participant envoie un EDI au concentrateur à destination du Gestionnaire de communauté, cet EDI est désenveloppé et les transactions EDI individuelles sont traitées. Un regroupement est associé à l'EDI d'origine, lors de son envoi à partir du participant. Cependant, l'EDI proprement dit n'étant pas distribué au Gestionnaire de communauté (il est désenveloppé dans le concentrateur sans aucun autre traitement), le regroupement n'est pas nécessaire. Lorsque vous définissez l'interaction correspondant à l'étape de désenveloppement, précisez un regroupement du côté de l'émetteur mais indiquez N/A du côté du destinataire.

Le paramétrage des définitions de flots de documents dans le cadre d'un EDI est décrit au Chapitre 8, «Configuration des flots de documents EDI», à la page 91.

Protocoles

Les protocoles fournis avec le système sont les suivants :

- Binaire

  Le protocole Binaire peut être utilisé avec les regroupements AS, Aucun et Intégration dorsale. Un document binaire ne contient pas de données sur sa source ou sa destination.

- EDI-X12, EDI-Consent, EDI-EDIFACT

  Ces protocoles EDI peuvent être utilisés avec les regroupements AS ou Aucun. Comme indiqué dans la section «N/A», à la page 5, si la transaction ou l'EDI est émis par le concentrateur ou lui est destiné, indiquez N/A comme regroupement. Les standards d'EDI X12 et EDIFACT sont utilisés pour l'échange de données. EDI-Consent désigne les types de contenus autres que X12 ou EDIFACT.

- Service Web

  Les demandes de Service Web ne peuvent être utilisées qu'avec le regroupement Aucun.

- cXML

  Les documents cXML ne peuvent être utilisés qu'avec le regroupement Aucun.

- 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 le regroupement Intégration dorsale. Ce protocole est décrit dans le *Guide d'intégration d'entreprise*.

Lorsque vous téléchargez des regroupements RNIF, vous extrayez également les protocoles associés (RosettaNet et RNSC). RosettaNet (le protocole utilisé entre le participant et le concentrateur) est associé au regroupement RNIF. RNSC (le protocole utilisé entre le concentrateur et l'application dorsale du Gestionnaire de communauté) est associé au regroupement Intégration dorsale.

Pour les transactions EDI ou les documents XML ou ROD qui feront l'objet d'une transformation, importez la mappe de transformation à partir du client Data Interchange Services. Dans le client Data Interchange Services, les 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. 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, consultez le *Guide de mappage* ou l'aide en ligne fournie avec le client Data Interchange Services.

Remarque : Les ID de l'émetteur et du réceptionnaire 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. Vérifiez que le spécialiste de mappage client Data Interchange Services est au courant 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 «Création de documents XML personnalisés», à la page 86.

Flot de documents

Le document lui-même peut se présenter dans divers formats. Les flots de documents fournis par le système 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 flots de documents, en suivant la procédure décrite à la section «Création de documents XML personnalisés», à la page 86.

Vue d'ensemble 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.

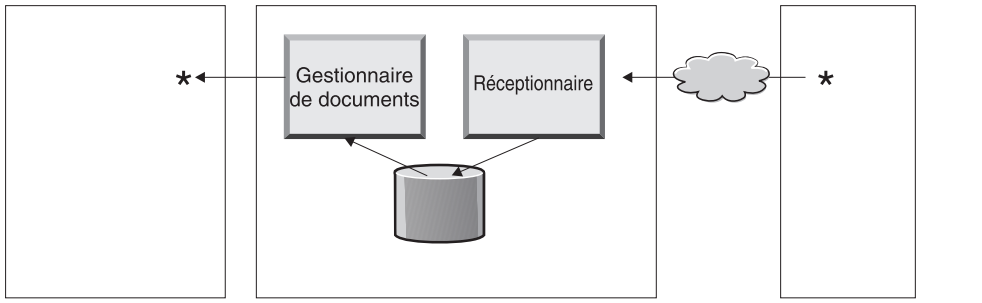

Figure 5. Composants du Réceptionnaire et du Gestionnaire de documents

La figure 5 montre comment un document est envoyé par un participant, reçu et traité par le concentrateur, puis envoyé à une application dorsale du Gestionnaire de communauté.

Remarque : Pour plus de clarté, le schéma montre un réceptionnaire 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. Consultez le *Guide d'installation* pour obtenir des informations sur les différentes topologies disponibles pour définir la passerelle WebSphere Partner Gateway.

Un document est reçu dans WebSphere Partner Gateway par le composant Réceptionnaire. Ce composant est chargé de surveiller le transfert 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 réceptionnaires sont spécifiques au transfert. Les instances de réceptionnaires spécifiques aux transferts sont appelées *cibles*. Vous devez définir une cible pour chaque type de transfert que le concentrateur devra gérer. Par exemple, s'il est prévu que des participants envoient des documents via HTTP, vous devez définir une cible HTTP pour pouvoir les réceptionner.

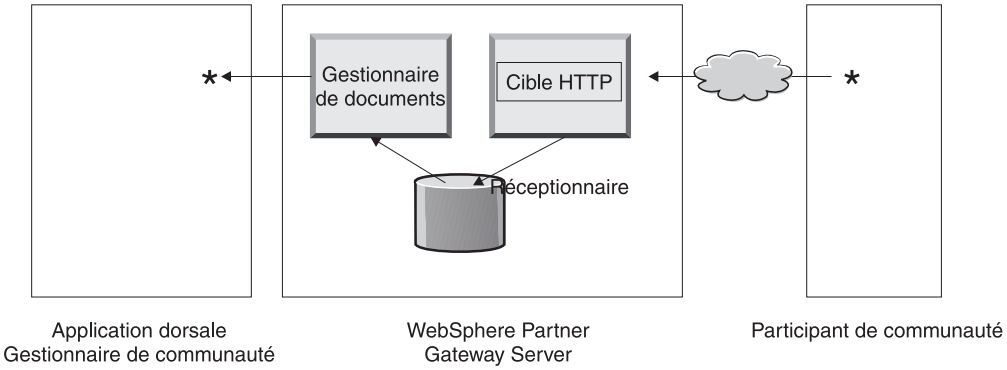

Figure 6. Cible HTTP

De la même façon, si l'application dorsale du Gestionnaire de communauté doit envoyer des documents via JMS, vous devez définir une cible JMS au niveau du concentrateur pour les réceptionner.

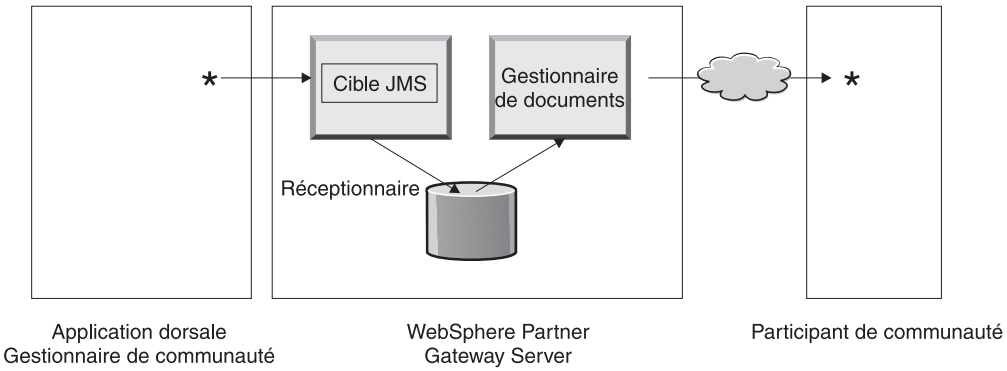

Figure 7. Cible JMS ;

Comme décrit au «Vue d'ensemble des transferts», à la page 2, WebSphere Partner Gateway Connect prend en charge divers modes de transferts, mais vous pouvez

télécharger un mode de transfert défini par l'utilisateur et l'utiliser pour définir une cible (voir procédure au «Configuration d'une cible pour un transfert défini par l'utilisateur», à la page 50).

Le Réceptionnaire 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), la cible 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 Gestionnaire de communauté peut envoyer un document EDI-X12 avec regroupement Aucun à destination du concentrateur, pour être livré à un participant qui attend un document EDI-X12 avec des en-têtes AS2. Le participant fournit l'URL HTTP où le document regroupé AS2 doit être envoyé, et le Gestionnaire de documents regroupe le document conformément aux attentes du participant. Pour envoyer le document au participant, le Gestionnaire de documents utilise la configuration de la passerelle pour ce participant (qui doit avoir été définie avec l'URL HTTP où le participant attend des documents AS2).

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

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 système des composants pour le traitement d'un document métier.

Pour modifier le comportement fourni par le système des cibles, passerelles, étapes de flux de travaux fixes et actions, vous utiliserez des *récupérateurs*. Il existe deux types de récupérateurs -- ceux fournis par WebSphere Partner Gateway et ceux définis par l'utilisateur. Pour plus d'informations sur la création des récupérateurs, voir le *Programmer Guide*.

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

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

Cibles

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

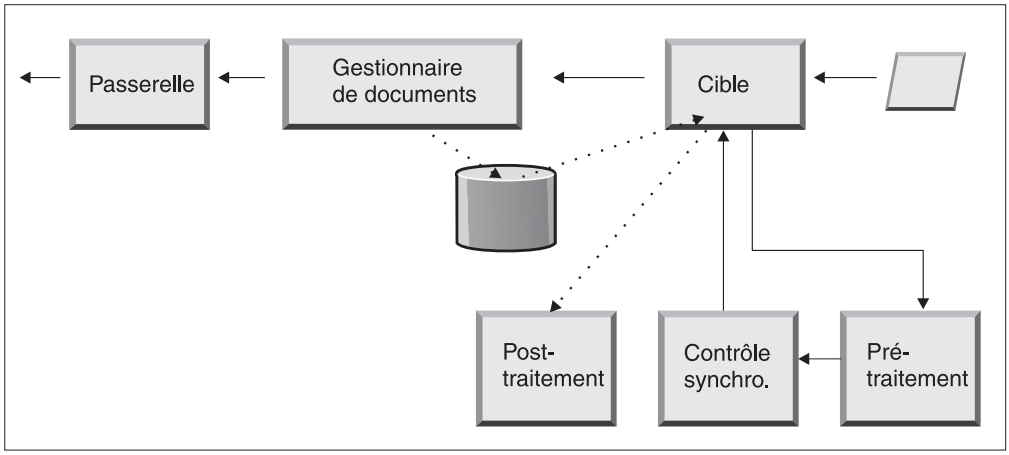

Figure 8. Points de configuration cible

La procédure s'exécute dans l'ordre suivant :

1. Une fois qu'il a reçu le document, le Réceptionnaire appelle les étapes Preprocess et SyncCheck.
2. Il appelle ensuite le Gestionnaire de documents pour traiter le document.
3. Dans le cas de flots synchrones, le Gestionnaire de documents apporte une Réponse synchrone. Le Réceptionnaire 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 récupérateur de fractionnement ROD lorsque vous définissez la cible. L'utilitaire de fractionnement ROD, ainsi que deux autres utilitaires de fractionnement fournis par le système vous sont proposés pour définir une cible. Si vous créez d'autres récupérateurs pour l'étape preprocess, ils sont également disponibles.

  Voir «Preprocess», à la page 51 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 un MDN (notification de disposition de message) de manière synchrone par la même connexion HTTP. WebSphere Partner Gateway propose plusieurs récupérateurs pour le contrôle synchrone. Leur liste dépend du transfert associé à la cible.

  SyncCheck s'applique uniquement aux transferts (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 des échanges synchrones, vous devez préciser le récupérateur SyncCheck associé sur la cible HTTP ou HTTPS.

  Voir «SyncCheck», à la page 54 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 55 pour obtenir des informations sur le paramétrage du point de configuration Postprocess.

Gestionnaire de documents

Les documents reçus par les cibles sont récupérés par le Gestionnaire de documents dans le système de fichiers commun, pour être traités. Le Gestionnaire de documents utilise les connexions du participant 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 participant est déterminée. Elle indique l'action à effectuer sur ce document. Après avoir effectué le flux de travaux variable, le Gestionnaire de documents effectue le flux de travaux fixe de communication sortante sur ce document.

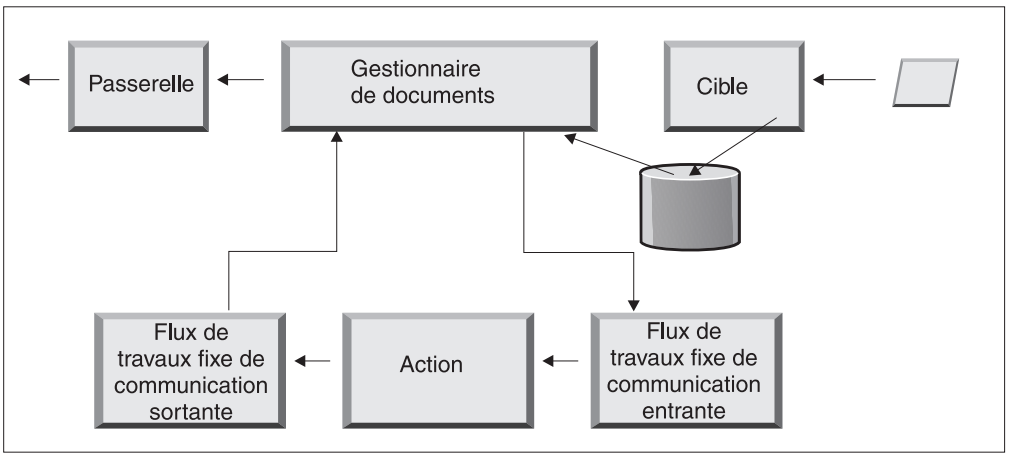

Figure 9. Flux de travaux fixe et actions

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

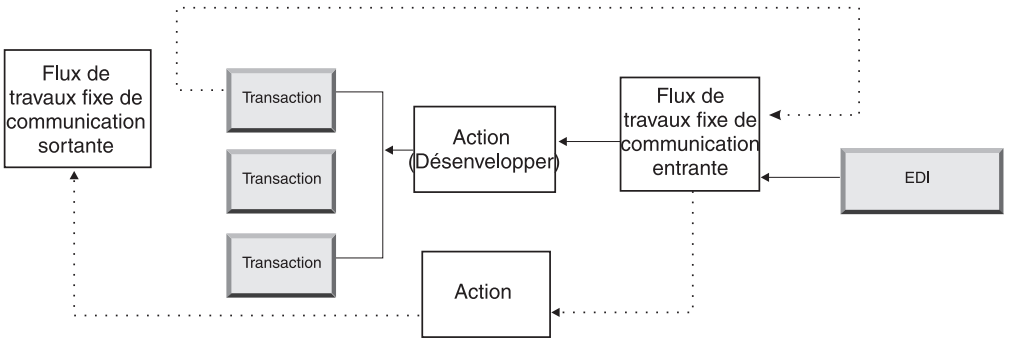

Figure 10. Flux de travaux fixe et actions pour un EDI

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 Réceptionnaire 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 récupérateurs 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 participant, 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 métier de l'expéditeur et du réceptionnaire 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.

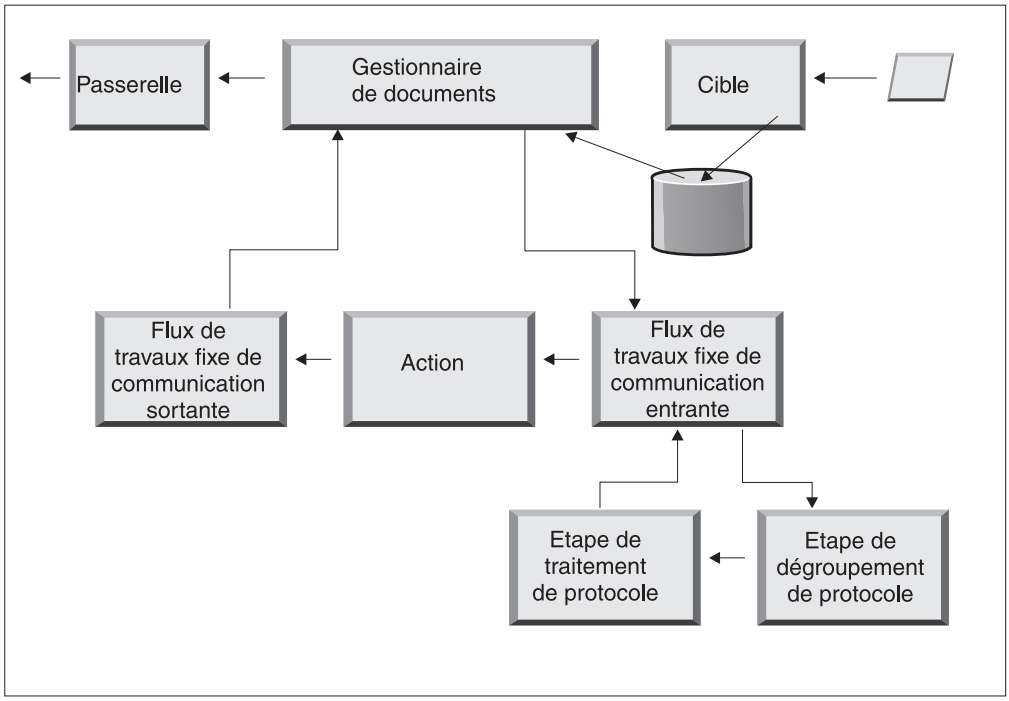

Figure 11. Flux de travaux fixe de la communication entrante

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 récupérateurs pour les regroupements RNIF, AS, Intégration dorsale et Aucun. Si des récupérateurs d'autres types sont nécessaires, vous pouvez les développer en tant qu'exits utilisateur. Consulter le *Programmer Guide* pour plus d'informations sur la programmation d'exits utilisateur.

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

Voir «Configuration des flux de travaux fixes», à la page 58 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 l'acheminement (telles que ID de l'émetteur et du réceptionnaire), sur le protocole et le flot de documents. WebSphere Partner Gateway peut traiter plusieurs protocoles, comme indiqué dans la section «Récupérateurs de traitement de protocole», à la page 59. 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 récupérateurs.

Voir «Configuration des flux de travaux fixes», à la page 58 pour obtenir des informations sur la configuration de cette étape.

Vous pouvez utiliser le récupérateur par défaut qui s'applique au protocole de votre document ou vous pouvez indiquer un autre récupérateur 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 système, qui n'applique aucune modification au document.

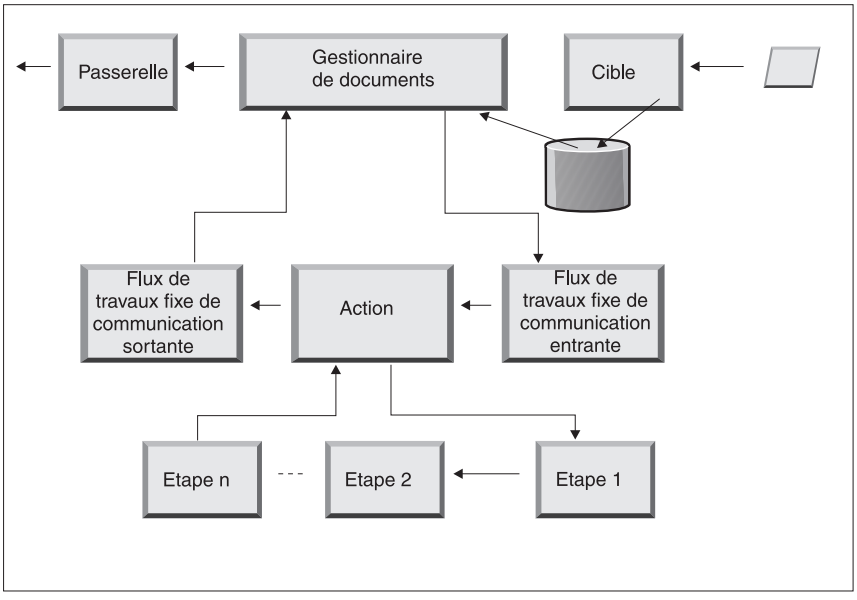

Figure 12. Etapes d'une action

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

Consultez la section «Configuration des actions», à la page 60 pour plus d'informations sur la création ou la copie d'une action fournie par le système, ainsi que sur la configuration d'une action définie par l'utilisateur.

Flux de travaux fixe de communication sortante

Le flux de travaux fixe de la communication sortante consiste en une seule étape, le regroupement 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 regroupement Intégration dorsale, certaines informations d'en-tête sont ajoutées au document avant qu'il soit transmis à la passerelle.

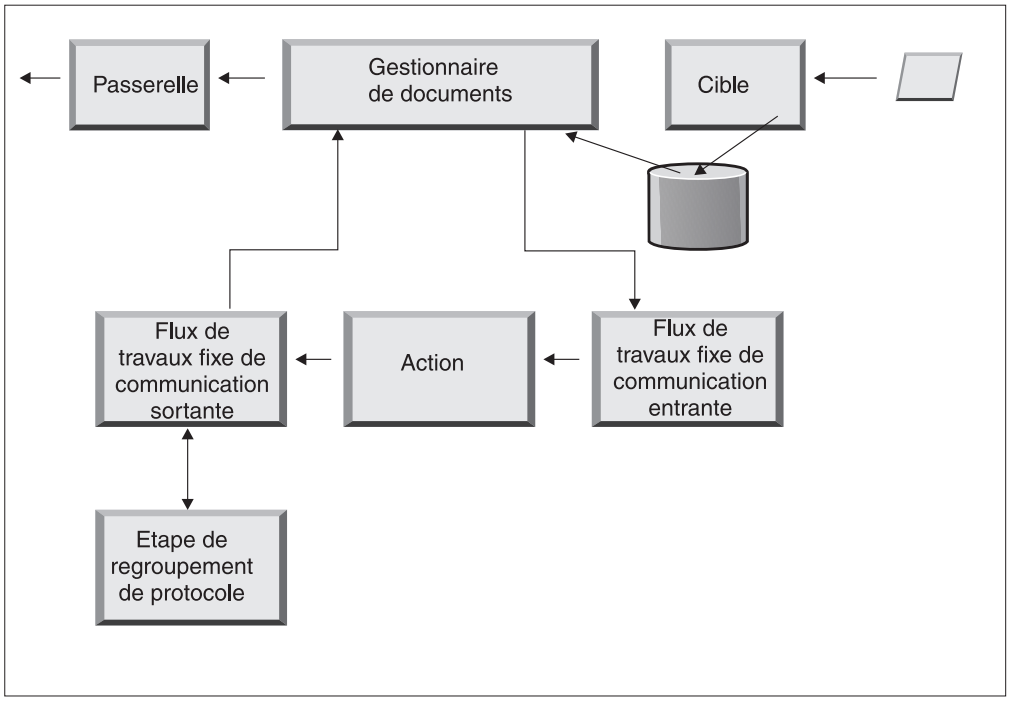

Figure 13. Flux de travaux fixe de la communication sortante

WebSphere Partner Gateway fournit des récupérateurs adaptés à divers regroupements et protocoles, indiqués dans la section «Flux de travaux de communication sortante», à la page 59. Si d'autres récupérateurs de regroupement 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 transfert spécifique au protocole métier

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

Voir «Configuration des flux de travaux fixes», à la page 58 pour obtenir des informations sur la configuration de cette étape du flux de travaux.

Passerelles

Après avoir quitté le Gestionnaire de documents, le document est envoyé au destinataire prévu à partir de la passerelle. La passerelle dispose de deux points de configuration — Preprocess et Postprocess.

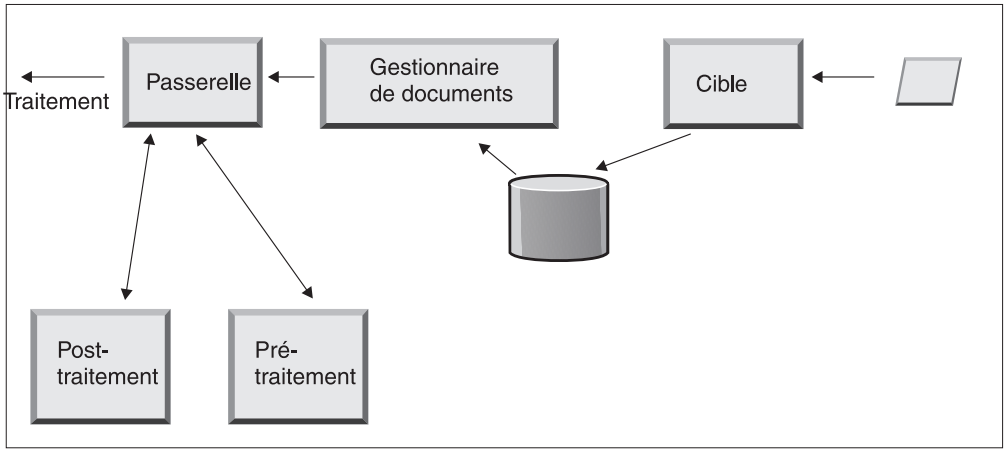

Figure 14. Points de configuration de la passerelle

- preprocess

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

Voir «Configuration de récupérateurs», à la page 151 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 la section «Informations nécessaires à la configuration du concentrateur», à la page 2, configurez le concentrateur et créez vos profils de participants. La présente section apporte des informations précises sur les tâches à effectuer.

Remarque : Lorsque vous configurez le concentrateur, consultez le *Guide de l'administrateur* pour obtenir des informations sur les codes d'événements et des conseils de dépannage.

Configuration du concentrateur

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 transferts utilisés. Cette procédure est décrite au Chapitre 2, «Etapes préalables à la configuration du concentrateur», à la page 19.
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 4, «Configuration de la Console de communauté», à la page 31.
3. Créez des cibles pour les types de transferts qui seront utilisés pour recevoir les documents sur le concentrateur. Cette procédure est décrite au Chapitre 5, «Définition des cibles», à la page 37.

   Remarque : Si vous prévoyez de configurer la cible avec des récupérateurs définis par l'utilisateur, vous devez les télécharger avant de créer la cible. Cette procédure est décrite à la section «Téléchargement de récupérateurs définis par l'utilisateur», à la page 38.
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 tel que fourni par le système, n'effectuez pas cette étape. Cette procédure est décrite au Chapitre 6, «Configuration des procédures et actions portant sur les flux de travaux fixes», à la page 57.

   Remarque : Vous devez télécharger les récupérateurs définis par l'utilisateur avant de configurer les flux de travaux et actions. Cette procédure est décrite à la section «Téléchargement de récupérateurs», à la page 57.
5. Créez des définitions de flots de documents (ou vérifiez que ceux dont vous avez besoin sont déjà disponibles) pour définir les types de documents reçus ou émis au niveau du concentrateur.
6. Créez des interactions pour indiquer la combinaison valide de deux définitions de flots de documents.

   La création de définitions de flots de documents et la création d'interactions sont décrites dans le Chapitre 7, «Configuration des flots de documents», à la page 63 et le Chapitre 8, «Configuration des flots de documents EDI», à la page 91.
7. Créez un profil pour le Gestionnaire de communauté, en fournissant des informations sur lui et en déterminant les types de documents qu'il peut envoyer et recevoir (ses capacités B2B). Cette procédure est décrite au Chapitre 9, «Création du profil du Gestionnaire de communauté et des capacités B2B», à la page 131.

Création de participants

Une fois que vous avez configuré le concentrateur, créez un profil pour chaque participant qui échangera des documents avec le Gestionnaire de communauté. Seul l'administrateur du concentrateur peut créer des participants.

En tant qu'administrateur du concentrateur, vous pouvez également paramétrer les capacités B2B des participants, établir leurs passerelles et configurer leurs profils de sécurité. Ces procédures peuvent être réalisées par les participants eux-mêmes.

Cette procédure est décrite au Chapitre 11, «Création de participants et de leurs capacités B2B», à la page 155. Cette procédure est décrite au Chapitre 10, «Création de passerelles», à la page 135. Cette procédure est décrite au Chapitre 13, «Configuration de la sécurité pour les échanges entrants et sortants», à la page 163.

Etablissement de connexions de documents

Une fois que vous avez configuré le concentrateur et créé des profils de participants, vous pouvez paramétrer des connexions. Les connexions indiquent les combinaisons valides d'émetteurs et réceptionnaires ainsi que les documents qu'ils peuvent échanger. Cette procédure est décrite au Chapitre 12, «Gestion des connexions», à la page 159.

Chapitre 2. Etapes préalables à la configuration du concentrateur

Dans les chapitres suivants, vous allez configurer les cibles et les passerelles décrites au Chapitre 1, «Introduction». Selon le types de transfert que vous envisagez d'utiliser pour recevoir les documents dans les cibles et les envoyer à partir des passerelles, vous devez exécuter certaines tâches de configuration.

Ce chapitre contient les rubriques suivantes :

- «Création d'un répertoire pour une passerelle fichier-répertoire»
- «Configuration du serveur FTP pour la réception de documents»
- «Configuration du concentrateur pour le protocole de transfert JMS», à la page 23

Il propose également une présentation rapide des scripts FTP exigés par les cibles et passerelles 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 de scripts FTP pour les passerelles et cibles de script FTP», à la page 25
- «Utilisation de mappes à partir du client Data Interchange Services», à la page 26

Si vous ne prévoyez pas de configurer ce type de cible ou de passerelle, passez directement au Chapitre 3, «Démarrage du serveur et affichage de la Console de communauté».

Création d'un répertoire pour une passerelle fichier-répertoire

Si vous envisagez d'utiliser une passerelle fichier-répertoire pour envoyer des documents au Gestionnaire de communauté, vous devez d'abord créer un répertoire dans le système de fichiers utilisé par le Gestionnaire de communauté.

Par exemple, supposons que vous vouliez créer un répertoire nommé PasserelleSystèmeFichiers dans le répertoire temporaire c:\temp d'une installation Windows. Voici comment procéder :

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

Configuration du serveur FTP pour la réception de documents

Remarque : Cette section concerne uniquement la réception de documents via FTP ou FTPS provenant de participants. L'envoi de documents à des participants est décrite dans «Configuration d'une passerelle FTP», à la page 140 et «Configuration d'une passerelle FTPS», à la page 146.

Si vous avez l'intention d'utiliser le protocole de transfert 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.

Configuration de la structure de répertoire requise sur le serveur FTP

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 répertoires précise pour permettre aux composants Réceptionnaire et Gestionnaire de documents d'identifier correctement le participant qui envoie le document entrant. La structure est décrite à la figure 15.

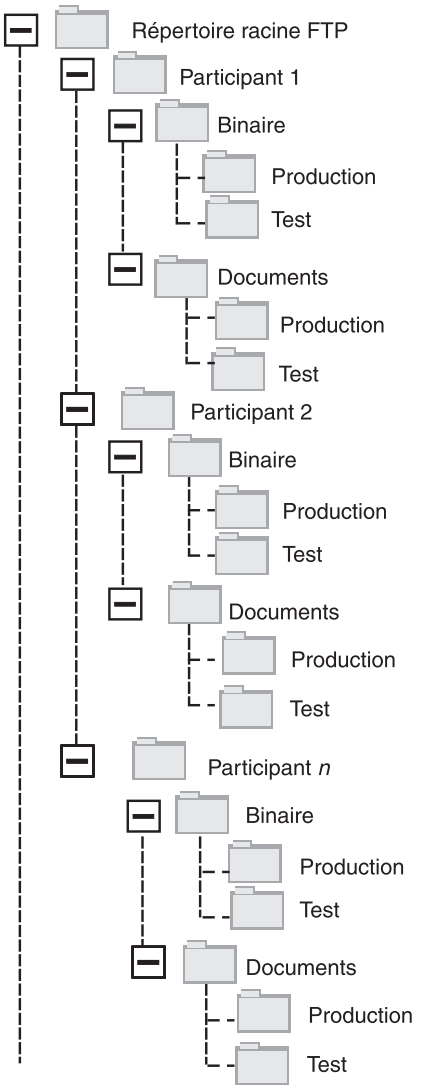

Figure 15. Structure de répertoire FTP

Le répertoire de chaque participant 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 participant envoie un document XML contenant des informations d'acheminement complètes (via FTP) vers le concentrateur. Il convient dans ce cas de créer une définition XML personnalisée.

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

Pour chaque participant appelé à envoyer ou recevoir des documents via FTP, vous devez créer les dossiers suivants à partir du répertoire racine de votre serveur FTP :

1. Créez un dossier pour chaque participant.

   Remarque : Le nom du dossier doit être identique à celui indiqué dans la zone **Nom de connexion de l'entreprise** lors de la création du participant. Cette procédure est décrite à la section «Création des profils des participants», à la page 155.
2. Sous ce dossier, créez les sous-dossiers `Binary` et `Documents`.
3. Sous les dossiers Binary et Documents, créez les sous-dossiers `Production` et `Test`.

Traitement des fichiers envoyés par 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 fichiers est :
<ID_participant_destinataire><Nom_fichier_unique>

Lorsqu'un fichier binaire est détecté par le Réceptionnaire, il est écrit dans la mémoire partagée puis transmis au Gestionnaire de documents en vue de son traitement.

Le nom du répertoire dans lequel le fichier a été détecté identifie le nom du participant d'origine, tandis que la première partie du nom du fichier identifie le nom du participant 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 participant d'origine` est `partenaireB` (car le fichier a été trouvé dans la section partenaireB de l'arborescence).
- Le `nom du participant de destination` est `partenaireA` (car la première partie du nom du fichier est 123456789, qui correspond à l'ID DUNS du partenaireA).

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

- La transaction est de type Production.

Le Gestionnaire de documents recherche ensuite une connexion de participants de production entre le partenaireB et le partenaireA pour :

- Regroupement : Aucun (N/A)
- Protocole : Binary (1.0)
- Flot de documents : Binary (1.0)

Le Gestionnaire de documents traite alors le fichier.

Fichiers XML

Un fichier XML n'obéit à aucune règle d'appellation de fichiers car il est inspecté par le Gestionnaire de documents et les informations d'acheminement sont extraites du document lui-même.

Lorsqu'un fichier XML est détecté par le Réceptionnaire, il est écrit dans la mémoire partagée puis transmis au Gestionnaire de documents en vue de son traitement.

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 la section «Création de documents XML personnalisés», à la page 86.) Le nom du Participant d'origine, le nom du Participant de destination et les informations d'acheminement 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 alors ces informations pour localiser la connexion de participants correspondante avant de traiter le fichier.

Configuration supplémentaire du serveur FTP

Après avoir créé la structure de répertoires requise, vous devez configurer votre serveur FTP pour chaque participant 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 :

1. Ajoutez un nouveau groupe (par exemple, Participants).
2. Ajoutez un utilisateur au groupe nouvellement créé pour chaque participant appelé à envoyer ou recevoir des documents via FTP.
3. Pour chaque participant, configurez le serveur FTP pour mapper le participant entrant sur la structure de répertoire respective que vous avez créée pour le participant dans la section précédente «Configuration de la structure de répertoire requise sur le serveur FTP», à la page 20. 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 FTPS pour recevoir des documents, les considérations relatives à la sécurité pour les sessions SSL sont gérées uniquement par le serveur FTPS et le client utilisés par le participant. Il n'existe pas de configuration de sécurité spécifique à WebSphere Partner Gateway pour les documents FTPS entrants. WebSphere Partner Gateway extrait les documents de la cible FTP (décrite

dans «Définition d'une cible FTP», à la page 41) une fois que le serveur a négocié les canaux sécurisés et reçu le document. Pour configurer un canal sécurisé qui puisse être contacté par un participant, 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 réceptionnaire aux participants. Si ce certificat est fourni par une Autorité de certification, fournissez également la chaîne de certificat de CA. Si l'authentification de client est prise en charge par le serveur FTPS, les certificats d'authentification client des participants doivent être précisés sur le serveur FTPS. Consultez la documentation du serveur FTPS pour obtenir des informations sur l'authentification client et les certificats.

Configuration du concentrateur pour le protocole de transfert JMS

Cette section indique comment paramétrer le concentrateur pour utiliser le transfert JMS. Si vous comptez utiliser le transfert 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 file d'attente éloignée et de transmission, consultez la documentation de WebSphere MQ.

Dans les sections suivantes de ce document, vous apprendrez comment configurer des passerelles ou cibles JMS (ou les deux). Ces tâches sont décrites dans les sections «Définition d'une cible JMS», à la page 44 et «Configuration d'une passerelle JMS», à la page 143.

Création d'un répertoire pour JMS

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 :

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

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 23. 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

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

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

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

Définition de la configuration JMS

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
   ```

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 24. 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 24. 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.

Utilisation de scripts FTP pour les passerelles et cibles de script FTP

Le transfert 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 le script lorsque vous créez la passerelle ou la cible de script FTP. WebSphere Partner Gateway met à jour les éléments remplaçables du script FTP avec les valeurs réelles entrées lorsque vous créez la cible ou la passerelle.

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 plus d'informations sur la création d'un script FTP pour une cible de script FTP, voir «Définition d'une cible de script FTP», à la page 46. Pour plus d'informations sur la création d'un script FTP pour une passerelle de script FTP, voir «Configuration d'une passerelle de script FTP», à la page 148.

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. Par exemple, vous souhaiterez peut-être qu'un bon de commande créé par une application dorsale soit transformé et envoyé à un participant de la communauté, 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 à la section «Importation de mappes», à la page 118.

Chapitre 3. 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 :

- «Démarrage de WebSphere MQ»
- «Démarrage des composants de WebSphere Partner Gateway»
- «Connexion à la Console de communauté», à la page 28

Démarrage de WebSphere MQ

Si vous ne l'avez pas encore fait, démarrez WebSphere MQ en utilisant l'une des procédures suivantes :

- Pour les systèmes UNIX :
  1. Entrez :
     ```
     su mqm
     ```
  2. Entrez :
     ```
     strmqm bcg.queue.manager
     ```
  3. Entrez :
     ```
     runmqlsr -t tcp -p 9999 -m bcg.queue.manager &
     ```
  4. Attendez 10 secondes et appuyez sur Entrée pour revenir à l'invite de commande.
  5. Entrez :
     ```
     strmqbrk -m bcg.queue.manager
     ```
- Pour les systèmes Windows :
  1. Entrez :
     ```
     strmqm bcg.queue.manager
     ```
  2. Entrez :
     ```
     runmqlsr -t tcp -p 9999 -m bcg.queue.manager
     ```
     Le programme d'écoute s'exécute dans cette fenêtre ; vous devez donc la laisser ouverte.
  3. Ouvrez une nouvelle fenêtre et démarrez le courtier JMS (le courtier de publication-souscription) à l'aide de la commande suivante :
     ```
     strmqbrk -m -bcg.queue.manager
     ```

Démarrage des composants de WebSphere Partner Gateway

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 Réceptionnaire.

1. Allez dans le répertoire \<*ProductDir*\bin.
2. Entrez la commande suivante pour démarrer la console :
   - Pour les systèmes UNIX :
     ```
     ./bcgStartServer.sh bcgconsole
     ```
   - Pour les systèmes Windows :
     ```
     bcgStartServer bcgconsole
     ```

3. Entrez la commande suivante pour démarrer le Réceptionnaire :
   ```
   ./bcgStartServer.sh bcgreceiver
   ```

   ou
   ```
   bcgStartServer bcgreceiver
   ```
4. Entrez la commande suivante pour démarrer le Gestionnaire de documents :
   ```
   ./bcgStartServer.sh bcgdocmgr
   ```

   ou
   ```
   bcgStartServer bcgdocmgr
   ```

Après avoir démarré les composants, démarrez le système d'aide. Pour cela, entrez la commande suivante :
```
./bcgStartHelp.sh
```

ou
```
bcgStartHelp.bat
```

Une fois tous les composants démarrés, connectez-vous à la Console de communauté, comme décrit dans la section «Connexion à la Console de communauté»

Pour plus d'informations sur le démarrage du client Data Interchange Services, consultez le *Guide de mappage*.

Connexion à la Console de communauté

La Console de communauté est le point d'accès à WebSphere Partner Gateway. La plupart des tâches de configuration du concentrateur nécessitent une connexion avec des droits d'administrateur du concentrateur (hubadmin), qui est le super-utilisateur du système.

Assurez-vous de disposer de l'adresse IP de l'ordinateur sur lequel la Console s'exécute, car vous devrez l'entrer dans la commande HTTP.

1. Dans un navigateur, tapez l'URL suivante :
   `http://<adresse_IP>:58080/console`
2. Entrez les informations suivantes :
   a. Dans la zone **Nom d'utilisateur**, tapez `hubadmin`
   b. Dans la zone **Mot de passe**, tapez `Pa55word`

      Remarque : Si vous vous êtes déjà connecté à la Console de communauté et que vous avez modifié le mot de passe par défaut (Pa55word), entrez votre nouveau mot de passe dans la zone **Mot de passe**.
   c. Dans la zone **Nom de connexion de l'entreprise**, tapez `Operator`

Vous obtenez la page Recherche du participant, qui est toujours la première page à s'afficher lorsque vous vous connectez à la Console de communauté.

C'est dans cette page que vous définirez ultérieurement les participants.

Si vous cliquez sur **Rechercher** à ce stade, un seul participant s'affichera, l'opérateur de communauté. Ce dernier est défini automatiquement par WebSphere Partner Gateway.

Remarque : Si vous n'avez pas modifié le mot de passe par défaut Pa55word, il vous sera demandé de le faire avant l'affichage de la page Recherche du participant.

Chapitre 4. Configuration de la Console de communauté

Ce chapitre indique comment configurer la Console de communauté pour préciser ce que voient les participants, 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 de la règle de mot de passe», à la page 33
- «Configuration des droits d'accès», à la page 34

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

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

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

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.

- L'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

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

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 regroupements 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 de la règle de mot 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 participant. 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 participant 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, procédez comme suit :

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 regroupements 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 entités communauté du concentrateur, opérateur de communauté et Gestionnaire de communauté, ainsi que les participants, disposent d'un utilisateur d'administration. Lorsque vous créez un Gestionnaire de communauté ou un participant, vous créez en fait l'utilisateur d'administration pour cette entité. (Dans le cas d'un opérateur de communauté, l'administrateur de concentrateur est automatiquement créé, de même qu'un autre utilisateur d'administration pour le concentrateur.)

Lorsque vous créez le participant (comme défini dans «Création des profils des participants», à la page 155), vous fournissez au participant des informations des connexion (nom et mot de passe de connexion). Une fois que le participant est connecté, il crée des utilisateurs supplémentaires au sein de l'organisation. Le participant 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 participant crée alors un groupe Volume et y ajoute des utilisateurs.

Remarque : En tant qu'utilisateur d'administration, vous pouvez également définir les utilisateurs et les groupes pour un participant.

L'utilisateur d'administration du participant 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 regroupement de rapports de document, mais, ce faisant, il désactive tous les autres regroupements pour le groupe Volume.

Les paramètres que vous définissez sur la page Droits d'accès en tant qu'utilisateur d'administration permettent de déterminer si un regroupement est répertorié dans la page Détails du groupe.

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

Activation et désactivation des droits d'accès

A partir de la page Liste des droits d'accès, vous pouvez déterminer les droits à accorder aux groupes ou aux 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**.

Chapitre 5. Définition des cibles

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

Vue d'ensemble

Comme l'explique la section «Vue d'ensemble du traitement des documents», à la page 7, le Réceptionnaire est chargé d'accepter les documents entrants en provenance d'un transfert donné. Une cible est une instance du Réceptionnaire configurée pour un déploiement particulier.

Les documents reçus sur une cible du concentrateur peuvent provenir de participants de la communauté (pour être remis au Gestionnaire de communauté) ou de l'application dorsale du Gestionnaire de communauté (pour être remis aux participants).

La figure 16, à la page 38 illustre un serveur WebSphere Partner Gateway sur lequel quatre cibles sont paramétrées. Deux des cibles (HTTP/S et FTP/S) reçoivent les documents émis par des participants. Elles représentent un URI HTTP et un répertoire FTP. Vous fournissez à vos participants des informations sur ces cibles pour leur indiquer où ils doivent vous envoyer des documents. Les deux autres cibles (JMS et fichier-répertoire) concernent des documents émis par l'application dorsale du Gestionnaire de communauté. Ces cibles représentent une file d'attente et un répertoire.

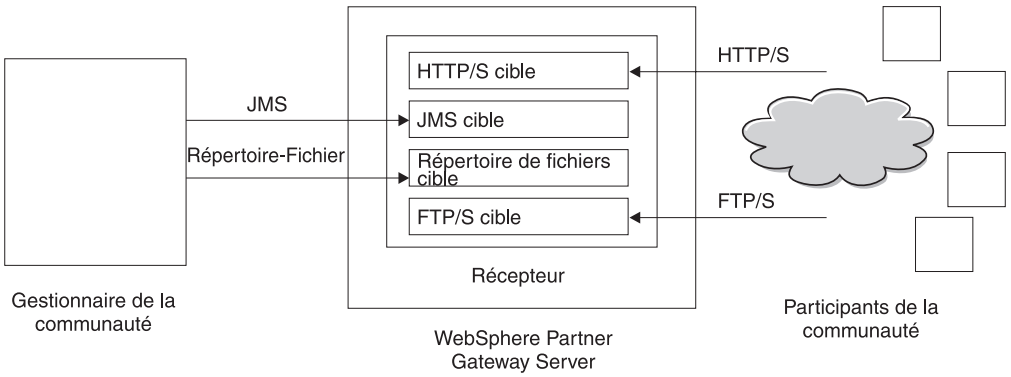

Figure 16. Transferts et cibles associées

Vous devez définir au moins une cible pour chaque type de transfert utilisé pour acheminer les documents qui seront envoyés au concentrateur. Par exemple, il doit exister une cible HTTP pour recevoir les documents envoyés par transfert HTTP ou HTTPS. Si les participants de votre communauté sont appelés à envoyer des documents via FTP, vous devez définir une cible FTP.

Le composant Réceptionnaire détecte l'arrivée des messages sur l'une des cibles. Pour déterminer si de nouveaux messages sont arrivés, certaines cibles interrogent leurs transferts à intervalles réguliers ou de façon planifiée. Les cibles WebSphere Partner Gateway basées sur une interrogation sont : JMS, FTP, SMTP, File et script FTP. La cible HTTP/S utilise le rappel, c'est-à-dire qu'elle reçoit une notification du transfert lorsque des messages arrivent. Les transferts définis par l'utilisateur peuvent être de type interrogation ou rappel.

Téléchargement de récupérateurs définis par l'utilisateur

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

Pour télécharger un récupérateur, procédez comme suit :

1. Dans le menu principal, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récupérateurs**.
2. Sélectionnez **Cible**.

   La liste des récupérateurs actuellement définis pour les cibles s'affiche. Notez que les récupérateurs fournis par WebSphere Partner Gateway sont associés à l'ID fournisseur **Produit**.
3. Dans la page Liste des récupérateurs, cliquez sur **Importer**.
4. Sur la page d'importation de récupérateur, indiquez le chemin d'accès au fichier XML qui décrit le récupérateur, ou utilisez le bouton **Parcourir** pour rechercher le fichier XML.

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

Définition de valeurs globales de transfert

Les attributs globaux de transfert s'appliquent à toutes les cibles HTTP/S et de script FTP. Si vous ne définissez pas de cibles HTTP/S ou de script FTP, cette section en vous concerne pas.

1. Pour afficher la liste des Cibles, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Sélectionnez **Attributs de transfert globaux** dans la liste des cibles.
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 **Transfert de scripts FTP** et **Cibles et passerelles de scripts FTP**.

   Le transfert de script FTP utilise un mécanisme de verrouillage qui empêche que plusieurs instances de script FTP n'accèdent à la même cible au même moment. Lorsqu'un transfert 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 cibles 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 **Transfert de script FTP**
     - **Nombre de relances du verrouillage**, le nombre de tentatives de la cible 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 **Cibles et passerelles de script FTP**
     - **Délai maximal de verrouillage (secondes)**, la durée pendant laquelle la cible peut maintenir le verrouillage. La valeur par défaut est 240 secondes.
     - **Délai maximal des files d'attente (secondes)**, la durée pendant laquelle la cible attendra dans une file d'attente pour obtenir le verrou. La valeur par défaut est 740 secondes.
6. Si nécessaire, modifiez les valeurs pour **Transfert HTTP/S**. Vous pouvez modifier :
   - **Temporisations synchrones 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.
7. Cliquez sur **Enregistrer**

Définition d'une cible HTTP/S

Le composant Réceptionnaire 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 une ou plusieurs cibles HTTP.

La procédure suivante indique comment définir une cible HTTP/S.

1. Pour afficher la page Liste des cibles, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Dans la page Liste des cibles, cliquez sur **Créer la cible**.

Caractéristiques de la cible

Dans la section **Caractéristiques de la cible**, procédez comme suit :

1. Attribuez un nom à la cible. Par exemple, vous pourriez la nommer CibleHttp1. Cette zone doit être renseignée. Le nom que vous entrez ici s'affichera dans la liste des cibles.
2. Indiquez éventuellement l'état de la cible. L'état par défaut est **Activé**. Une cible activée est prête à accepter des documents. Une cible désactivée ne peut pas accepter de documents.
3. Entrez éventuellement une description pour la cible.
4. Sélectionnez **HTTP/S** dans la liste des **transferts**.

Configuration de la cible

Dans la section **Configuration de la cible**, procédez comme suit :

1. Indiquez éventuellement le type de passerelle. Le type de passerelle 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 de la cible HTTP/S. Le nom doit commencer par **bcgreceiver**. Par exemple, vous pouvez entrer bcgreceiver/submit. Les documents entrant dans le serveur via HTTP/S seront alors reçus dans bcgreceiver/submit.

   Remarque : Les valeurs **Réacheminement synchronisé** sont déjà renseignées et ne peuvent être modifiées dans cette page. Pour les modifier, utilisez la page Attributs de transfert globaux, de la façon indiquée dans la section «Définition de valeurs globales de transfert», à la page 39.

Récupérateurs

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le récupérateur 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 réceptionnaire pour le protocole associé dans le point de configuration SyncCheck. Vous pouvez également modifier les points de configuration Postprocess pour la cible.

Pour modifier un point de configuration, consultez la section «Modification des points de configuration», à la page 51. Sinon, cliquez sur **Sauvegarder**.

Définition d'une cible FTP

Une cible FTP interroge votre serveur FTP selon un intervalle prédéfini, pour rechercher de nouveaux documents.

La procédure suivante indique comment définir une cible FTP.

1. Pour afficher la page Liste des cibles, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Dans la page Liste des cibles, cliquez sur **Créer la cible**.

Caractéristiques de la cible

Dans la section **Caractéristiques de la cible**, procédez comme suit :

1. Attribuez un nom à la cible. Par exemple, vous pourriez la nommer CibleFTP1. Cette zone doit être renseignée. Le nom que vous entrez ici s'affichera dans la liste des cibles.
2. Indiquez éventuellement l'état de la cible. L'état par défaut est **Activé**. Une cible activée est prête à accepter des documents. Une cible désactivée ne peut pas accepter de documents.
3. Entrez éventuellement une description pour la cible.
4. Sélectionnez **Répertoire FTP** dans la liste des **transferts**.

Configuration de la cible

Dans la section **Configuration de la cible**, 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 participant dans le répertoire racine FTP. Cette zone doit être renseignée. 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 19.

   Remarque : Saisissez le chemin permettant d'accéder au répertoire FTP racine. N'incluez pas les sous-répertoires du participant.
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 : Ne mettez pas de point avant l'extension du nom de fichier (par exemple : .exe ou . txt). Indiquez uniquement les caractères qui composent l'extension.

Récupérateurs

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

Pour modifier un point de configuration Preprocess, consultez la section «Modification des points de configuration», à la page 51. Sinon, cliquez sur **Sauvegarder**.

Définition d'une cible SMTP

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

La procédure suivante indique comment définir une cible SMTP (POP3).

1. Pour afficher la page Liste des cibles, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Dans la page Liste des cibles, cliquez sur **Créer la cible**.

Caractéristiques de la cible

Dans la section **Caractéristiques de la cible**, procédez comme suit :

1. Attribuez un nom à la cible. Par exemple, vous pourriez la nommer CiblePOP31. Cette zone doit être renseignée. Le nom que vous entrez ici s'affichera dans la liste des cibles.
2. Indiquez éventuellement l'état de la cible. L'état par défaut est **Activé**. Une cible activée est prête à accepter des documents. Une cible désactivée ne peut pas accepter de documents.
3. Entrez éventuellement une description pour la cible.
4. Sélectionnez **POP3** dans la liste des **transferts**.

Configuration de la cible

Dans la section **Configuration de la cible**, procédez comme suit :

1. Indiquez éventuellement le type de passerelle. Le type de passerelle 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. 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).

Planification

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 avez sélectionné **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. **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.

Définition d'une cible JMS

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

La procédure suivante indique comment définir une cible JMS.

1. Pour afficher la page Liste des cibles, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Dans la page Liste des cibles, cliquez sur **Créer la cible**.

Caractéristiques de la cible

Dans la section **Caractéristiques de la cible**, procédez comme suit :

1. Attribuez un nom à la cible. Par exemple, vous pourriez la nommer CibleJMS1. Cette zone doit être renseignée. Le nom que vous entrez ici s'affichera dans la liste des cibles.
2. Indiquez éventuellement l'état de la cible. L'état par défaut est **Activé**. Une cible activée est prête à accepter des documents. Une cible désactivée ne peut pas accepter de documents.
3. Entrez éventuellement une description pour la cible.
4. Sélectionnez **JMS** dans la liste des **transferts**.

Configuration de la cible

Dans la section **Configuration de la cible**, procédez comme suit :

1. Indiquez éventuellement le type de passerelle. Le type de passerelle 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 24.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. Renseignez la zone Nom de file d'attente JMS. Cette zone doit être renseignée. 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 bindings (étape 4, à la page 25).

   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. Précisez le nom de la fabrique JMS. Cette zone doit être renseignée. 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 25).

Si vous avez entré le sous-dossier pour le contexte JMS à l'étape 2, à la page 44, 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. Indiquez le regroupement URL du fournisseur (facultatif).
7. Précisez le nom de la fabrique JNDI. Si vous n'en indiquez pas, c'est la valeur value com.sun.jndi.fscontext.RefFSContextFactory qui est utilisée. Cette zone doit être renseignée.
8. Entrez éventuellement une valeur dans la zone **Délai d'inactivité**, pour indiquer le nombre de secondes durant lesquelles la cible vérifiera la présence de documents sur le serveur JMS. Cette zone doit être renseignée.
9. 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 une cible JMS analogue à celle de l'exemple du «Configuration du concentrateur pour le protocole de transfert JMS», à la page 23, vous indiquerez les valeurs suivantes :

1. **CibleJMS** dans la zone **Nom de la cible** ;
2. Entrez la valeur **file:/C:/TEMP/JMS/JMS** dans la zone **URL du fournisseur JMS**.
3. **enFA** dans la zone **Nom de file d'attente JMS** ;
4. **Hub** dans la zone **Nom de la fabrique JMS**.

Récupérateurs

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le récupérateur 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 51. Sinon, cliquez sur **Sauvegarder**.

Définition d'une cible Système de fichiers

Une cible Système de fichiers interroge un répertoire selon un intervalle prédéfini, pour rechercher de nouveaux documents.

La procédure suivante indique comment définir une cible Système de fichiers.

1. Pour afficher la page Liste des cibles, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Dans la page Liste des cibles, cliquez sur **Créer la cible**.

Caractéristiques de la cible

Dans la section **Caractéristiques de la cible**, procédez comme suit :

1. Attribuez un nom à la cible. Par exemple, vous pourriez la nommer CibleFichier1. Cette zone doit être renseignée. Le nom que vous entrez ici s'affichera dans la liste des cibles.
2. Indiquez éventuellement l'état de la cible. L'état par défaut est **Activé**. Une cible activée est prête à accepter des documents. Une cible désactivée ne peut pas accepter de documents.
3. Entrez éventuellement une description pour la cible.

4. Sélectionnez **Fichier-répertoire** dans la liste des **transferts**.

Configuration de la cible

Dans la section **Configuration de la cible**, procédez comme suit :

1. Indiquez éventuellement le type de passerelle. Le type de passerelle 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 une valeur dans la zone **Répertoire principal du document** pour indiquer le répertoire dans lequel les documents seront reçus.
3. Renseignez éventuellement la zone **Intervalle de sondage** 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.
4. 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.
5. 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).

Récupérateurs

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le récupérateur 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 51. Sinon, cliquez sur **Sauvegarder**.

Définition d'une cible de script FTP

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

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

Création du script FTP

Les serveurs FTP peuvent avoir certaines exigences spécifiques pour les commandes qu'ils acceptent. Pour utiliser une cible 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 cibles 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 la cible est mise 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 d'une cible de script FTP. Dans cet exemple, %BCGOPTION% est le nom du répertoire dans la commande `cd`. Les paramètres de script et les zones de cible de script FTP qui leur sont associées sont indiqués dans le tableau 2:

Tableau 2. Mappage des paramètres de script avec les entrées de zone de cible de script FTP

Paramètre de script	**Entrée dans la zone de la cible 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

  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.

- 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 crée un répertoire sur le serveur 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 cible FTP doit être :

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

  Cette commande ferme 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.
- rename

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

  Cette commande supprime 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 de la cible

La procédure suivante indique ce dont vous avez besoin pour spécifier une cible de script FTP.

1. Pour afficher la page Liste des cibles, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Dans la page Liste des cibles, cliquez sur **Créer la cible**.

Dans la section **Caractéristiques de la cible**, procédez comme suit :

1. Attribuez un nom à la cible. Par exemple, vous pourriez la nommer CibleFTPScripting1. Cette zone doit être renseignée. Le nom que vous entrez ici s'affichera dans la liste des cibles.
2. Indiquez éventuellement l'état de la cible. L'état par défaut est **Activé**. Une cible activée est prête à accepter des documents. Une cible désactivée ne peut pas accepter de documents.
3. Entrez éventuellement une description pour la cible.
4. Sélectionnez **Script FTP** dans la liste Transfert.

Configuration de la cible

Dans la section **Configuration de la cible**, procédez comme suit :

1. Indiquez éventuellement le type de passerelle. Le type de passerelle 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 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. Indiquez si la cible fonctionnera en mode SSL (Secure Sockets Layer). Dans ce cas, vous devrez échanger des certificats avec vos participants, comme indiqué au Chapitre 13, «Configuration de la sécurité pour les échanges entrants et sortants», à la page 163.
5. Envoyez le script en procédant comme suit :
   a. Cliquez sur **Télécharger le fichier de script**.
   b. Entrez le nom du fichier contenant le script de traitement des documents, ou utilisez **Parcourir** pour accéder au fichier.
   c. Cliquez sur **Charger le fichier** pour charger le fichier de script dans la zone de texte **Fichier de script actuellement chargé**.
   d. Si ce fichier de script est bien celui que vous voulez utiliser, cliquez sur **Enregistrer**.
   e. 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 utilisateur**, indiquez si la cible demandera un verrouillage pour qu'aucune autre instance de cible 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 les modifier, utilisez la page Attributs de transfert globaux, de la façon indiquée dans la section «Définition de valeurs globales de transfert», à la page 39.

Attributs définis par l'utilisateur

Si vous souhaitez préciser des attributs supplémentaires, procédez comme suit. 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.

Voici 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 avez sélectionné **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. **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.

Récupérateurs

Si vous pensez recevoir des fichiers contenant plusieurs documents EDI, XML ou ROD devant être fractionnés, configurez le récupérateur 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 51. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une cible pour un transfert défini par l'utilisateur

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

Procédez comme suit :

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

   Remarque : Dans la liste des cibles, vous pouvez également supprimer un type de transfert défini par l'utilisateur. Vous ne pouvez pas supprimer un transfert fourni par WebSphere Partner Gateway. Vous ne pouvez pas non plus supprimer un transfert défini par l'utilisateur une fois qu'il a été utilisé pour la création d'une cible.
5. Cliquez sur **Créer la cible**.
6. Attribuez un nom à la cible. Cette zone doit être renseignée. Le nom que vous entrez ici s'affichera dans la liste des cibles.
7. Indiquez éventuellement l'état de la cible. L'état par défaut est **Activé**. Une cible activée est prête à accepter des documents. Une cible désactivée ne peut pas accepter de documents.
8. Entrez éventuellement une description pour la cible.
9. Sélectionnez dans la liste un transfert défini par l'utilisateur.
10. Renseignez les zones (qui seront uniques à chaque transfert défini par l'utilisateur).

11. Pour modifier des points de configuration pour cette cible, consultez la section «Modification des points de configuration». Sinon, cliquez sur **Sauvegarder**.

Modification des points de configuration

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

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

Pour appliquer un récupérateur écrit par l'utilisateur à ces points de configuration, vous devez d'abord télécharger le récupérateur, comme décrit dans la section «Téléchargement de récupérateurs définis par l'utilisateur», à la page 38. Vous pouvez également utiliser un récupérateur fourni par le système, déjà disponible et qu'il n'est pas nécessaire de télécharger.

Preprocess

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

Attributs Preprocess

Le tableau 3 décrit les attributs que vous pouvez définir dans un récupérateur Preprocess, ainsi que les récupérateurs de fractionnement auxquels s'appliquent ces attributs.

Les attributs ROD pris comme exemple dans ce tableau correspondent à ceux utilisés «Exemple ROD vers EDI», à la page 231. Dans cet exemple, les attributs ROD sont contenus dans la mappe S_DT_ROD_TO_EDI.eif, qui comprend les définitions suivantes de flot de documents :

- Regroupement : Aucun (version N/A)
- Protocole : ROD_TO_EDI_DICT (version TOUTE)
- Flot de documents : DTROD-TO-EDI_ROD (version TOUTE)

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

Tableau 3. Attributs de récupérateur de fractionnement

Attribut	Description	Récupérateur de fractionnement
Codage	Le codage des caractères du document. La valeur par défaut est ASCII.	ROD Générique XML EDI

Tableau 3. Attributs de récupérateur de fractionnement (suite)

Attribut	Description	Récupérateur 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 106.	ROD Générique XML
Nom du regroupement d'origine	Le regroupement associé au document. La valeur doit correspondre au regroupement indiqué dans la définition du flot de documents. Par exemple, pour un document dont le regroupement est Aucun, la valeur doit être **Aucun**.	ROD Générique
Version du regroupement d'origine	La version du regroupement indiquée dans le Nom du regroupement d'origine. Par exemple, pour un document dont le regroupement est Aucun, la valeur doit être **N/A**.	ROD Générique
Nom du protocole d'origine	Le protocole associé au document. La valeur doit correspondre au protocole indiqué dans la définition du flot de documents. Par exemple, pour un document ROD, cette valeur doit être **ROD-TO-EDI_DICT**.	ROD Générique
Version du protocole d'origine	La version du protocole indiquée dans le Nom du regroupement d'origine. Par exemple, pour le protocole ROD-TO-EDI_DICT, la valeur doit être **TOUT**.	ROD Générique
Code du processus d'origine	Le processus (flot de document) associé à ce document. La valeur doit correspondre au flot de document indiqué dans la définition du flot de documents. Par exemple, pour un document ROD, cette valeur doit être DTROD-TO-EDI_ROD.	ROD Générique
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 Générique
Métadictionnaire	Le métadictionnaire donne des informations qui permettent à WebSphere Partner Gateway d'interpréter les données. Par exemple, pour un document ROD document, cette valeur doit être **ROD-TO-EDI_DICT**.	ROD Générique
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 Générique
Métasyntaxe	La métasyntaxe décrit le format du document en cours de fractionnement. La valeur par défaut est **rod**.	ROD Générique

Remarques :

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

Modification du point de configuration Preprocess

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

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

   Quatre récupérateurs preprocess sont fournis (par défaut) et figurent dans la **Liste des récupérateurs disponibles**.

   - 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

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

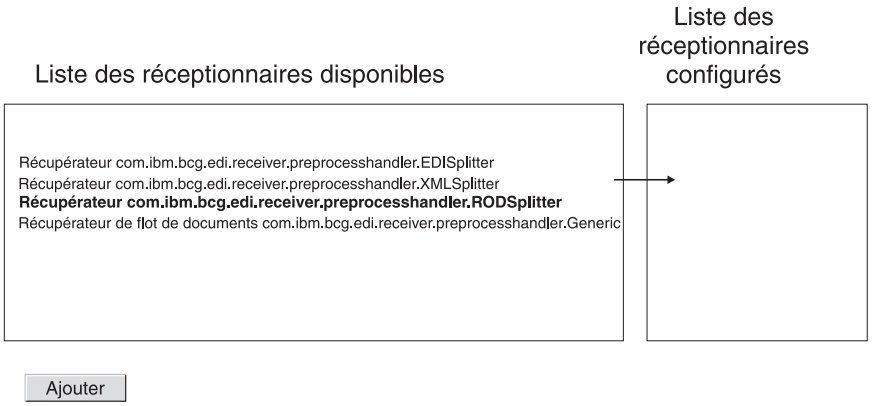

Figure 17. Configuration du preprocess

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

      N'oubliez pas que pour les cibles, les récupérateurs sont appelés dans leur ordre d'apparition dans la liste des **récupérateurs configurés**. Le premier récupérateur disponible traite la requête et les récupérateurs suivants de la liste ne sont pas appelés.
   c. Pour configurer le récupérateur, sélectionnez-le et cliquez sur **Configurer**:
      - Si vous avez ajouté le récupérateur EDISplitterHandler, vous pouvez modifier le codage de ses attributs. Le codage par défaut est ASCII.

- Si vous avez ajouté le récupérateur XMLSplitterHandler, vous pouvez modifier le codage de ses attributs (BCGBATCHDOCs). La valeur par défaut est **ON**. Voir «Attributs Preprocess», à la page 51 pour obtenir des informations sur cet attribut.
- Si vous avez ajouté le récupérateur 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 regroupement d'origine, Version du regroupement 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 51 pour obtenir des informations sur ces attributs.
- Si vous avez ajouté le GenericDocumentFlowHandler, vous pouvez préciser des valeurs pour 11 attributs. Le codage et BATCHDOCS ont des valeurs par défaut. Vous devez saisir une valeur pour les autres attributs, à savoir Nom du regroupement d'origine, Version du regroupement 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. Voit «Attributs Preprocess», à la page 51 pour obtenir des informations sur ces attributs.

SyncCheck

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

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

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

   Six récupérateurs SyncCheck sont fournis (par défaut) pour une cible HTTP/S. Ces récupérateurs figurent dans la **Liste des récupérateurs 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

   Par exemple, si vous configurez une cible HTTP/S, la Liste des récupérateurs disponibles se présente ainsi :

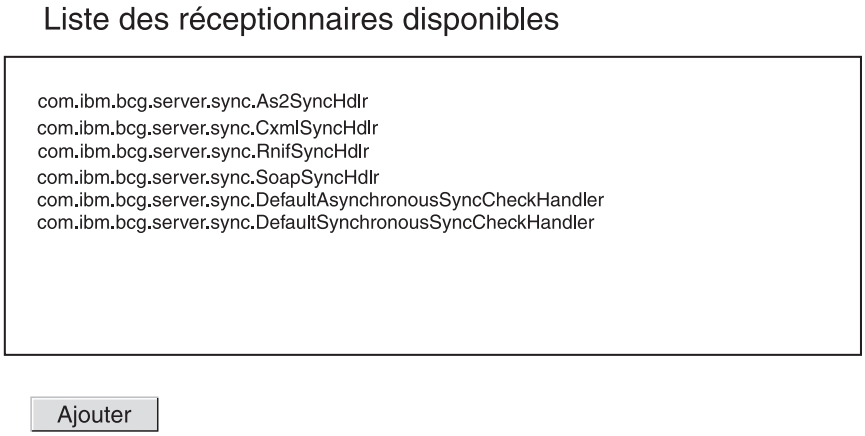

Figure 18. Liste des récupérateurs disponibles pour un point de configuration SyncCheck HTTP/S

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

DefaultAsynchronousSyncCheckHandler et DefaultSynchronousSyncCheckHandler peuvent être utilisés avec d'autres cibles (telles qu'une cible JMS).

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

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

Postprocess

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

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

Vous pouvez ajouter un récupérateur de postprocess en en téléchargeant un qui soit conforme à l'un de ces types. Utilisez l'option **Importer** de la page Liste des récupérateurs pour télécharger un récupérateur défini par l'utilisateur. Lorsque

vous téléchargez un récupérateur cible défini par l'utilisateur, le récupérateur est ajouté à la liste des récupérateurs. Il apparaît également sur la liste des récupérateurs 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 **Récupérateurs des points de configuration**.
2. Sélectionnez un récupérateur défini par l'utilisateur dans la **Liste des récupérateurs disponibles** et cliquez sur **Ajouter**. Notez que le récupérateur passe de la **Liste des récupérateurs disponibles** à la **Liste des récupérateurs configurés**.

Modification de la Liste des récupérateurs configurés

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

- Supprimez un récupérateur en le sélectionnant dans la liste des **récupérateurs configurés** et en cliquant sur **Supprimer**. Le récupérateur passe dans la liste des **récupérateurs disponibles**.
- Pour modifier l'ordre du récupérateur 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 récupérateur, sélectionnez-le dans la liste des **récupérateurs configurés** et cliquez sur **Configurer**. La liste des attributs pouvant être configurés s'affiche.

Chapitre 6. 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 :

Téléchargement de récupérateurs

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

Remarque : Comme dans la «Configuration des composants de traitement des documents à l'aide de récupérateurs», à la page 9, seuls les récupérateurs définis par l'utilisateur ont besoin d'être téléchargés. Les récupérateurs 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 récupérateurs avec lesquels vous les associez.

Remarque : Pour dresser la liste des types de récupérateurs valides pour les actions et les flux de travaux fixes, cliquez sur **Administrateur de concentrateur > Configuration du concentrateur > Récupérateurs > Actions > Types de récupérateurs**, ou **Administrateur de concentrateur > Configuration du concentrateur > Récupérateurs > Flux de travaux fixes > Types de récupérateurs** . Utilisez cette liste pour confirmer que le type de votre récupérateur 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 récupérateur, procédez comme suit :

1. Dans le menu principal, cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Récupérateurs**.
2. Sélectionnez le type de récupérateur (**Action** ou **Flux de travaux fixe**).

   La liste des récupérateurs actuellement définis pour le composant en question s'affiche à l'écran. Remarquez que les récupérateurs répertoriés sont ceux fournis par WebSphere Partner Gateway. Ils sont associés à l'ID fournisseur **Produit**.
3. Dans la page Liste des récupérateurs, cliquez sur **Importer**.

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

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

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

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

Configuration des flux de travaux fixes

Le Chapitre 1, «Introduction» 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 le regroupement de protocole.

Si vous prévoyez d'utiliser un récupérateur défini par l'utilisateur pour configurer une étape de flux de travaux, téléchargez le récupérateur comme décrit à la section «Téléchargement de récupérateurs», à la page 57.

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 récupérateurs configurés pour cette étape, est répertoriée. Pour la liste des récupérateurs par défaut, voir «Flux de travaux de communication entrante», à la page 59 et «Flux de travaux de communication sortante», à la page 59.
4. Cliquez sur l'icône **Edition** pour modifier la liste des récupérateurs.
5. Exécutez une ou plusieurs des tâches ci-après pour chaque étape que vous souhaitez modifier.
   a. Ajoutez un récupérateur en le sélectionnant dans la liste des **récupérateurs disponibles** et en cliquant sur **Ajouter**. (Un récupérateur apparaît dans la liste des **récupérateurs disponibles** si vous avez téléchargé un récupérateur défini par l'utilisateur ou si vous avez précédemment supprimé un récupérateur de la liste des **récupérateurs configurés**.) Le récupérateur passe dans la liste des **récupérateurs configurés**.
   b. Supprimez un récupérateur en le sélectionnant dans la liste des **récupérateurs configurés** et en cliquant sur **Supprimer**. Le récupérateur passe dans la liste des **récupérateurs disponibles**.
   c. Pour modifier l'ordre d'appel des récupérateurs, sélectionnez un récupérateur dans la liste et cliquez sur le bouton de **déplacement vers le haut** ou **déplacement vers le bas**.

Les récupérateurs sont appelés dans l'ordre de la liste des **récupérateurs configurés**. Le premier récupérateur 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 récupérateur associé à ce type de document (dans cet exemple, com.ibm.bcg.edi.business.process.RODScannerHandler).

6. Cliquez sur **Enregistrer**.

Flux de travaux de communication entrante

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

Récupérateurs de dégroupement de protocole

Par défaut, les récupérateurs 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

Récupérateurs de traitement de protocole

Par défaut, les récupérateurs 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

Flux de travaux de communication sortante

Par défaut, les récupérateurs ci-dessous sont configurés pour l'étape de regroupement 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 1, «Introduction» indiquait que les actions pouvaient être constituées d'une ou de 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 récupérateurs (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 61).

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 61).

Si vous prévoyez d'utiliser un récupérateur défini par l'utilisateur pour configurer une action, téléchargez-le comme décrit à la section «Téléchargement de récupérateurs», à la page 57.

Modification d'une action définie par l'utilisateur

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 récupérateurs (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 récupérateur associé dans la liste des **récupérateurs disponibles** et en cliquant sur **Ajouter**. Le récupérateur passe dans la liste des **récupérateurs configurés**.
   b. Supprimez un récupérateur en le sélectionnant dans la liste des **récupérateurs configurés** et en cliquant sur **Supprimer**. Le récupérateur passe dans la liste des **récupérateurs disponibles**.
   c. Pour modifier l'ordre d'appel des récupérateurs, sélectionnez un récupérateur dans la liste et cliquez sur le bouton de **déplacement vers le haut** ou **déplacement vers le bas**.
   d. Pour exécuter un récupérateur plusieurs fois, sélectionnez-le, puis cliquez sur **Répéter**.

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

Création d'actions

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

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

Création d'une action

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 doit être renseignée.
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 récupérateur associé en le sélectionnant dans la liste des **récupérateurs disponibles** et en cliquant sur **Ajouter**. Le récupérateur passe dans la liste des **récupérateurs configurés**.

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

Copie d'une action

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 doit être renseignée.
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 Community Manager Cancellation fournie par le système pour le processus RosettaNet, la liste suivante de récupérateurs disponibles et configurés s'affiche :

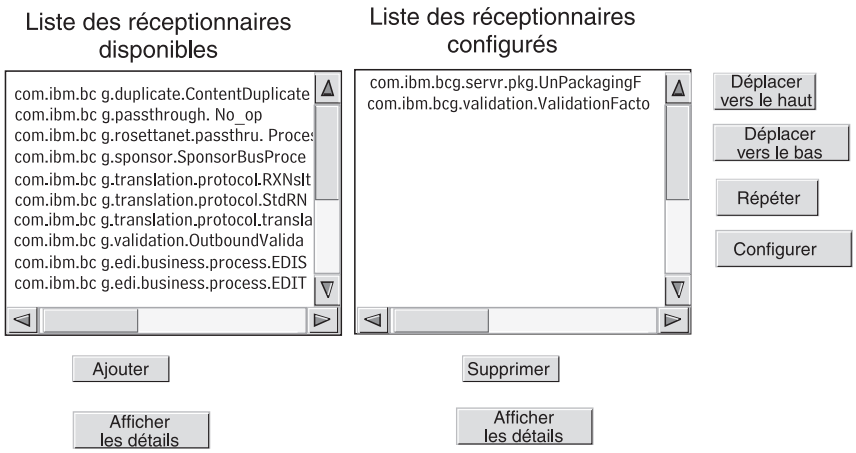

Figure 19. Clonage d'une action

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

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

b. Supprimez une étape en sélectionnant le récupérateur associé dans la liste des **récupérateurs configurés** et en cliquant sur **Supprimer**. Le récupérateur passe dans la liste des **récupérateurs disponibles**.

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

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

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

7. Cliquez sur **Enregistrer**.

Chapitre 7. Configuration des flots de documents

Ce chapitre explique comment configurer les documents non EDI que vous échangerez avec les participants de la communauté et avec vos applications dorsales. La configuration des flots de documents EDI et leurs interactions (à l'exception des documents EDI en transit) sont décrits au Chapitre 8, «Configuration des flots de documents EDI», à la page 91. Le Chapitre 8 décrit également comment configurer les flots de documents et les interactions pour les documents XML ou ROD (record-oriented-data).

Ce chapitre contient les rubriques suivantes :

Généralités

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

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

Les sections suivantes décrivent rapidement les étapes de définition d'un flot de documents entre le Gestionnaire de communauté et un participant.

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

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

Lors de la définition d'un flot 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. Ils permettent un paramétrage global du regroupement, protocole ou flot de documents associés. Les attributs disponibles varient selon la définition du flot de documents. Les attributs des définitions de flots de documents EDI sont différents de ceux des définitions de flots de documents RosettaNet.

Par exemple, si vous indiquez une valeur pour l'attribut **Heure d'accuser réception** du regroupement AS, elle s'applique à tous les documents regroupés avec AS. (L'attribut **Heure d'accuser 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'accuser réception** au niveau des capacités B2B, cette valeur supplante celle qui a été indiquée au niveau de la définition du flot de documents.

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

Le flot de documents doit figurer sur la page Gérer des définitions de flots de documents pour que vous puissiez créer des interactions.

Etape 2 : Créez des interactions

Créez des interactions pour les flux de documents définis. L'interaction indique à WebSphere Partner Gateway les actions à effectuer sur un document. Pour certains échanges, deux flots suffisent : un pour décrire le document reçu dans le concentrateur (de la part du participant ou du Gestionnaire de communauté) et un qui décrit le document envoyé depuis le concentrateur (au participant ou au Gestionnaire de communauté. 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.

Etape 3 : Créez les profils, capacités B2B et les passerelles des participants

Créez les profils des participants pour le Gestionnaire de communauté et les participants. Définissez des passerelles (qui déterminent quels documents seront envoyés) et des capacités B2B pour définir les documents que le Gestionnaire de communauté et les participants peuvent envoyer et recevoir. La page Capacités B2B répertorie tous les flots de documents définis.

Vous pouvez définir des attributs au niveau des capacités B2B. Tout attribut défini à ce niveau a la précédence sur ceux qui ont été définis au niveau de la définition du flot de documents. Par exemple, si vous définissez **Heure d'accuser réception** sur 30 au niveau de la définition du flot de documents pour un regroupement AS, puis la définissez sur 60 dans les capacités B2B, la valeur 60 est utilisée. Le fait de définir un attribut au niveau B2B vous permet de le personnaliser en fonction d'un participant spécifique.

Vous devez définir les profils et capacités B2B du Gestionnaire de communauté et des participants avant de pouvoir créer des connexions entre eux.

Etape 4 : Activez les connexions

Activez les connexions entre le Gestionnaire de communauté et les participants. Les connexions disponibles dépendent des capacités B2B des participants. Les capacités B2B sont basées sur les interactions que vous avez créées. Ces dernières dépendent de la disponibilité des définitions de flots de documents.

Pour certains échanges, une seule connexion est requise. Par exemple, c'est le cas si un participant envoie un document binaire à une application dorsale du

Gestionnaire de communauté. 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 B2B. Par exemple, si vous définissez **Heure d'accuser réception** sur 60 au niveau des fonctionnalités B2B pour le regroupement 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 participants et applications impliqués.

Exemple de flot

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

1. Sur la page Gérer les définitions de flot de documents, vérifiez que la définition du flot de documents (qui décrit le type de document envoyé dans le concentrateur par le participant de la communauté) est activée.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
   b. Cliquez sur l'icône **Développer** en regard de **Regroupement : AS**. Notez que **EDI-X12** figure déjà dans la liste.
   c. Cliquez sur l'icône **Développer** en regard de **Protocole : EDI-X12**. Notez que **Flot de documents : ISA** figure déjà dans la liste.
2. Sur la page Gérer la définition du flot de documents, vérifiez que la seconde définition de flot de documents (qui décrit le type de document envoyé à l'application dorsale) est activée.
   a. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**. Notez que **EDI-X12** figure déjà dans la liste.
   b. Cliquez sur l'icône **Développer** en regard de **Protocole : EDI-X12**. Notez que **Flot de documents : ISA** figure déjà dans la liste.
3. Créez une interaction indiquant si le flot de documents sera un flot source ou un flot cible.
   a. La page Gérer la définition du flot de documents étant toujours affichée, cliquez sur **Gérer les interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Dans la colonne Source, développez **Regroupement : AS**, **Protocole : EDI-X12 (TOUT)**, puis cliquez sur **Flot de documents : ISA**.
   d. Dans la colonne Cible, développez **Regroupement : Aucun**, **Protocole : EDI-X12 (TOUT)**, et cliquez sur **Flot de documents : ISA**.
   e. Dans cet exemple, aucune transformation n'a lieu. Par conséquent, ne sélectionnez aucun élément dans la liste **Mappe de transformation**.
   f. Dans la liste des **actions**, sélectionnez **Passe-système**.
   g. Cliquez sur **Enregistrer**.

A ce point, vous avez précisé si le concentrateur accepte les échanges EDI-X12 (standard ISA) regroupés en tant que AS. Vous avez également indiqué qu'il est capable d'en envoyer sans regroupement. 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).

Vous n'avez pas encore précisé quel participant peut envoyer ce type d'EDI au concentrateur. Pour cela, vous devez définir le profil et les capacités B2B du participant. (Définissez également un profil et les capacités B2B du système dorsal du Gestionnaire de communauté.) Une fois ces tâches effectuées, créez une connexion entre le participant et l'application dorsale. La figure 20 illustre la connexion entre le participant et l'application dorsale du Gestionnaire de communauté, dans le cadre de cet exemple.

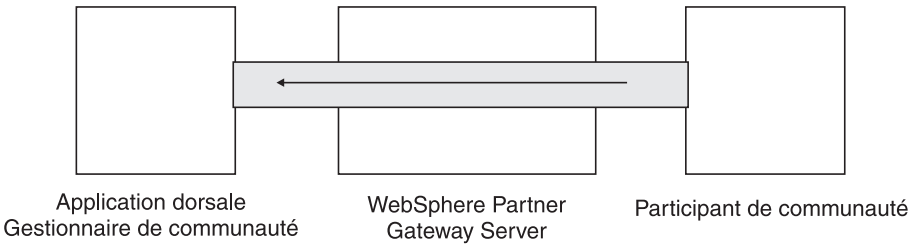

Figure 20. Connexion unidirectionnelle depuis un participant vers un Gestionnaire de communauté

Vous pouvez vérifier l'existence d'une connexion dans la page Gestion des connexions (**Administrateur du compte > Connexions du participant**). Sur la page Gestion des connexions, sélectionnez le participant dans la liste des **Sources**, le Gestionnaire de communauté dans la liste des **Cibles**, 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 flots 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 flot 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 transmis tels quels au concentrateur. Par conséquent, l'échange de documents binaires entre un participant de la communauté et une application dorsale du Gestionnaire de communauté se fait de façon directe. Le protocole binaire est déjà disponible pour les regroupements AS, Aucun et Intégration dorsale. De ce fait, l'«Etape 1 : Assurez-vous que la définition de flot de documents est disponible», à la page 63 est déjà effectuée.

Remarque : Vous pouvez ajouter des attributs à tous les niveaux (Regroupement, Protocole ou Flot de documents) pour modifier le traitement par défaut, en cliquant sur l'icône **Edition des valeurs d'attribut**. Aucun attribut n'est associé par défaut au protocole binaire ou au flot de documents.

De même, quatre interactions impliquant des documents binaires sont déjà fournies par défaut et n'exigent pas d'appliquer l'Etape 2 : Créez des interactions. Des interactions sont fournies pour les échanges suivants :

Tableau 4. Interactions fournies par le système

Regroupement/protocole/flot de documents source	Regroupement/protocole/flot de documents cible
AS/binaire/binaire	Intégration dorsale/binaire/binaire
Intégration dorsale/binaire/binaire	AS/binaire/binaire
AS/binaire/binaire	Aucun/binaire/binaire
Aucun/binaire/binaire	AS/binaire/binaire

Pour échanger des documents binaires, vous devez toujours appliquer les étapes suivantes :

- Etape 3 : Créez les profils, capacités B2B et les passerelles des participants, au Chapitre 9, «Création du profil du Gestionnaire de communauté et des capacités B2B», à la page 131, Chapitre 11, «Création de participants et de leurs capacités B2B», à la page 155 et Chapitre 10, «Création de passerelles», à la page 135.
- Etape 4 : Activez les connexions, au Chapitre 12, «Gestion des connexions», à la page 159.

Documents EDI avec actions de passe-système

WebSphere Partner Gateway offre la possibilité de désenvelopper et transformer des EDI. Cette procédure est décrite au Chapitre 8, «Configuration des flots de documents EDI», à la page 91.

La figure 21 illustre le flot d'un EDI transmis d'un participant au Gestionnaire de communauté.

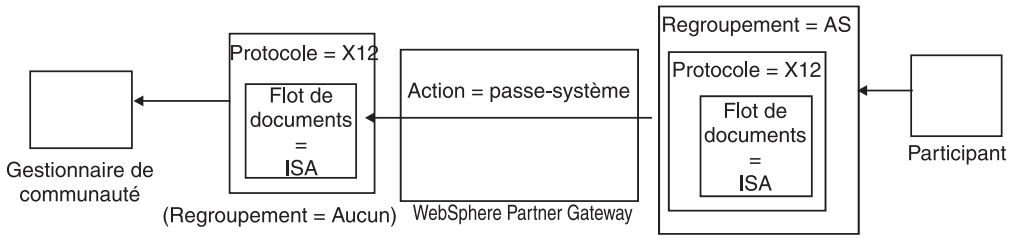

Figure 21. EDI entrant avec action passe-système

Dans cet exemple, les en-têtes AS2 sont supprimés, mais le reste de l'EDI est laissé intact et traverse le système vers la passerelle du Gestionnaire de communauté.

Création de définitions de flots de documents

Le flot de documents pour les échanges de passe-système EDI est déjà disponible (par défaut) sur la page Gérer des définitions de flots de documents, décrite dans la section «Exemple de flot», à la page 65. 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 flot de documents.

Supposons que vous souhaitiez modifier l'attribut **Heure d'accuser réception** d'un document EDI regroupé avec AS. Voici comment procéder :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur l'icône **Edition des valeurs d'attribut** en regard de **Regroupement : AS**.
3. Faites défiler la page vers le bas, jusqu'à la section **Attributs de contexte du flot de documents**.
4. Sur la ligne **Heure d'accuser réception**, tapez une valeur différente dans la colonne **Mettre à jour**.
5. Cliquez sur **Enregistrer**.

Notez que, dans cet exemple, vous avez modifié un attribut de regroupement. Les attributs de flot de protocole (par exemple, EDI-X12) et de flot de documents (par exemple, ISA) ne conviennent pas à une action de passe-système. Cet attribut de regroupement s'applique à tous les documents compris dans le regroupement AS.

Création d'interactions

Pour créer l'interaction pour un EDI avec action passe-système, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Dans la page Gérer les définitions du flot de documents, cliquez sur **Gérer les interactions**.
3. Cliquez sur **Création d'une interaction**.
4. Sous **Source**, développez **Regroupement : AS** et **Protocole : EDI-X12**, puis sélectionnez **Flot de documents : ISA**.
5. Sous **Cible**, développez **Regroupement : Aucun** et **Protocole : EDI-X12**, puis sélectionnez **Flot de documents : ISA**.
6. Dans la liste des **actions**, sélectionnez **Passe-système**.

Les étapes 1 à 6 ont permis à WebSphere Partner Gateway d'accepter un échange EDI-X12 regroupé en tant que AS, à partir d'un participant source, pour envoyer un échange EDI-X12 sans regroupement vers le participant cible et autoriser le transfert passe-système de la source vers la cible.

Si vous souhaitez définir une interaction avec un document source regroupé en tant que Aucun/EDI-X12/ISA et un document cible regroupé en tant que AS/EDI-X12/ISA, développez **Regroupement : Aucun** à l'étape 4 (dans la colonne **Source**) puis développez **Regroupement : AS** à l'étape 5 (dans la colonne **Cible**).

Documents RosettaNet

Cette section propose des informations générales sur les documents RosettaNet et vous indique comment définir des définitions de flots de documents et interactions pour ces documents.

Généralités

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 de regroupement de messages, de protocoles de transfert et de sécurité. Deux versions ont été publiées : 1.1 et 2.0. Un 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 le regroupement du message transformé en un message RNSC (RosettaNet Service Content) que le système dorsal peut traiter. Pour plus d'informations sur le regroupement utilisé avec ces messages pour fournir des informations d'acheminement, reportez-vous au *Guide d'intégration d'entreprise*.

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 participant). Vous fournissez les définitions de flot 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'événement 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 participants 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*.

Regroupements de flot de documents RNIF et PIP

Pour prendre en charge l'échange de messages RosettaNet, WebSphere Partner Gateway fournit deux jeux de fichiers compressés appelés regroupements. Les *regroupements RNIF* comportent définitions de flot de documents nécessaires pour prendre en charge le protocole RNIF. Ces regroupements se trouvent dans le répertoire B2BIntegrate.

Pour RNIF V1.1, les regroupements sont :

- Package_RNIF_1.1.zip
- Package_RNSC_1.0_RNIF_1.1.zip

Pour RNIF V02.00, les regroupements sont :

- Package_RNIF_V02.00.zip
- Package_RNSC_1.0_RNIF_V02.00.zip

Le premier regroupement de chaque paire fournit les définitions de flot de documents requises pour la prise en charge des communications RosettaNet avec les participants, tandis que le second fournit les définitions nécessaires pour la prise en charge des communications RosettaNet avec les systèmes dorsaux.

Le second jeu se compose de regroupements de flot de documents PIP. Chaque regroupement de flot 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 flot 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 regroupements de flot 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 regroupements de flot de documents PIP :

- Pour l'échange de messages RNIF 1.1 avec les participants
- Pour l'échange de messages RNIF 1.1 avec les systèmes dorsaux
- Pour l'échange de messages RNIF 2.0 avec les participants
- Pour l'échange de messages RNIF 2.0 avec les systèmes dorsaux

Chaque regroupement de flot 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 participants 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 regroupement. Pour les regroupements de flot de documents PIP destinés à l'échange de messages entre WebSphere Partner Gateway et les participants, le format est le suivant :

`BCG_Package_RNIF<version_RNIF>_<PIP><version_PIP>.zip`

Pour les regroupements de flot 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 regroupement 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 participants et WebSphere Partner Gateway à l'aide du protocole RNIF 1.1. Quant aux regroupements de flot 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 le regroupement utilisé avec ces messages, reportez-vous au *Guide d'intégration d'entreprise*.

Création de définitions de flots de documents

Pour l'échange de messages RosettaNet, WebSphere Partner Gateway exige les regroupements RNIF de la version utilisée pour envoyer les messages. Pour chaque processus PIP pris en charge par WebSphere Partner Gateway, il faut les deux regroupements de flot 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 regroupements 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 regroupement prend en charge l'échange de messages RosettaNet avec les participants, le second l'échange de messages RosettaNet avec les systèmes dorsaux. Les troisième et quatrième regroupements permettent à WebSphere Partner Gateway de transmettre des messages 3A4 entre des participants et des systèmes dorsaux par le biais du protocole RNIF 2.0.

Pour télécharger des regroupements RosettaNet :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Téléchargement des regroupements**.
3. Sélectionnez **Non** pour **Regroupement WSDL**.
4. Cliquez sur **Parcourir** et sélectionnez le regroupement RNIF pour communiquer avec les participants.

   Par défaut, les regroupements RNIF sont situés dans le répertoire B2BIntegrate/Rosettanet du support d'installation. Par exemple, pour télécharger le regroupement 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 regroupement RNIF pour communiquer avec les applications dorsales.

   Par exemple, pour télécharger le regroupement 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 regroupements nécessaires pour communiquer avec les participants 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 **Regroupement : RNIF/Protocole : RosettaNet**, qui représente le regroupement pour communiquer avec les participants, et **Regroupement : Intégration dorsale/Protocole : RNSC**, qui est le regroupement pour communiquer avec les applications dorsales.
9. Pour chaque PIP que vous souhaitez prendre en charge, téléchargez le regroupement de flot 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 participant, 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 flot de documents sous **Regroupement : 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 flot de documents sous **Regroupement : Intégration dorsale/Protocole : RNSC** , sur la page Gérer les définitions de flots de documents. Si WebSphere Partner Gateway ne fournit pas de regroupement pour le processus ou la version PIP que vous souhaitez utiliser, vous pouvez créer votre propre regroupement et le télécharger. Pour plus d'informations, voir «Création de regroupements de flot de documents PIP», à la page 241.

Configuration des valeurs d'attribut

Pour les définitions de flot 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 :

Regroupement RNIF (1.0)

- **GlobalSupplyChainCode** - Identifie le type de chaîne d'approvisionnement utilisée par le participant. Les différents types sont Composants électroniques, Technologie d'informations et Fabrication de semiconducteurs. Cet attribut n'a pas de valeur par défaut.

Regroupement 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 participant 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 regroupements de flot 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 à sens unique, cependant, vous voyez le document entrant sur la console et un code 0KB 200 est renvoyé au participant.

Pour définir les attributs, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur les icônes **Développer** pour développer un noeud jusqu'au niveau Définition du flot de documents approprié, ou sélectionnez **Tout** pour développer tous les noeuds de définition de flot de documents de l'arborescence.
3. Dans la colonne **Actions**, cliquez sur l'icône **Edition des valeurs d'attribut** du regroupement que vous souhaitez modifier (par exemple Regroupement : RNIF (1.1) ou Regroupement : RNIF (V02.00)).
4. Dans la section **Attributs de contexte du flot de documents**, allez dans la colonne **Mettre à jour** de l'attribut que vous souhaitez définir et sélectionnez ou entrez la nouvelle valeur dans la zone. Répétez l'opération pour chaque attribut à définir.
5. Cliquez sur **Enregistrer**.

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 160.

Création d'interactions

La procédure suivante décrit la création d'une interaction entre un système dorsal et un participant. 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 flot de documents RNIF ont été téléchargées, ainsi que les regroupements 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 72.

Pour créer une interaction pour un PIP particulier, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**.
3. Cliquez sur **Création d'une interaction**.
4. Développez l'arborescence **Source** jusqu'au niveau **Action** et l'arborescence **Cible** jusqu'au niveau **Action**.
5. Dans les arborescences, sélectionnez les définitions de flot de documents à utiliser pour les contextes source et cible. Par exemple, si le participant est l'initiateur d'un processus PIP 3C6 (PIP à une action), sélectionnez les définitions de flot de documents suivantes :

Tableau 5. Processus PIP 3C6 lancé par un participant

Source	Cible
Regroupement : RNIF (V02.00)	Regroupement : Intégration dorsale (1.0)
Protocole : RosettaNet (V02.00)	Protocole : RNSC (1.0)
Flot de documents : 3C6 (V01.00)	Flot de documents : 3C6 (V01.00)
Activité : Notification d'avis de paiement	Activité : Notification d'avis de paiement

Tableau 5. Processus PIP 3C6 lancé par un participant (suite)

Source	Cible
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 flot de documents suivantes :

Tableau 6. Processus PIP 3C6 lancé par un système dorsal

Source	Cible
Regroupement : Intégration dorsale (1.0)	Regroupement : RNIF (V02.00)
Protocole : RNSC (1.0)	Protocole : RosettaNet (V02.00)
Flot de documents : 3C6 (V01.00)	Flot de documents : 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 participant, sélectionnez les définitions de flot de documents suivantes pour la première action :

Tableau 7. Processus PIP 3A4 lancé par un participant

Source	Cible
Regroupement : RNIF (V02.00)	Regroupement : Intégration dorsale (1.0)
Protocole : RosettaNet (V02.00)	Protocole : RNSC (1.0)
Flot de documents : 3A4 (V02.02)	Flot 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 flot de documents suivantes pour la première action :

Tableau 8. Processus PIP 3A4 lancé par un système dorsal

Source	Cible
Regroupement : Intégration dorsale (1.0)	Regroupement : RNIF (V02.00)
Protocole : RNSC (1.0)	Protocole : RosettaNet (V02.00)
Flot de documents : 3A4 (V02.02)	Flot 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

6. Dans la zone Action, sélectionnez **Translation bidirectionnelle de RosettaNet et de RosettaNet Service Content avec Validation**.
7. Cliquez sur **Enregistrer**.
8. 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 flot de documents suivantes pour la seconde action d'un processus PIP 3A4 lancé par un participant. Il s'agit de l'action par laquelle le système dorsal envoie la réponse.

Tableau 9. Processus PIP 3A4 lancé par un participant (seconde action)

Source	Cible
Regroupement : Intégration dorsale (1.0)	Regroupement : RNIF (V02.00)
Protocole : RNSC (1.0)	Protocole : RosettaNet (V02.00)
Flot de documents : 3A4 (V02.02)	Flot 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 flot de documents suivantes :

Tableau 10. Processus PIP 3A4 lancé par un système dorsal (seconde action)

Source	Cible
Regroupement : RNIF (V02.00)	Regroupement : Intégration dorsale (1.0)
Protocole : RosettaNet (V02.00)	Protocole : RNSC (1.0)
Flot de documents : 3A4 (V02.02)	Flot 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

9. Si vous voulez générer la Notification of Failure 0A1, créez une interaction pour XMLEvent.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
   b. Cliquez sur **Gestion des interactions**.
   c. Cliquez sur **Création d'une interaction**.
   d. Développez l'arborescence **Source** jusqu'au niveau **Flot de documents** et l'arborescence **Cible** jusqu'au niveau **Flot de documents**.
   e. Sélectionnez les définitions de flots de documents suivants :

Tableau 11. Définition d'un flot de documents d'événement XML

Source	Cible
Regroupement : Intégration dorsale (1.0)	Regroupement : Intégration dorsale (1.0)
Protocole : XMLEvent (1.0)	Protocole : XMLEvent (1.0)
Flot de documents : XMLEvent (1.0)	Flot de documents : XMLEvent (1.0)

   f. Dans la zone Action, sélectionnez **Passe-système**.
   g. Cliquez sur **Enregistrer**.
10. Création d'une interaction pour XMLEvent vers 0A1 RNSC.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
   b. Cliquez sur **Gestion des interactions**.
   c. Cliquez sur **Création d'une interaction**.
   d. Développez l'arborescence **Source** jusqu'au niveau **Flot de documents** et l'arborescence **Cible** jusqu'au niveau **Activité**.

e. Sélectionnez les définitions de flots de documents suivants :

Tableau 12. Définition d'un flot de documents d'événement XML à 0A1

Source	Cible
Regroupement : Intégration dorsale (1.0)	Regroupement : Intégration dorsale (1.0)
Protocole : XMLEvent (1.0)	Protocole : RNSC (1.0)
Flot de documents : XMLEvent (1.0)	Flot de documents : 0A1 (V02.00)
	Activité : Distribution de notification d'échec.

f. Dans la zone Action, sélectionnez **Conversion bidirectionnelle de RosettaNet et XML avec Validation**.

g. Cliquez sur **Enregistrer**.

Services Web

Un participant peut demander un Service Web fourni par le Gestionnaire de communauté. Un Gestionnaire de Communauté peut également demander un Service Web fourni par un participant. Le participant ou le Gestionnaire de communauté appelle le serveur WebSphere Partner Gateway pour obtenir le Service Web. 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.

La présente section comprend les informations suivantes pour configurer un Service Web qui sera utilisé par un participant ou Gestionnaire de communauté.

- Identification des participants pour un Service Web
- Configuration d'une définition de flot de documents pour un service Web
- Ajout d'une définition de flot de documents aux capacités B2B d'un participant
- Restrictions et limitations relatives à un support de Service Web

Identification des participants pour un Service Web

Lorsqu'un Service Web est fourni par le Gestionnaire de communauté pour être utilisé par des participants, WebSphere Partner Gateway impose que le participant s'identifie. Lorsque vous postez la demande de Service Web, définissez l'identité de l'une des façons suivantes :

1. Utilisez l'authentification de base HTTP avec un ID utilisateur de la forme *<ID métier du participant>/<nom de l'utilisateur de la console>* (par exemple 123456789/joesmith), et le mot de passe du nom d'utilisateur de la console.
2. Présentez un certificat client SSL qui a déjà été chargé dans WebSphere Partner Gateway pour le participant.

Lorsque le Service Web est fourni par un participant pour être utilisé par le Gestionnaire de communauté, l'URL public utilisé par le Gestionnaire de communauté pour appeler le Service Web ne doit pas contenir la chaîne de requête `?to=<ID métier du participant>` . Exemple :

`http://<adresse_IP>/bcgreceiver/Receiver?to=123456789`

Ceci indique à WebSphere Partner Gateway que le fournisseur du Service Web est le participant dont l'ID métier est 123456789.

Création de définitions de flots de documents

Pour effectuer la définition de flot de documents, téléchargez les fichiers WSDL (Web Service Definition Language) qui définissent le Service Web, ou entrez manuellement les définitions équivalents de flots de documents par la Console de communauté.

Téléchargement de fichiers WSDL pour un Service Web

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"/>
```

Et que le fichier WSDL `bindingRPC.wsdl` importé contient l'élément import suivant :

```
<import namespace="http://www.helloworld.com/wsdl/helloRPC.wsdl" location=
"port/porttypeRPC.wsdl"/>
```

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 WebSphere Partner Gateway. Ils sont transmis directement, avec l'URL du point d'extrémité du service d'origine.) 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 regroupements. 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 passerelle 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 : Les 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 du flot de documents**.
2. Cliquez sur **Téléchargement des regroupements**.
3. Pour **Module WSDL**, cliquez sur **Oui**.
4. Pour **URL public du Service Web**, appliquez une des procédures suivantes :
   - Si le Service Web est fourni par le Gestionnaire de communauté (qui sera appelé par un participant), entrez l'URL public du Service Web, Exemple :

     `https://<hôte_cible:port>/bcgreceiver/Receiver`

     L'URL correspond généralement à la cible HTTP de production définie dans les cibles.
   - Si le Service Web est fourni par un participant (qui sera appelé par le Gestionnaire de communauté), tapez l'URL public avec une chaîne de requête. Exemple :

     `https://<hôte_cible:port>/bcgreceiver/Receiver?to=<ID_métier_du_participant>`
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 regroupements 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 flot de documents

Pour entrer manuellement les définitions équivalentes de flot de documents, suivez les procédures indiquées dans cette section. Vous devez également créer individuellement le flot 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 flot de documents en terme de regroupement, protocole, flot de documents, activité et hiérarchie des actions, un Service Web pris en charge se présente comme suit :

- **Regroupement : Aucun**
- **Protocole : Service Web (1.0)**
- **Flot de documents :** {*<espace-nom_du_Service_Web>*:*<nom_du_Service_Web>*} (nom et code), qui doit être unique parmi les flots 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 = premier_enfant_de_soap:body>*}:
  <nom_élément_xml_identifiant = 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 participant. 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 flot 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

Pour créer une interaction pour un Service Web, utilisez la même action de flot de documents de Service Web pour la source et la cible.

Pour créer des interactions, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**.
3. Cliquez sur **Création d'une interaction**.
4. Sous **Source**, développez **Regroupement : Aucun > Protocole : Service Web > Flot de documents : <** *flot de documents*> **> Action :** <*action*>. Répétez cette étape 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 la prise en charge 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 :

- 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).
- Soap avec les pièces jointes n'est pas pris en charge.

Documents cXML

La présente section propose une vue d'ensemble de la prise en charge cXML ainsi que des informations relatives à la création de définitions du flot de documents pour les échanges cXML.

Généralités

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 est pour 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 flot de documents cXML. Pour plus d'informations sur l'association du DTD avec le flot de documents cXML, voir «Association de mappes à des définitions de flot de documents», à la page 89.

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 du document.

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. L'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 commercial 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 de réponse cXML. La document de 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 à la définition du flot 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 flot de documents dans WebSphere Partner Gateway :

Elément cXML	**Définition de flot de documents**
DOCTYPE cXML	Protocole
Version DTD	Version de protocole
Demande (type) Par exemple, OrderRequest	Flot de document

Réponse : Le participant cible envoie une réponse cXML pour indiquer au participant 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 flot de documents de WebSphere Partner Gateway :

Elément cXML	Définition de flot de documents
DOCTYPE cXML	Protocole
Version DTD	Version de protocole
Réponse (type) Par exemple, ProfileResponse	Flot de document

Message : Un message cXML contient les informations de flot 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 flot de documents créé dans WebSphere Partner Gateway. Dans l'exemple suivant, SubscriptionChangeMessage est le flot 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 flot de documents de WebSphere Partner Gateway :

Elément cXML	Définition de flot de documents
DOCTYPE cXML	Protocole
Version DTD	Version de protocole
Message	Flot 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 flot de documents cXML :

- D'un participant au Gestionnaire de communauté : Aucun/cXML vers Aucun/cXML avec Passe-système et validation
- Du Gestionnaire de communauté à un participant :
  - Aucun/cXML à Aucun/cXML avec Passe-système et validation
  - Aucun/XML à Aucun/cXML avec Passe-système, validation et transformation

Création de définitions de flots de documents

Procédez comme suit pour créer une définition de flot 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 flot de documents. La version par défaut est 1.2.009.

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **Définition du flot de documents**.
2. Cliquez sur **Création d'une définition du flot de documents**. La page Création d'une définition du flot de documents s'affiche.
3. Sélectionnez **Flot de documents** comme type de flot de documents.
4. Selon le type de document, appliquez l'une des étapes suivantes :
   - Pour les demandes, entrez son type (par exemple `OrderRequest`) dans les zones **Code** et **Nom**
   - Pour les réponses, si Response n'a aucun autre code enfant que `<Status>` , entrez `Response`. Sinon, entrez le nom de code 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 **Regroupement : Aucun** pour étendre les options de sélection de regroupement.
11. Sélectionnez **Protocole : cXML (1.2.009): cXML**.
12. Cliquez sur **Enregistrer**.

Création d'interactions

Après avoir créé la définition du flot de documents, définissez une interaction pour le document cXML.

Pour créer des interactions, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur** > **Configuration du concentrateur** > **Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**.
3. Cliquez sur **Création d'une interaction**.
4. Si le document cXML est la source, sous **Source**, développez **Regroupement : Aucun** et **Protocole : cXML**, puis sélectionnez **Flot de documents :**<*document_flow*>. Si le document cXML est la cible, développez **Regroupement : Aucun** et **Protocole : cXML**, puis sélectionnez **Flot de documents :** <*document_flow*> dans la colonne **Cible**.
5. 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 regroupement et le protocole et sélectionnez son flot de documents.
6. 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.)

Création de documents XML personnalisés

Cette section explique comment créer des documents XML personnalisés.

Généralités

XML (Extensible Markup Language) est le format universel des documents et des données structurés à l'échelle du Web. Dans la page Gestion des protocoles XML,

vous pouvez créer et gérer les formats XML personnalisés qui pourront être ajoutés à la liste des définitions de flot de documents disponibles.

Un format XML définit les chemins parmi un ensemble de documents XML. Il permet au Gestionnaire de documents de récupérer les valeurs qui identifient de façon unique un document et d'accéder aux informations contenues dans le document qui s'avèrent nécessaires à un acheminement et à un traitement corrects.

La procédure de création d'un format XML comporte plusieurs étapes. Vous devez en effet :

1. créer un protocole pour le format et l'associer à un ou plusieurs regroupements ;
2. créer un flot de documents pour le format et l'associer au protocole nouvellement créé ;
3. créer le format.

Vous devez ensuite créer une interaction correcte pour le nouveau format.

Ces étapes sont décrites dans les sections qui suivent. Vous trouverez également un exemple de ces étapes à la section «Configuration du concentrateur pour les documents XML personnalisés», à la page 201.

Création d'un format de définition de protocole

La procédure suivante explique comment créer un format de définition de protocole XML personnalisé :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définitions du flot de documents > Création de définition de flot de documents**.
2. Dans la liste déroulante **Type de flot de documents**, sélectionnez **Protocole**.
3. Dans la zone **Code**, indiquez la valeur du type d'objet que vous avez sélectionné à l'étape précédente. Par exemple, vous pouvez entrer XML.
4. Dans la zone **Nom**, indiquez un identificateur pour la définition de flot de documents. Par exemple, pour un protocole XML personnalisé, vous pouvez entrer XML_Personnalisé. Cette zone doit être renseignée.
5. Dans la zone **Version**, entrez **1.0**.
6. Entrez éventuellement une description du protocole.
7. Donnez au paramètre **Niveau du document** la valeur **Non**, car vous définissez un protocole et non un flot de documents (que vous définirez dans la section suivante).
8. Réglez le paramètre **Etat** sur **Activé**.
9. Réglez le paramètre **Visibilité** pour ce protocole. Il est probable que vous souhaiterez le rendre visible à tous les participants.
10. Sélectionnez les regroupements dans lesquels ce nouveau protocole sera encapsulé. Par exemple, si vous souhaitez que ce protocole soit associé aux trois regroupements, sélectionnez **Regroupement : AS**, **Regroupement : Aucun** et **Regroupement : Intégration dorsale**.
11. Cliquez sur **Enregistrer**.

Création d'une définition de flot de documents

Ensuite, utilisez de nouveau la page Création d'une définition du flot de documents pour créer un flot de documents.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définitions du flot de documents > Création de définition de flot de documents**.
2. Dans la liste déroulante **Type de flot de documents**, sélectionnez **Flot de documents**.
3. Dans la zone **Code**, indiquez la valeur du type d'objet (flot de documents) que vous avez sélectionné à l'étape précédente.
4. Dans la zone **Nom**, indiquez un identificateur pour la définition de flot de documents. Par exemple, vous pouvez entrer Testeur_XML comme nom de flot de documents. Cette zone doit être renseignée.
5. Dans la zone **Version**, entrez **1.0**.
6. Entrez éventuellement une description du protocole.
7. Donnez au paramètre **Niveau du document** la valeur **Oui** (car vous définissez un niveau de document).
8. Réglez le paramètre **Etat** sur **Activé**.
9. Réglez le paramètre **Visibilité** pour ce flot. Il est probable que vous souhaiterez le rendre visible à tous les participants.
10. Cliquez sur l'icône **Développer** pour développer chaque regroupement sélectionné lors de l'étape 10, à la page 87. Développez le dossier, puis sélectionnez le nom du protocole créé à la section précédente (en l'occurrence, Protocole : XML_Personnalisé.).
11. Cliquez sur **Enregistrer**.

La page Gérer des définitions de flots de documents contient désormais un flot de documents Testeur_XMLpage et un protocole XML_personnalisé sous les regroupements AS, Aucun et Intégration dorsale.

Création d'un format XML

Une fois que vous avez créé un protocole XML personnalisé (et que vous l'avez associé avec un regroupement ou un groupe de regroupements) et que vous avez créé un flot de documents associé, vous pouvez créer le format XML.

Pour créer un format XML, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Formats XML**.
2. Cliquez sur **Création du format XML**.
3. Pour la zone **Format d'acheminement**, sélectionnez la définition de flot de documents avec laquelle ce format sera associé.
4. Dans la zone **Type de fichier**, sélectionnez **XML**.

   Remarque : XML est la seule option disponible pour le type de fichier.
5. Dans la zone **Type d'identificateur**, sélectionnez l'élément utilisé pour identifier le type de document entrant. Les options sont **DTD**, **Espace-nom** ou **Code racine**.
6. Pour chaque zone pour laquelle une option de ce type est fournie, sélectionnez **Chemin d'accès à l'élément**, qui est le chemin d'accès à la valeur dans le document, ou **Constante**, qui est la valeur réelle du document. Indiquez ensuite une valeur.
   a. Dans les zones **ID métier source/cible**, entrez le chemin d'accès de l'ID métier. Cette zone doit être renseignée.

b. Pour la zone **Flot & Version du flot de documents source**, entrez une expression qui définit le chemin d'accès au flot de documents et à la valeur de la version dans le document XML. Cette zone doit être renseignée.
c. Dans la zone **Identificateur du document**, entrez le chemin d'accès au numéro d'identification du document.
d. Dans la zone **Horodatage du document**, entrez le chemin d'accès pour l'horodatage de la création du document.
e. Pour les zone **Clé de vérification en double 1 à 5**, entrez les chemins permettant d'identifier l'acheminement d'un document en double.

7. Cliquez sur **Sauvegarder**.

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».

Ajout de mappes de validation

Vous pouvez associer une action à une mappe de validation pour être certain que le participant 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 du flot 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 flot de documents

Pour associer une mappe de validation à une définition du flot 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 du flot de documents.
3. Cliquez sur l'icône **Développer** en regard d'un regroupement pour le développer jusqu'au niveau voulu (par exemple **Action** pour un document RosettaNet).

4. Sélectionnez la définition du flot de documents que vous voulez associer à la mappe de validation.
5. Cliquez sur **Enregistrer**.

Affichage de documents

L'Afficheur de documents présente des informations sur les documents qui constituent un flot 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.

Pour ouvrir l'Afficheur de documents, cliquez sur **Afficheurs > Afficheur de documents**. Pour obtenir davantage d'informations sur l'Afficheur de documents, consulter le *Guide de l'administrateur*.

Chapitre 8. Configuration des flots de documents EDI

Le présent chapitre décrit la méthode de configuration des définitions de flots 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 67.

Vue d'ensemble de l'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 conversion 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 de l'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 transations 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 13. 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, à la page 93 illustre un exemple d'EDI X12, avec les segments qui le composent.

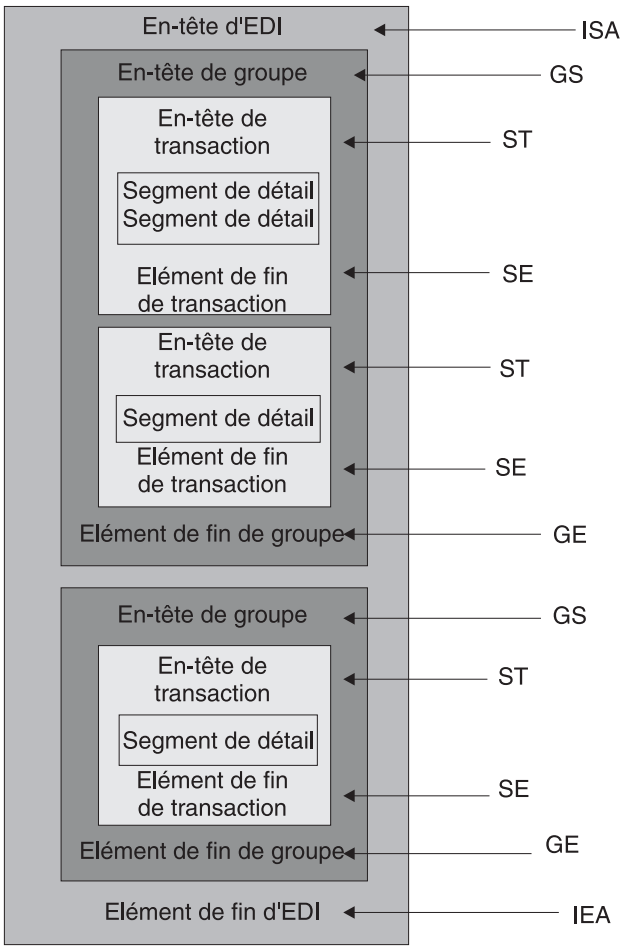

Figure 22. Une enveloppe d'EDI

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.

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 «Accusés de

réception fonctionnels», à la page 128 pour obtenir une liste de ces mappes. 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 conversion 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 participant ou du Gestionnaire de communauté télécharge régulièrement des documents à envoyer. Si plusieurs documents XML ou ROD arrivent dans un fichier, le Réceptionnaire appelle le récupérateur de l'utilitaire de fractionnement (XMLSplitterHander ou RODSplitterHandler) pour fractionner le groupe de documents. (Les récupérateurs d'utilitaires de fractionnement sont configurés lors de la création d'une cible. Pour plus d'informations, voir «Preprocess», à la page 51.) Les documents sont ensuite réintroduits dans le Gestionnaire de documents pour être traités individuellement.

Remarque : Les ID de l'émetteur et du réceptionnaire 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 Réceptionnaire appelle le récupérateur 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 flots de documents et de la définition des attributs

Une définition de flot de documents se compose, au minimum, d'un regroupement, d'un protocole et d'un flot de documents. Les définitions de flots de documents précisent les types de documents qui seront traités par WebSphere Partner Gateway.

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

Les sections suivantes décrivent rapidement les étapes de définition d'un flot de documents entre le Gestionnaire de communauté et un participant. Elles décrivent également les points où vous pouvez définir des attributs.

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

Avant de pouvoir envoyer ou recevoir un document, vous devez procéder à la définition du flot de documents auquel il sera lié. WebSphere Partner Gateway propose plusieurs définitions de flots 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 flot 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 flot de documents s'affiche sur la page. Vous pouvez créer vos propres définitions de flots de documents.

Lors de la définition d'un flot 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. Ils permettent un paramétrage global du regroupement, protocole ou flot de documents associé. Les attributs disponibles varient selon la définition du flot de documents. Les attributs des définitions de flots de documents EDI sont différents de ceux des définitions de flots de documents RosettaNet.

Par exemple, si vous spécifiez une valeur pour **Autoriser une requête TA1** au niveau du flot 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 capacités B2B pour un participant ou le Gestionnaire de communauté, cette valeur supplante celle qui était indiquée au niveau de la définition de flot de documents.

Pour les attributs qui peuvent être définis à plusieurs niveaux de la définition du flot de documents, les valeurs définies au niveau du flot de document prévalent sur celles définies au niveau du protocole, et ces dernières sont prioritaires sur celles paramétrées au niveau du regroupement. 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 flot de documents TA1, c'est ce dernier qui est utilisé.

Le flot de documents doit figurer sur la page Gérer des définitions de flots de documents pour que vous puissiez créer des interactions.

Etape 2 : Créez des interactions

Ensuite, vous définissez les interactions, qui sont des modèles pour créer les connexions des participants. Les interactions décrivent comment arrive le document, les traitements qu'il subit et comment il est envoyé depuis le concentrateur.

Pour certains protocoles, deux flots suffisent : un pour décrire le document reçu dans le concentrateur (de la part du participant ou du Gestionnaire de communauté) et un qui décrit le document envoyé depuis le concentrateur (au participant ou au Gestionnaire de communauté). 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, capacités B2B et les passerelles des participants

Ensuite, créez les profils des participants pour le Gestionnaire de communauté et les participants. Définissez des passerelles (qui déterminent quels documents seront envoyés) et les capacités B2B qui identifient les documents que le Gestionnaire de communauté ou un participant peuvent envoyer et recevoir. La page Capacités B2B répertorie tous les flots de documents définis.

Vous pouvez définir des attributs au niveau des capacités B2B. Tout attribut défini à ce niveau a la précédence sur ceux qui ont été définis au niveau de la définition du flot de documents. Par exemple, si vous définissez **Autoriser une requête TA1** sur **Non** au niveau de la définition du flot de documents pour les documents ISA, puis sur **Oui** au niveau des capacités B2B, la valeur **Oui** est utilisée. Le fait de définir un attribut au niveau B2B vous permet de le personnaliser pour un participant donné.

Si vous définissez le profil d'enveloppe au niveau du protocole ou du flot de documents (sur la page Gérer des définitions de flots de documents) puis sur une valeur différente sur la page des capacités B2B, c'est cette dernière valeur qui est utilisée.

Vous devez définir les profils et capacités B2B du Gestionnaire de communauté et des participants avant de pouvoir créer des connexions entre eux.

Etape 4 : Activez les connexions

Enfin, activez les connexions entre le Gestionnaire de communauté et les participants. Les connexions disponibles dépendent des capacités B2B des participants et des interactions que vous avez créées. Ces dernières dépendent de la disponibilité des définitions de flots de documents.

Pour certains échanges, une seule connexion est requise. Par exemple, c'est le cas si un participant envoie un document binaire à une application dorsale du Gestionnaire de communauté. 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 B2B. Par exemple, si vous définissez **Autoriser une requête TA1** sur **Oui** au niveau des capacité B2B, 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 participants et applications impliqués.

Vue d'ensemble des flots 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 «Procédure générale de définition d'échanges de documents», à la page 118.

Flot EDI vers EDI

WebSphere Partner Gateway peut accepter un EDI émis par un participant ou le Gestionnaire de communauté, le transformer en un type d'EDI différent (par exemple, EDI-X12 vers EDIFACT), puis envoyer le document au Gestionnaire de communauté ou au participant. 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, à la page 98 montre un EDI X12 composé de trois transactions désenveloppées. Les transactions sont transformées au format EDIFACT puis enveloppées et envoyées au participant.

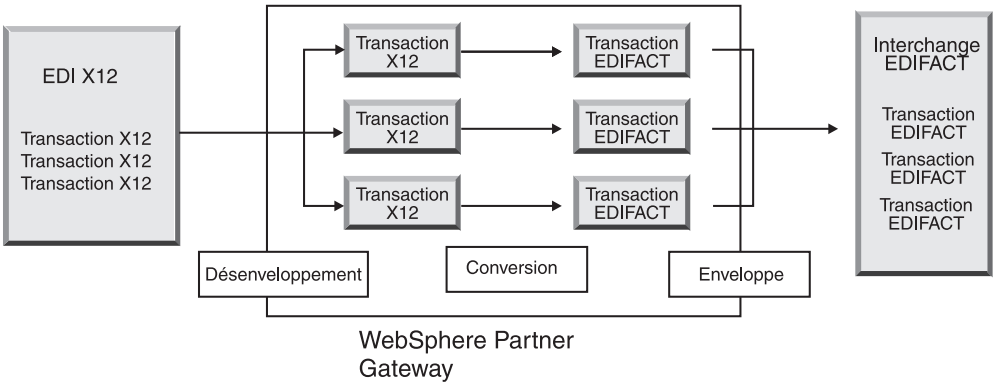

Figure 23. Flot EDI vers EDI

Une mappe de transformation est associée à chaque transaction et indique de quelle façon elle est transformée. 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 le «Enveloppeur», à la page 105 pour une description générale de l'Enveloppeur (un composant qui rassemble plusieurs transactions destinées à un participant, 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 106.

Une mappe de validation peut également être associée à la transaction.

Flot EDI vers XML ou ROD

WebSphere Partner Gateway peut accepter un EDI émis par un participant ou le Gestionnaire de communauté, le désenvelopper, et transformer les transactions EDI obtenues en documents XML ou ROD.

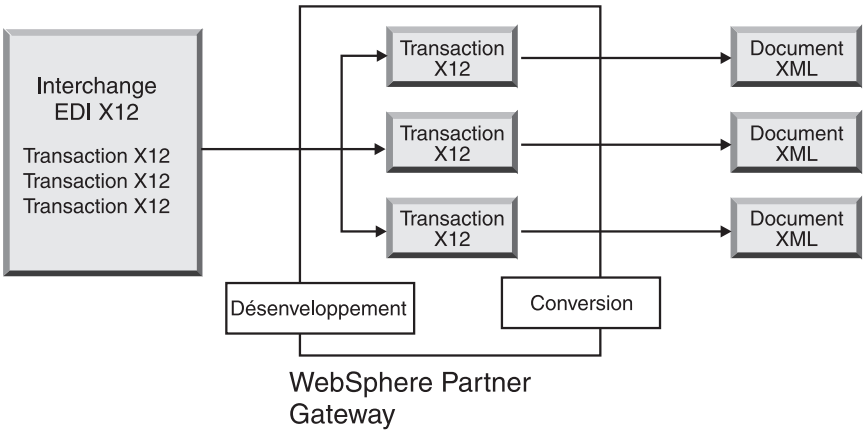

Figure 24. EDI vers un flot de documents XML

La transaction peut être transformée en un seul document ou en plusieurs, si le chaînage de mappe a été utilisé pour créer la mappe.

Flot XML ou ROD vers EDI

WebSphere Partner Gateway peut recevoir des documents XML ou ROD d'un participant ou du Gestionnaire de communauté, transformer les documents en transactions EDI, envelopper les transactions et les envoyer au Gestionnaire de communauté ou à un participant.

La figure 25 montre des documents XML transformés en transactions X12 puis enveloppés.

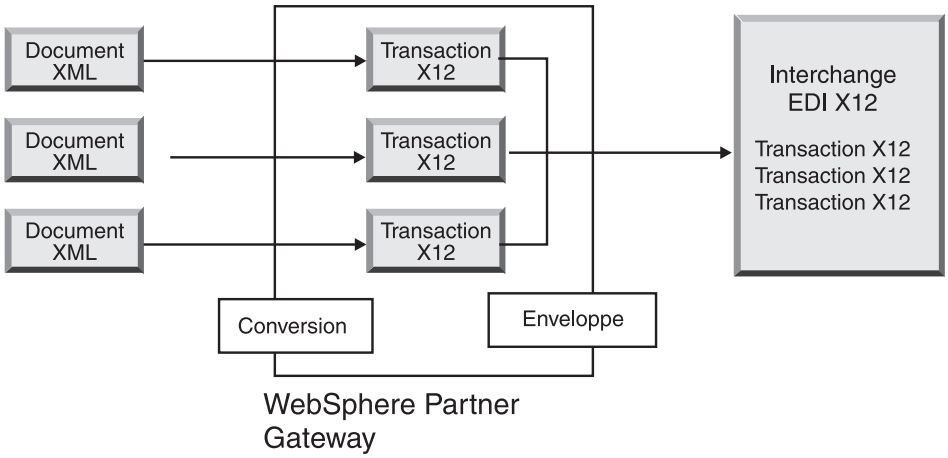

Figure 25. Flot de document XML en EDI

Un document peut être transformé en plusieurs transactions (si le chaînage de mappe a été utilisé), qui seront enveloppées en différents EDI. La figure 26 montre un document XML transformé en trois transactions X12. Deux des transactions sont enveloppées ensemble. La dernière est placée dans une enveloppe séparée.

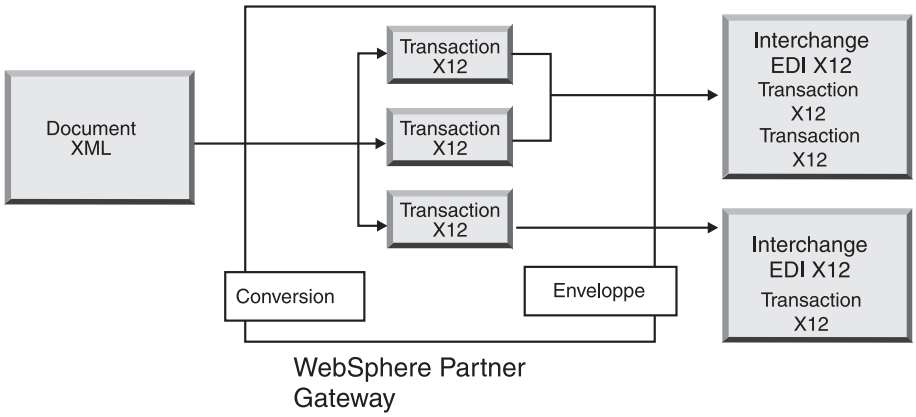

Figure 26. Flot de document XML vers plusieurs transactions EDI

Flot de plusieurs documents XML ou ROD vers EDI

WebSphere Partner Gateway peut recevoir un fichier composé d'un ou plusieurs documents XML ou ROD de la part d'un participant ou du Gestionnaire de communauté, le transformer en transactions EDI, placer les transactions EDI dans plusieurs enveloppes et les envoyer au Gestionnaire de communauté ou au participant.

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 montre le fractionnement d'un ensemble de documents XML pour obtenir des documents XML séparés. Les documents XML sont transformés en transactions X12 qui sont ensuite enveloppées.

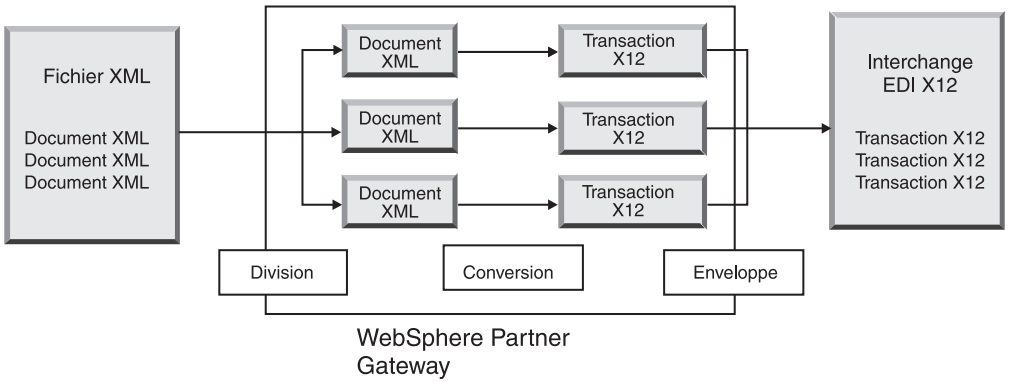

Figure 27. Flot de plusieurs documents XML vers un EDI

Dans figure 27, les documents sont fractionnés (par le récupérateur de fractionnement XML) et les transactions transformées sont enveloppées ensemble. Pour cela, le récupérateur 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 «Mode de traitement par lot», à la page 106.

Flot XML vers ROD ou ROD vers XML

WebSphere Partner Gateway peut recevoir un document XML ou ROD d'un participant ou du Gestionnaire de communauté, le transformer en tout autre type de document (XML vers ROD ou ROD vers XML), puis l'envoyer au participant ou au Gestionnaire de communauté.

La figure 28, à la page 101 montre plusieurs documents XML transformés en documents ROD.

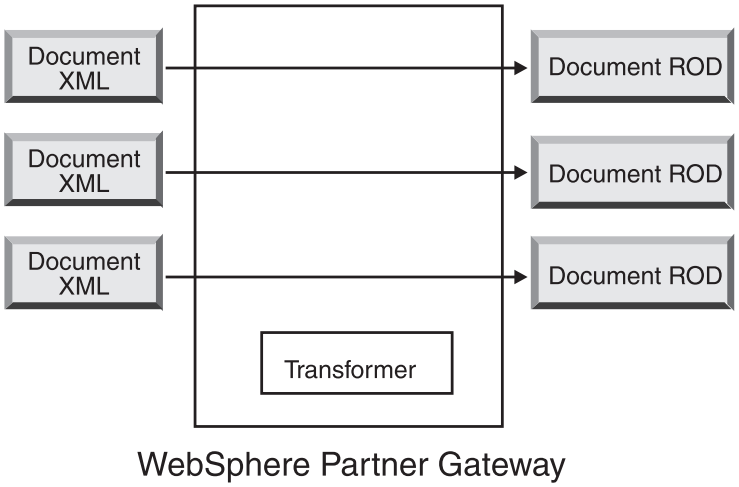

Figure 28. Flot de document XML en document ROD

Le document peut être transformé en un seul document ou en plusieurs si le chaînage de mappe a été utilisé pour créer la mappe.

Flot XML vers XML ou ROD vers ROD

WebSphere Partner Gateway peut recevoir un document XML ou ROD d'un participant ou du Gestionnaire de communauté, le transformer en document de même type (XML vers XML ou ROD vers ROD), puis l'envoyer au participant ou au Gestionnaire de communauté.

La figure 29 montre des documents XML transformés en documents XML de format différent.

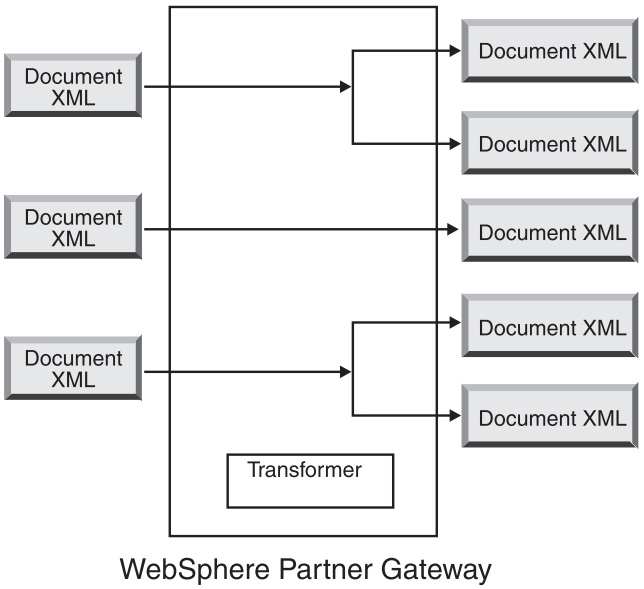

Figure 29. Flot de document XML en document XML

Le document peut être transformé en un seule document, ou en plusieurs si le chaînage de mappe a été utilisé pour créer la mappe.

Traitement des 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 participant pour indiquer que l'EDI a été reçu. Par conséquent, l'échange d'EDI exige plusieurs actions (comme leur désenveloppement, transformation et validation). 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 métiers des participants émetteurs et réceptionnaires, 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 réceptionnaire 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)
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 Gestionnaire de communauté, les documents sont transformés en transactions EDI standard. Les transactions EDI obtenues sont enveloppées avant d'être envoyées au participant. 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 114.

L'illustration qui suit montre comment un EDI, regroupé en tant que AS, est envoyé depuis un participant avec pour objectif de fournir deux documents XML transformés à deux passerelles différentes du système dorsal du Gestionnaire de communauté. 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.

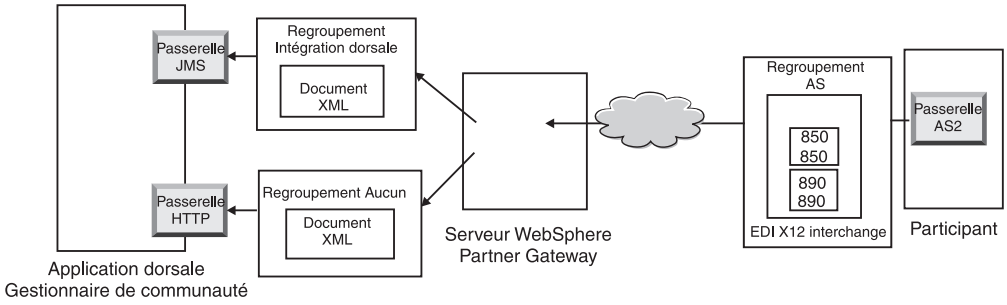

Figure 30. Flot général depuis un participant vers un Gestionnaire de communauté

Au lieu d'une seule connexion du participant vers le Gestionnaire de communauté, cet échange demande trois (?) connexions :

- Une du participant au concentrateur pour désenvelopper l'EDI. Comme il s'agit d'une étape intermédiaire (l'EDI est désenveloppé, mais n'est pas livré au participant), le côté cible de la connexion du participant est N/A.

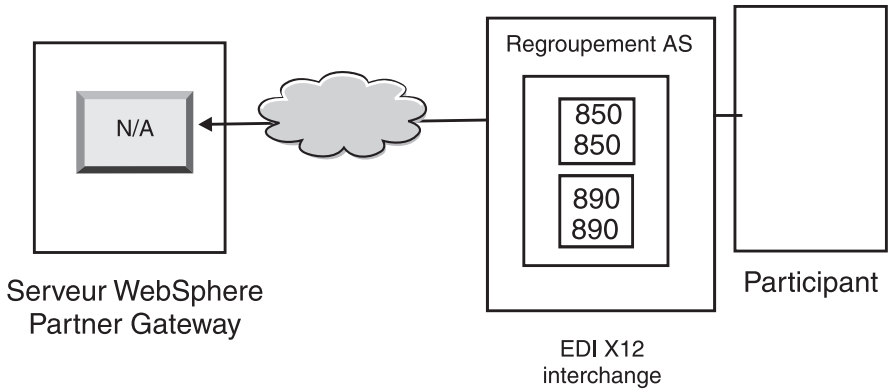

Figure 31. La connexion de désenveloppement

- Une pour la première transaction à transformer et à fournir à la passerelle JMS et au Gestionnaire de communauté, et une pour la seconde transaction à transformer et envoyer à la passerelle HTTP du Gestionnaire de communauté.

  Pour les transactions, le regroupement 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 **Regroupement : N/A** dans la connexion du participant.

  Pour la transaction qui est transformée en XML et qui va circuler vers l'application dorsale via JMS, la passerelle cible sur la connexion du participant doit être définie comme la passerelle JMS du Gestionnaire de communauté. Pour la transaction qui est transformée en XML et qui va circuler vers l'application dorsale via HTTP, la passerelle cible sur la connexion du participant doit être définie comme la passerelle HTTP.

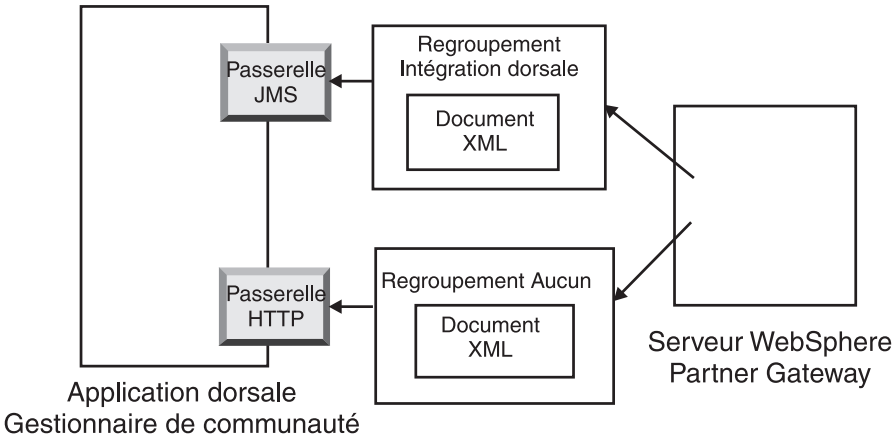

Figure 32. Connexions des transactions individuelles

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 de l'administrateur*.

Si l'émetteur exige des accusés de réception, vous devez mettre en place d'autres connexions :

- Une pour chaque accusé de réception renvoyé au participant. Les accusés de réception fonctionnels sont générés par le système. Par conséquent, le côté source de la connexion du participant doit être indiqué comme **Regroupement : N/A**. Les accusés de réception fonctionnels sont enveloppés avant d'être livrés. Par conséquent, le côté cible de la connexion du participant doit également être indiqué comme **Regroupement : N/A**. L'Enveloppeur rassemble les accusés de réception votre définition. Voir «Enveloppeur», à la page 105 pour plus d'informations sur la configuration du programme.
- Une pour envelopper les accusés de réception avant qu'ils ne soient renvoyés au participant. L'enveloppe est générée par le système. Par conséquent, le côté source de la connexion du participant doit être indiqué comme **Regroupement : N/A**. Le côté cible de la connexion du participant doit avoir la passerelle cible définie comme la passerelle du participant et, dans ce cas, avec **Regroupement : AS**. Vous pouvez soit utiliser une enveloppe par défaut pour le standard EDI, soit personnaliser des enveloppes. Voir «Profils d'enveloppe», à la page 107 pour plus d'informations sur la personnalisation des enveloppes.

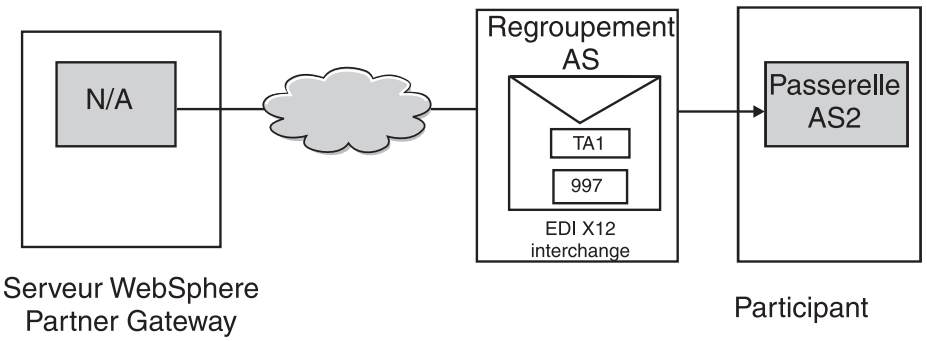

Figure 33. Enveloppement et envoi d'accusés de réception à l'émetteur

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 Gestionnaire de communauté, ils sont transformés en documents XML ou ROD ou en transactions EDI. Ces dernières sont enveloppées avant d'être envoyées au participant. 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.

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 système, 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 participant, 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 l'utilisateur 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 récupérateurs de fractionnement fait partie de la définition des cibles. Elle est décrite «Modification des points de configuration», à la page 51.) BCG_BATCHDOCS est l'un des attributs du récupérateur 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 fichie 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

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 une date 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.) **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.

6. Cliquez sur **Enregistrer**.

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 du flot 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 108.

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 des flots 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 flots de documents ou de la page Capacités B2B associée au participant) 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 capacités B2B.
3. Les attributs définis au niveau des capacités B2B sont prioritaires sur ceux qui ont été configurés au niveau de la définition du flot de documents.
4. Tous les attribus définis ailleurs (dans la mappe de transformation ou dans la définition du flot de documents, dans les capacités B2B 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 306.

Modification des valeurs par défaut

La section «Attributs de profil d'enveloppe», à la page 295 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. 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 réceptionnaire, à utiliser de la façon convenue entre les participants.
- Pour le standard EDIFACT, vous pouvez modifier les zones suivantes :
  - **UNB0101 : ID de syntaxe**, qui est l'dentification 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 réceptionnaires**, qui est le Mot de passe affecté par le réceptionnaire, à utiliser de la façon convenue entre les participants.
  - **UNB0602 : Référence des réceptionnaires/qualificatif de mot de passe**, qui est un qualificatif du Mot de passe du réceptionnaire, à utiliser de la façon convenue entre les participants.
  - **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 participant. 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 EDI, comme convenu avec le participant.
  - **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 réceptionnaire 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 : Réceptionnaire 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 réceptionnaire 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 réceptionnaire de l'application**, qui est le qualificatif du code d'ID de réceptionnaire. 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 réceptionnaire.

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 participants 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 **Enregistrer**.
8. Répétez les étapes 2, à la page 108 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 des profils de connexions avec des transactions désenveloppées et des EDI créés par l'Enveloppeur. Pour les transactions, le profil de connexion détermine le mode de traitement de la transaction une fois qu'elle est désenveloppé. Pour les EDI, le profil de connexion détermine leur mode de livraison.

La table suivante indique les attributs de profil de connexion, les noms de zones correspondants sur la page de détails Profil de connexion, et indique s'ils s'appliquent aux EDI ou aux transactions :

Tableau 14. Attributs du profil de connexion

Attribut	Nom de la zone	EDI	Transaction EDI
Qualificatif 1 de profil de connexion	Qualificatif 1	X	
Indicateur de syntaxe EDI	Type de syntaxe EDI		X
Identificateur d'émetteur d'application de groupe	ID de l'émetteur de l'application		X
Identificateur de réceptionnaire d'application de groupe	ID du réceptionnaire de l'application		X
Mot de passe d'application de groupe	Mot de passe		X

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 réceptionnaire 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 flot 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 participants source et cible, regroupement, 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 réceptionnaire de groupe** et **Mot de passe d'application de groupe** pour différencier les transactions.

EDI

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 (regroupement Aucun) ou Internet (regroupement 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 participants pour le même EDI source mais avec deux cibles différentes (l'une pour le regroupement Aucun, l'autre pour le regroupement 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 regroupement source (N/A) mais un regroupement cible différent (Aucun ou AS2). La connexion du participant avec le profil CPNone aura sa passerelle cible définie sur la passerelle de script FTP qui peut se connecter au VAN. La connexion du participant avec le profil CPAS2 aura son regroupement cible défini sur AS.
4. Associez le profil de connexion adapté à chacun.

L'Enveloppeur utilise l'attribut **Qualificatif 1 de profil de connexion** do côté "Vers" de la connexion du participant 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

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 participant, 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 «EDI», à la page 113 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 EDI de test, de production ou d'information. Voir «Transactions», à la page 112 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 réceptionnaire de l'application** pour indiquer l'application ou la division de l'entreprise associée au réceptionnaire 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 réceptionnaire.
10. Cliquez sur **Enregistrer**.

Pour les transactions que vous voulez insérer dans certaines enveloppes d'EDI, 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 flot de documents (vous pouvez par exemple modifier les attributs du protocole X12V5R1 dans la fenêtre Gestion des définitions de flots 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'Envelopeur utilise des numéros de contrôle pour assurer la numérotation unique des EDI, groupes et transactions d'une enveloppe. Ces numéros sont établis pour le Gestionnaire de communauté et les participants. Lors de l'échange de documents, des numéros de contrôle sont générés pour la *paire* de participants.

A chaque participant bénéficiant de capacités B2B 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 participants. Les valeurs d'initialisation s'appliquent au participant auquel l'EDI est envoyé. Lorsqu'un document a été envoyé d'un participant à un autre, les derniers numéros utilisés s'affichent sur la page Numéros de contrôle actuels. Pour une paire donnée de participants, 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 15 pour une description des codes disponibles :

Tableau 15. 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 participant.
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.
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.

Tableau 15. Masques des numéros de contrôle (suite)

Code	Numéro de contrôle	Description
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.
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 *o* 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

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. Tapez le nom d'un participant et cliquez sur **Rechercher** ou cliquez sur **Rechercher** sans entrer de nom, pour afficher tous les participants. Si vous laissez **Prêt pour l'EDI** coché, vous limitez la recherche aux participants qui bénéficient de capacités B2B de document EDI. Si vous décochez la case, vous effectuez une recherche sur tous les participants.
3. Cliquez sur l'icône **Afficher les détails** en regard du participant.
4. Les affectations actuelles du numéro de contrôle du participant (le cas échéant) sont indiquées sur la page Détails de configuration du numéro de contrôle. Cliquez sur l'icône **Edition** pour ajouter des valeurs ou en modifier.
5. Entrez (ou modifiez) la valeur en regard de **EDI** pour indiquer le numéro que vous souhaitez utiliser pour initialiser la génération de numéro de contrôle pour les EDI.
6. Entrez (ou modifiez) la valeur en regard de **Groupe** pour indiquer le numéro que vous souhaitez utiliser pour initialiser la génération de numéro de contrôle pour les groupes. Sinon, vous pouvez cliquer sur **Masque** et indiquer le masque à utiliser à la place d'une valeur fixe.
7. Entrez (ou modifiez) la valeur en regard de **Transaction** pour indiquer le numéro que vous souhaitez utiliser pour initialiser la génération de numéro de contrôle pour les transactions. Sinon, vous pouvez cliquer sur **Masque** et indiquer le masque à utiliser à la place d'une valeur fixe.
8. Cliquez sur **Enregistrer**.

Numéros de contrôle en actuels

Pour une paire de participants 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 participants 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 participants, laissez **Tout participant** sélectionné dans la liste des participants et cliquez sur **Afficher le statut en cours**.
   - Pour consulter le statut des participants sélectionnés, procédez comme suit :

a. Entrez le nom des participants source et cible et cliquez sur **Rechercher**. Si vous souhaitez limiter les résultats de la recherche aux participants qui échangent des documents EDI, laissez **Rechercher les participants prêts pour l'EDI** coché.
b. Dans les listes obtenues, sélectionnez un ou plusieurs participants, et cliquez sur **Afficher le statut en cours**.

Procédure générale de définition d'échanges de documents

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 procédures d'activation des capacités B2B des participants (pour tous les types d'échanges de documents) sont décrites dans la section «Configuration des capacités B2B», à la page 156. 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 159. Pour étudier un exemple d'échange de document EDI, depuis l'importation des mappes jusqu'à la gestion des connexions, consultez l'Annexe B, «Exemples d'EDI», à la page 205. Cette annexe propose les exemples suivants :

- «Exemple EDI vers ROD», à la page 205
- «Exemple EDI vers XML», à la page 218
- «Exemple ROD vers EDI», à la page 231
- «Exemple de document XML vers EDI», à la page 224

Importation de mappes

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.

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 flot de documents (regroupement, protocole et flot de documents) sur les pages Mappe de transformation et Gérer des définitions de flots 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 <ID_utilisateur_base_de_données> <mot_de_passe> <mappe_de_chaîne_de_contrôle>`
   - Sous Windows :

     `<ProductDir>\bin\bcgDISImport.bat <ID_utilisateur_base_de_données> <mot_de_passe> <mappe_de_chaîne_de_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 flot 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 flots 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 > Définitions du flot de documents**.
   d. Développez les regroupements et protocoles associés aux définitions de documents affichées dans la page Mappes de transformation, pour vérifier que les flots de documents sont affichés sur la page Gérer les définitions de flot 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 conversion 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.

Configuration d'un flot EDI vers EDI

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 flot 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 regroupement **N/A** sur l'interaction cible.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
   b. Vérifiez s'il existe déjà une définition de flot de documents. Par exemple, si un participant prévoit d'envoyer un EDI en tant que regroupement AS, protocole EDI-X12 et flot de documents ISA, la définition est déjà disponible. De la même façon, une définition de flot 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 (non livrée) en cas d'erreur dans l'une des transactions, cliquez sur l'icône **Edition des valeurs d'attribut** en regard de **Flot de document**. Sur la ligne **Annuler l'enveloppe en cas d'erreur**, sélectionnez **Oui** dans la liste.
   d. Si aucune définition de flot de documents n'existe, créez-en une en sélectionnant Regroupement, Protocole et Flot de documents.
2. Créez une interaction pour l'EDI.
   a. Cliquez sur **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Sélectionnez **Création d'une interaction**.
   c. Sélectionnez les définitions de flots de documents source et cible. A l'exception du regroupement (qui sera **N/A** pour la cible), les définitions de flot 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 de mappes», à la page 118.

   Si l'EDI contient plusieurs transactions, répétez cette étape pour chacune.
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 du flot 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 du flot 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 flot de documents. Par exemple, vous pouvez modifier la **Mappe de validation** associée au flot 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 **Administrateur du concentrateur > Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sous **Source**, sélectionnez le flot de documents associé à la transaction. Développez le regroupement et le protocole, et sélectionnez le flot de documents. En général, ce sera **N/A** (car la transaction elle-même n'est pas créée à l'origine par le participant), 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 flot de documents pour le document transformé. Développez le regroupement et le protocole, et sélectionnez le flot de documents. Comme la transaction sera enveloppée (et donc ne sera pas livrée directement à un participant), le regroupement 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 conversion EDI**.
6. Vérifiez si une définition de flot 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 du flot de documents**.
   b. Vérifiez s'il existe déjà une définition de flot de documents. Le regroupement source sera N/A, le protocole et le flot 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 flot de documents n'existe, créez-en une en sélectionnant Regroupement, Protocole et Flot de documents.
7. Créez une interaction pour l'EDI envoyé par le concentrateur une fois la transaction transformée.
   a. Cliquez sur **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sélectionnez les documents source et cible. A l'exception du regroupement (qui sera **N/A** pour le document source), les définitions de flot de documents seront les mêmes.
   d. Sélectionnez **Passe-système** dans la liste **Action**.

Pour ajouter un accusé de réception au flot, consultez la section «Configuration des accusés de réception», à la page 127.

Après avoir configuré les interactions, créez des capacités B2B pour les participants.

- Pour le participant source, activez trois définitions de flot de documents (sous **Définition de la source**), une pour le flot de documents source, une pour la transaction EDI et une pour l'enveloppe.
- Pour le participant cible, activez trois définitions de flot de documents (sous **Définition de la cible**), une pour le flot de documents désenveloppé, une pour la transaction EDI et une pour l'enveloppe EDI.

Les étapes de création des capacités B2B sont détaillées «Configuration des capacités B2B», à la page 156.

Une fois définies les capacités B2B des participants, créez les connexions. Vous avez besoin de trois connexions :

- Une pour l'enveloppe depuis le participant source vers le concentrateur.
- Une pour la transaction EDI source vers la transaction EDI cible.
- Une pour l'enveloppe depuis le concentrateur vers le participant.

Les étapes de création des connexions sont détaillées Chapitre 12, «Gestion des connexions», à la page 159.

Configuration d'un flot EDI vers XML ou ROD

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 flot EDI vers XML, voir «Exemple EDI vers XML», à la page 218. Pour un exemple complet de flot EDI vers ROD, voir «Exemple EDI vers ROD», à la page 205.

1. Vérifiez qu'une définition de flot 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 regroupement **N/A** sur l'interaction cible.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
   b. Vérifiez s'il existe déjà une définition de flot de documents. Par exemple, si un participant prévoit d'envoyer un EDI en tant que regroupement AS, protocole EDI-X12 et flot de documents ISA, la définition est déjà disponible. De la même façon, une définition de flot de documents N/A/EDI-X12/ISA existe déjà.
   c. Si aucune définition de flot de document n'existe, créez-en une.
2. Créez une interaction pour l'EDI reçu au niveau du concentrateur.
   a. Cliquez sur **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Sélectionnez **Création d'une interaction**.
   c. Sélectionnez les documents source et cible. A l'exception du regroupement (qui sera **N/A** pour la cible), les définitions de flot 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 de mappes», à la page 118.

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 **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sous **Source**, sélectionnez le flot de documents associé à la transaction. Développez le regroupement et le protocole, et sélectionnez le flot de documents. En général, ce sera **N/A** (car la transaction elle-même n'est pas créée à l'origine par le participant), 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 flot de documents pour le document (XML ou ROD) transformé. Développez le regroupement et le protocole, et sélectionnez le flot 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 conversion EDI**.

Pour ajouter un accusé de réception au flot, consultez la section «Configuration des accusés de réception», à la page 127.

Après avoir configuré les interactions, créez des capacités B2B pour les participants.

- Pour le participant source, activez deux définitions de flot de documents (sous **Définition de la source**), une pour la transaction EDI et une pour l'enveloppe.
- Pour le participant cible, activez deux définitions de flot de documents (sous **Définition de la cible**), une pour l'enveloppe EDI et une pour le document XML ou ROD.

Les étapes de création des capacités B2B sont détaillées à la section «Configuration des capacités B2B», à la page 156.

Une fois définies les capacités B2B des participants, créez les connexions. Vous avez besoin de deux connections :

- Une pour l'enveloppe depuis le participant 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 159.

Configuration d'un flot XML ou ROD vers EDI

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 flot XML vers EDI, voir «Exemple de document XML vers EDI», à la page 224. Pour un exemple complet de flot ROD vers EDI, voir «Exemple ROD vers EDI», à la page 231.

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 de mappes», à la page 118.
2. Créez une interaction pour la mappe que vous venez d'importer.

a. Cliquez sur **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
b. Cliquez sur **Création d'une interaction**.
c. Sous **Source**, sélectionnez la définition de flot de documents associée au document XML ou ROD. Développez le regroupement et le protocole, et sélectionnez le flot de documents.
d. Sous **Cible**, sélectionnez le flot de documents associé à la transaction EDI. Développez le regroupement et le protocole, et sélectionnez le flot de documents. Comme la transaction ne sera pas livrée directement (elle sera placée dans une enveloppe avant d'être livrée), vous utiliserez le regroupement **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 **Conversion XML et validation EDI** ou **Conversion ROD et validation EDI**.

3. Vérifiez si une définition de flot 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 du flot de documents**.
   b. Vérifiez s'il existe déjà une définition de flot de documents. Pour le document source (l'EDI envoyé depuis le concentrateur), le regroupement sera **N/A**.
   c. Editez tout attribut qui s'applique à l'EDI en cours de livraison.
   d. Si aucune définition de flot de documents n'existe, créez-en une en sélectionnant Regroupement, Protocole et Flot de documents.
4. Créez une interaction pour l'EDI envoyé par le concentrateur une fois le document transformé.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sélectionnez les documents source et cible. Les documents source et cible ont des regroupements différents (le document source est regroupé N/A), mais le protocole (EDI-X12 par exemple) et le flot de documents (ISA par exemple) doivent être identiques.
   d. Sélectionnez **Passe-système** dans la liste des actions.

Après avoir configuré les interactions, créez des capacités B2B pour les participants.

- Pour le participant source, le nombre de définitions de flot de documents à définir (sous **Définition de la source**) dépend du type de flot de documents.
  - Par exemple, pour un document XML dont le flot de documents est ICGPO et la conversion EDI est MX12V3R1, vous activerez trois définitions de flot 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 flot 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 participant cible, activez deux définitions de flot 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.

Les étapes de création des capacités B2B sont détaillées à la «Configuration des capacités B2B», à la page 156.

Une fois définies les capacités B2B des participants, 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 participant.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 159.

Configuration de plusieurs documents XML ou ROD en un flot de fichier vers EDI

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 de mappes», à la page 118.
2. Créez une interaction pour les documents source et cible.
   a. Cliquez sur **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sélectionnez les documents source et cible, et **Conversion XML et validation EDI** ou **Conversion ROD et validation EDI** dans la liste des actions.
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 flot 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 du flot de documents**.
   b. Vérifiez s'il existe déjà une définition de flot de documents. La source sera N/A, le protocole et le flot de documents correspondant 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 flot de documents n'existe, créez-en une en sélectionnant Regroupement, Protocole et Flot de documents.
5. Créez une interaction pour l'EDI envoyé par le concentrateur une fois la transaction transformée.
   a. Cliquez sur **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.

c. Sélectionnez les documents source et cible. Les documents source et cible ont des regroupements différents (le document source est regroupé N/A), mais le protocole (EDI-X12 par exemple) et le flot de documents (ISA par exemple) doivent être identiques.

d. Sélectionnez **Passe-système** dans la liste des actions.

Après avoir configuré les interactions, créez des capacités B2B pour les participants.

- Pour le participant source, le nombre de définitions de flot de documents à définir (sous **Définition de la source**) dépend du type de flot de documents.
  - Par exemple, pour un document XML dont le flot de documents est ICGPO et la conversion EDI est MX12V3R1, vous activerez trois définitions de flot 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, vou activerez deux définitions de flot de documents (sous **Définition de la source**), une pour le document XML ou ROD document, et une pour l'enveloppe envoyée depuis le concentrateur.

Les étapes de création des capacités B2B sont détaillées à la section «Configuration des capacités B2B», à la page 156.

Une fois définies les capacités B2B des participants, 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 participant.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 159.

Configuration d'un flot de documents XML vers ROD ou ROD vers XML

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 de mappes», à la page 118.
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 **Administrateur du concentrateur > Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
4. Sélectionnez les documents source et cible, et **Conversion XML et validation EDI** ou **Conversion ROD et validation EDI** dans la liste des actions.

Après avoir configuré les interactions, créez des capacités B2B pour les participants.

- Pour le participant source, activez les définitions de flot de documents (sous **Définition de la source**) pour le document XML ou ROD.
- Pour le participant cible, activez les définitions de flot de documents (sous **Définition de la cible**) pour le document XML ou ROD.

Les étapes de création des capacités B2B sont détaillées à la section «Configuration des capacités B2B», à la page 156.

Une fois définies les capacités B2B des participants, créez les connexions. Vous avez besoin d'une connexion, pour le flot XML vers ROD ou pour le flot ROD vers XML. Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 159.

Configuration d'un flot de documents XML vers XML ou ROD vers ROD

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 de mappes», à la page 118.
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 **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sélectionnez les documents source et cible.
   d. Sélectionnez **Conversion XML et validation EDI** ou **Conversion ROD et validation EDI** dans la liste Action.

Après avoir configuré les interactions, créez des capacités B2B pour les participants.

- Pour le participant source, activez une définition de flot de documents (sous **Définition de la source**) pour le document XML ou ROD.
- Pour le participant cible, activez une définition de flot de documents (sous **Définition de la cible**) pour le document XML ou ROD.

Les étapes de création des capacités B2B sont détaillées à la section «Configuration des capacités B2B», à la page 156.

Une fois définies les capacités B2B des participants, créez les connexions. Vous avez besoin d'une connexion, pour le flot XML vers XML ou pour le flot ROD vers ROD. Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 159.

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 participant. 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 **Regroupement : Aucun** dans la page Définitions de flot 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 participants, 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 flots de documents sous **Regroupement : N/A** :

Tableau 16. Mappes d'accusé de réception fonctionnel fournies par le système

Protocole	Flot de documents	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 flot de documents TA1 associé) figure sous **Regroupement : N/A**. Cette mappe est utilisée pour générer un TA1. TA1 est un accusé de réception fonctionnel généré pour les EDI X12 entrants.

Le protocole &WDIEVAL (avec un X12ENV associé) est également fourni sous **Regroupement : 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 flot de documents

Pour ajouter un accusé de réception à un flot, procédez comme suit :

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 de mappes», à la page 118.
2. Associez la mappe FA à une définition de flot 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 regroupement pour le développer jusqu'au niveau voulu (par exemple pour développer les dossiers **Regroupement** et **Protocole**, puis sélectionner une transaction).
   d. Cliquez sur **Enregistrer**.
3. Créez une interaction pour la mappe que vous venez d'importer.
   a. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sous **Source**, sélectionnez le flot de documents associé à l'accusé de réception fonctionnel. Développez le regroupement et le protocole, et sélectionnez le flot de documents.
   d. Sous **Cible**, sélectionnez les mêmes valeurs.
   e. Dans la liste des actions, sélectionnez **Passe-système**.
4. Vérifiez si une définition de flot 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 du flot de documents**.
   b. Vérifiez s'il existe déjà une définition de flot de documents. La source sera N/A, le protocole et le flot de documents correspondant 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 flot de documents n'existe, créez-en une en sélectionnant Regroupement, Protocole et Flot de documents.

5. Créez une interaction pour l'EDI envoyé par le concentrateur une fois le document transformé.
   a. Cliquez sur **Administrateur du concentrateur> Configuration du concentrateur > Définitions du flot de documents > Gestion des interactions**.
   b. Cliquez sur **Création d'une interaction**.
   c. Sélectionnez les documents source et cible.
   d. Sélectionnez **Passe-système** dans la liste **Action**.

Après avoir configuré les interactions, créez des capacités B2B pour les participants. Notez que le participant cible dans une transmission d'accusé de réception fonctionnel est le participant source du document EDI initial.

- Pour le participant source, activez les définitions de flot de documents (sous **Définition de la source**) pour l'accusé de réception fonctionnel. Activez également une définition de flot de documents pour l'enveloppe qui est envoyée par le concentrateur.
- Pour le participant cible, activez une définition de flot de documents (sous **Définition de la cible**) pour l'accusé de réception fonctionnel. Activez également une définition de flot 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.

Les étapes de création des capacités B2B sont détaillées à la section «Configuration des capacités B2B», à la page 156.

Une fois définies les capacités B2B des participants, 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 participant.

Les étapes de création des connexions sont détaillées au Chapitre 12, «Gestion des connexions», à la page 159.

Affichage d'échanges et de transactions EDI

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 flot 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.

Pour ouvrir l'Afficheur de documents, cliquez sur **Afficheurs > Afficheur de documents**. Pour obtenir davantage d'informations sur l'Afficheur de documents, consulter le *Guide de l'administrateur*.

Chapitre 9. Création du profil du Gestionnaire de communauté et des capacités B2B

Maintenant que vous avez configuré le concentrateur, notamment les cibles, et configuré les définitions de flot de documents et les interactions, vous pouvez créer le Gestionnaire de la communauté du concentrateur. Vous pouvez ensuite établir ses capacités B2B. Une fois que vous avez créé des participants (de la façon décrite au Chapitre 11, «Création de participants et de leurs capacités B2B», à la page 155), vous pouvez activer les connexions réelles entre le Gestionnaire de communauté et les participants, de façon à ce que des documents puissent être échangés.

Ce chapitre contient les rubriques suivantes :

Création du profil du Gestionnaire de communauté

Le Gestionnaire de communauté est généralement la société propriétaire du serveur WebSphere Partner Gateway, et qui l'utilise pour communiquer avec les participants. Le Gestionnaire de communauté est considéré comme un participant du concentrateur, et possède un profil, des passerelles et des capacités B2B.

Pour créer le profil du Gestionnaire de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Créer**.
3. Pour **Nom de connexion de l'entreprise**, saisissez le nom que le Gestionnaire de communauté indiquera dans la zone Entreprise, lors de la connexion au concentrateur. Par exemple, vous pouvez entrer Gestionnaire.
4. Pour **Nom affiché du participant**, entrez le nom de la société ou tout autre nom descriptif pour le Gestionnaire de communauté. Il s'agit du nom affiché dans la liste **Recherche du participant**.
5. Dans la liste Type de participant, sélectionnez **Gestionnaire de communauté**.

   Remarque : WebSphere Partner Gateway n'accepte qu'un seul Gestionnaire de communauté et un seul Opérateur de communauté. L'Opérateur de communauté est créé automatiquement lorsque vous installez WebSphere Partner Gateway.
6. Sélectionnez le statut du Gestionnaire de communauté. Il est probable que vous utiliserez la valeur par défaut, à savoir **Activé**.
7. Indiquez éventuellement le type de la société dans la zone **Fournisseur**.
8. Vous pouvez également préciser le site Web du Gestionnaire de communauté.
9. Sous **ID Métier**, cliquez sur **Nouveau**.
10. 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 Gestionnaire de communauté.

    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 métier au Gestionnaire de communauté. Dans certains cas, plusieurs ID métier 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 Gestionnaire de communauté et les participants impliqués dans ce type de flot 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.

11. Vous pouvez éventuellement entrer une adresse IP pour le Gestionnaire de communauté, en procédant comme suit :
    a. Sous **Adresse IP**, cliquez sur **Nouveau**.
    b. Spécifiez le type de passerelle.
    c. Entrez l'adresse IP du Gestionnaire de communauté.
12. Cliquez sur **Sauvegarder**.
13. Vous obtiendrez un mot de passe qui sera utilisé par le Gestionnaire de communauté pour se connecter au concentrateur. Notez-le. Vous l'indiquerez à l'utilisateur d'administration du Gestionnaire de communauté.

    Remarque : Lorsque vous créez le profil Gestionnaire de communauté, vous créez en fait l'utilisateur d'administration du Gestionnaire de communauté. Les utilisateurs d'administration peuvent créer des utilisateurs individuels au sein de leur organisations ou, en tant qu'Administrateur du concentrateur, vous pouvez créer les utilisateurs pour les participants.

Lorsque vous avez créé le profil d'un Gestionnaire de communauté, établissez les passerelles qui seront utilisées par le concentrateur pour envoyer des documents au Gestionnaire de communauté. Consultez les sections suivantes pour paramétrer des passerelles pour le Gestionnaire de communauté :

- «Configuration d'une passerelle HTTP», à la page 138
- «Configuration d'une passerelle HTTPS», à la page 139
- «Configuration d'une passerelle JMS», à la page 143
- «Configuration d'une passerelle fichier-répertoire», à la page 145

Une fois que vous avez paramétré les passerelles du Gestionnaire de communauté, configurez ses capacités B2B.

Configuration des capacités B2B

Le Gestionnaire de communauté dispose de capacités B2B qui définissent les types de documents que le Gestionnaire de communauté peut recevoir et envoyer.

La fonction Capacités B2B vous permet d'associer les capacités B2B d'un Gestionnaire de communauté à une définition du flot de documents.

Pour définir les capacités B2B du gestionnaire de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère de recherche pour afficher la liste de tous les participants.
3. Cliquez sur l'icône **Afficher les détails** en regard du Gestionnaire de communauté.
4. Cliquez sur **Capacités B2B**. La page des capacités B2B s'affiche. Dans la partie de droite apparaissent les regroupements, les protocoles et les flots de documents pris en charge par le système en tant que définitions du flot de documents.
5. Cliquez sur l'icône **Rôle inactif** dans la colonne **Définition de la source** pour les regroupements de droite qui contiennent les documents que le Gestionnaire de communauté enverra aux participants.
6. Sélectionnez **Définition de la cible** si vous envisagez de recevoir les mêmes documents des participants. La Console de communauté indique par une coche que la définition du flot de documents est activée.

   Remarque : La sélection de la Définition de la source sera la même pour toutes les actions d'un processus PIP à double sens même si la requête provient d'un participant et la confirmation associée d'un autre. Cela vaut également pour la colonne Définition de la cible.
7. Cliquez sur l'icône **Développer** au niveau **Regroupement** pour développer un noeud jusqu'au niveau Définition du flot de documents approprié, ou sélectionnez un nombre de **0 à 4**, ou cliquez sur **Tous** pour développer tous les noeuds Définition de flot de documents jusqu'au niveau sélectionné.
8. Sélectionnez à nouveau **Définition de la source**, **Protocole** ou les deux rôles à la fois pour les niveaux inférieurs **Protocole** et **Flot de documents**, pour chaque définition de flot de documents prise en charge par votre système.

   Si une définition est activée au niveau **Flot de documents**, les définitions **Action** et **Activité** (s'il en existe) seront activées automatiquement.
9. Cliquez éventuellement sur **Activé** sous la colonne **Activé** pour mettre une définition du flot 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 regroupement est désactivé, toutes les définitions de flot de documents de niveau inférieur de ce même noeud sont également désactivées, même si leur état respectif était Activé. Si une définition du flot de documents de niveau inférieur est désactivée, toutes les définitions de niveau supérieur appartenant au même contexte restent activées. Lorsqu'une définition de flot de documents est désactivée, les connexions et attributs existants continuent de fonctionner. La définition de flot de documents désactivée ne fait que limiter la création de nouvelles connexions.

10. Cliquez sur l'icône **Edition** si vous souhaitez modifier l'un des attributs d'un protocole, d'un regroupement, d'un flot 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**.

    Comme indiqué à l'étape 10, à la page 131, le Gestionnaire de communauté peut (et dans certains cas doit) avoir plusieurs ID métier. Si le participant ne doit recevoir qu'une seule forme d'ID, vous devez sélectionner la valeur appropriée. Pour sélectionner l'ID :

    a. Cliquez sur l'icône **Edition** en regard de **Aucun**.

       L'attribut (**ID métier AS**) associé au regroupement Aucun s'affiche.

    b. Dans la liste **Mettre à jour**, sélectionnez l'ID métier AS2 dans le format accepté par le participant.

    c. Cliquez sur **Sauvegarder**.

    Remarque : Si vous définissez l'attribut dans l'écran Capacités B2B, il s'applique à tous les échanges émis par le Gestionnaire de communauté avec le regroupement Aucun. Pour personnaliser la sélection en fonction d'une connexion particulière, vous pouvez définir la valeur (ou supplanter la valeur définie ici) au niveau de la Connexion. Voir «Activation des connexions de participants», à la page 159.

Chapitre 10. Création de passerelles

Une fois que vous avez créé les participants, définissez leurs passerelles. Les passerelles définissent des points d'entrée dans le système du participant.

Ce chapitre contient les rubriques suivantes :

Vue d'ensemble

WebSphere Partner Gateway fait appel à des passerelles pour acheminer les documents jusqu'à leur destination. Le destinataire peut être un participant de la communauté ou le Gestionnaire de communauté.

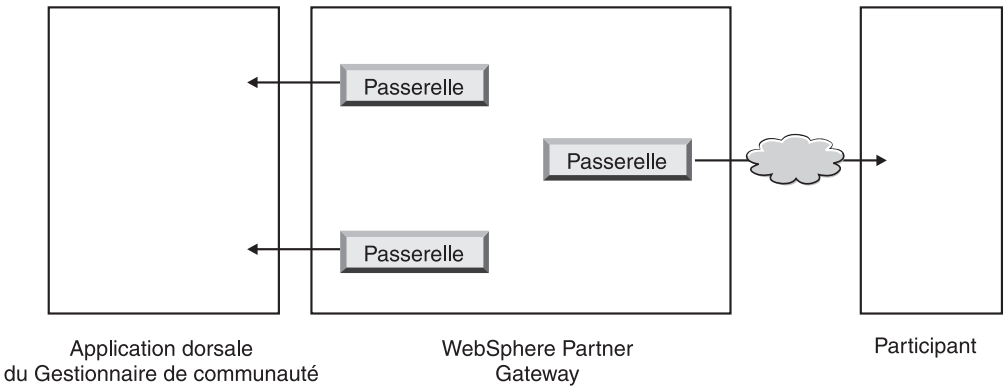

Figure 34. Passerelles vers le Gestionnaire de communauté et les participants

Les informations utilisées lors de la configuration d'une passerelle dépendent du protocole de transfert des documents sortants.

Les transferts suivants sont pris en charge (par défaut) pour les passerelles des participants :

- HTTP/1.1

- HTTPS/1.0
- HTTPS/1.1
- FTP
- FTPS
- JMS
- SMTP

  Remarque : Vous ne pouvez définir de passerelle SMTP que pour les participants (pas pour le Gestionnaire de communauté).
- fichier-répertoire
- script FTP

Vous pouvez également indiquer un type de transfert défini par l'utilisateur, que vous téléchargez lors de la création de la passerelle.

En tant qu'administrateur du concentrateur, vous pouvez définir les passerelles de vos participants. Vous pouvez également leur laisser le soin d'effectuer cette opération. Dans ce chapitre, vous apprendrez comment exécuter cette tâche pour les participants.

Définition des valeurs de transfert globales

Définissez les attributs de transfert globaux qui s'appliquent à toutes les passerelles de script FTP. Si vous ne définissez pas de passerelles de script FTP, cette section ne vous concerne pas.

Le mode de transfert par scrip FTP utilise un système de verrou qui empêche que plusieurs instances de script FTP n'accèdent à la même passerelle 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 > Participant de communauté**.
2. Cliquez sur **Passerelles**.
3. Sélectionnez **Attributs de transfert globaux** dans la liste des passerelles.

   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 transfert 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 **Transfert 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 passerelle 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 passerelle 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

Pour les transferts HTTP et HTTPS, vous pouvez définir un proxy direct afin que les documents soient envoyés via un serveur proxy configuré. Avec WebSphere Partner Gateway, vous pouvez définir les types suivants :

- Prise en charge de proxy sur HTTP
- Prise en charge de proxy sur HTTPS
- Prise en charge de proxy sur HTTPS avec authentification
- Prise en charge de proxy sur SOCKS

Une fois que vous avez défini un proxy direct, vous pouvez le rendre utilisable pour l'ensemble du transfert (par exemple, toutes les passerelles HTTP utiliseront le proxy direct), en le définissant comme passerelle par défaut.

Pour définir un proxy direct, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Passerelles**.
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 transfert dans la liste.

   Remarque : Les transferts 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 participant bénéficiant d'une prise en charge proxy).
10. Cliquez sur **Enregistrer**.

Configuration d'une passerelle HTTP

Configurez une passerelle HTTP pour que des documents puissent être envoyés depuis le concentrateur à l'adresse IP des participants. Lorsque vous configurez une passerelle HTTP, vous pouvez également demander que les documents soient envoyés via un serveur proxy configuré.

Pour commencer à créer une passerelle HTTP, procédez comme suit.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère de recherche pour afficher la liste de tous les participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Depuis la page **Liste des passerelles** procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée. Il s'agit du nom qui apparaîtra dans la liste des passerelles.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **HTTP/1.1** dans la liste **Transferts**.
2. 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 participant sélectionné utilise un serveur proxy différent, choisissez-en un autre dans la liste. Si vous ne voulez pas utiliser cette fonctionnalité avec ce participant, sélectionnez **Ne pas utiliser de proxy direct**.
3. Dans la zone **Adresse**, entrez l'URI de la destination du document. Cette zone doit être renseignée.

   Le format est : http://*<nom_serveur>*:*<port_facultatif>*/*<chemin>*

   Exemple :

   ```
   http://anotherserver.ibm.com:57080/bcgreceiver/Receiver
   ```

   Lorsque vous configurez une passerelle 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.
4. Entrez éventuellement un nom d'utilisateur et un mot de passe s'il en faut un pour accéder au serveur HTTP.

5. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle 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 passerelle doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
7. Dans la zone **Nombre d'unités d'exécution**, indiquez le nombre de documents qui peuvent être traités simultanément. La valeur par défaut est 3.
8. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous voulez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.
9. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous voulez que la passerelle soit mise hors ligne (automatiquement) lorsque le nombre de relances a été épuisé. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.

   Si vous sélectionnez **Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la passerelle n'a pas été mise en ligne manuellement.
10. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion pourra rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
11. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs», à la page 151.Sinon, cliquez sur **Sauvegarder**.

Configuration d'une passerelle HTTPS

La configuration d'une passerelle HTTPS permet d'envoyer des documents depuis le concentrateur aux adresses IP des participants. Lorsque vous configurez une passerelle HTTPS, vous pouvez également indiquer que les documents soient envoyés via un serveur proxy configuré.

Pour créer des passerelles HTTPS, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
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 participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Dans la page Liste des passerelles, procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **HTTPS/1.0** ou **HTTPS/1.1**, dans la liste des **transferts**.
2. 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 participant sélectionné utilise un serveur proxy différent, choisissez-en un autre dans la liste. Si vous ne voulez pas utiliser cette fonctionnalité avec ce participant, sélectionnez **Ne pas utiliser de proxy direct**.
3. Dans la zone **Adresse**, entrez l'URI de la destination du document. Cette zone doit être renseignée.

   Le format est : https://*<nom_serveur>*:*<port_facultatif>*/*<chemin>*

   Exemple :

   ```
   https://anotherserver.ibm.com:57443/bcgreceiver/Receiver
   ```
4. Entrez éventuellement un nom d'utilisateur et un mot de passe s'ils sont obligatoires pour accéder au serveur HTTP sécurisé.
5. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle 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 passerelle doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
7. Dans la zone **Nombre d'unités d'exécution**, indiquez le nombre de documents qui peuvent être traités simultanément. La valeur par défaut est 3.
8. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous voulez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.
9. 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 métier associé au document. Par défaut, **Non** est sélectionné.
10. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous voulez que la passerelle soit mise hors ligne (automatiquement) lorsque le nombre de relances a été épuisé. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.

    Si vous sélectionnez **Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la passerelle n'a pas été mise en ligne manuellement.
11. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion pourra rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
12. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs», à la page 151.Sinon, cliquez sur **Sauvegarder**.

Configuration d'une passerelle FTP

Pour créer une passerelle FTP, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.

2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère de recherche pour afficher la liste de tous les participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Dans la page Détails sur la passerelle, procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **FTP** dans la liste des **transferts**.
2. Dans la zone **Adresse**, entrez l'URI de la destination du document. Cette zone doit être renseignée.

   Le format est : ftp://<*nomserveur_ftp*>:<*numéroport*>

   Exemple :

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Si vous ne définissez pas de numéro de port, le port FTP standard est utilisé.
3. Entrez éventuellement un nom d'utilisateur et un mot de passe s'il en faut pour accéder au serveur FTP.
4. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle 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 passerelle 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**, indiquez le nombre de documents qui peuvent être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous voulez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous voulez que la passerelle soit mise hors ligne (automatiquement) lorsque le nombre de relances a été épuisé. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.

   Si vous sélectionnez **Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la passerelle n'a pas été mise en ligne manuellement.
9. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion pourra rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.

10. Dans la zone **Utiliser un nom de fichier unique**, laissez la case cochée si vous voulez que le document conserve son nom d'origine lorsqu'il est envoyé. Dans le cas contraire, décochez-la, ce qui indiquera à WebSphere Partner Gateway d'attribuer un nom au fichier.
11. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs», à la page 151.Sinon, cliquez sur **Sauvegarder**.

Configuration d'une passerelle SMTP

Pour créer une passerelle SMTP, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
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 participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Dans la page Liste des passerelles, procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **SMTP** dans la liste des **transferts**.
2. Dans la zone **Adresse**, entrez l'URI de la destination du document. Cette zone doit être renseignée.

   Le format est : mailto:<*utilisateur@nomserveur*>

   Exemple :

   ```
   mailto:admin@anotherserver.ibm.com
   ```
3. Entrez éventuellement un nom d'utilisateur et un mot de passe s'ils sont obligatoires pour accéder au serveur HTTP.
4. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle 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 passerelle 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**, indiquez le nombre de documents qui peuvent être traités simultanément. La valeur par défaut est 3.

7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous voulez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous voulez que la passerelle soit mise hors ligne (automatiquement) lorsque le nombre de relances a été épuisé. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.

   Si vous sélectionnez **Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la passerelle n'a pas été mise en ligne manuellement.
9. Dans la zone **Authentification obligatoire**, indiquez si un nom d'utilisateur et un mot de passe doivent être fournis pour le document. Par défaut, **Non** est sélectionné.
10. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs», à la page 151.Sinon, cliquez sur **Sauvegarder**.

Configuration d'une passerelle JMS

Pour créer des passerelles JMS, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère de recherche pour afficher la liste de tous les participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Dans la page Liste des passerelles, procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **JMS** dans la liste des **transferts**.
2. Dans la zone **Adresse**, entrez l'URI de la destination du document. Cette zone doit être renseignée.

   Pour WebSphere MQ JMS, le format de l'identificateur URI de la cible est le suivant :

   `file:///<chemin_liaisons_JNDI_MQ_défini_utilisateur>`

   Exemple :

   `file:///opt/JNDI-Directory`

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 passerelle interne JMS (la passerelle de votre système dorsal), ceci doit correspondre à la valeur que vous avez 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 24). 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 passerelles, le participant fournira sans doute le fichier ".bindings".

Cette zone doit être renseignée.

3. Entrez éventuellement un nom d'utilisateur et un mot de passe s'ils sont obligatoires pour accéder à la file d'attente JMS.
4. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle 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 passerelle 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**, indiquez le nombre de documents qui peuvent être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous voulez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous voulez que la passerelle soit mise hors ligne (automatiquement) lorsque le nombre de relances a été épuisé. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.

   Si vous sélectionnez **Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la passerelle n'a pas été mise en ligne manuellement.
9. Dans la zone **Authentification obligatoire**, indiquez si un nom d'utilisateur et un mot de passe doivent être fournis pour le document. Par défaut, **Non** est sélectionné.
10. Dans la zone **Nom de la fabrique JMS**, indiquez le nom de la classe Java qu'utilise le fournisseur JMS pour se connecter à la file d'attente JMS. Cette zone doit être renseignée.

    Pour des passerelles 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 25).

    Si vous avez entré le sous-dossier pour le contexte JMS à l'étape 2, à la page 143, 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`).
11. 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 doit être renseignée.
12. Dans la zone **Type de message JMS**, indiquez le type de message. Cette zone est facultative.

13. Dans la zone **Modules d'URL du fournisseur**, entrez le nom des classes (ou du fichier JAR) utilisées 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.
14. Dans la zone **Nom de file d'attente JMS**, entrez le nom de la file d'attente JMS vers laquelle les documents doivent être envoyés. Cette zone doit être renseignée.

    Pour des passerelles 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 25).

    Si vous avez entré le sous-dossier pour le contexte JMS à l'étape 2, à la page 143, 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`).
15. Dans la zone **Nom de la fabrique du JNDI du JMS**, indiquez le nom de la fabrique utilisée pour se connecter au service désigné. Cette zone doit être renseignée. Vous utiliserez probablement la valeur com.sun.jndi.fscontext.RefFSContextFactory, si vous définissez votre configuration JMS comme indiqué à la section «Configuration du concentrateur pour le protocole de transfert JMS», à la page 23.
16. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs», à la page 151.Sinon, cliquez sur **Sauvegarder**.

Configuration d'une passerelle fichier-répertoire

Pour créer des passerelles fichier-répertoire, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère de recherche pour afficher la liste de tous les participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Dans la page Liste des passerelles, procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **Fichier-répertoire** dans la liste des **transferts**.

2. Dans la zone **Adresse**, entrez l'URI de la destination du document. Cette zone doit être renseignée.

   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>*

   Exemple :

   ```
   file:///localfiledir
   ```

   où *localfiledir* est un répertoire du répertoire racine.

   Pour les systèmes Windows dans lesquels le répertoire de fichiers et WebSphere Partner Gateway sont sur des unités distinctes, le format est : file:///*<lettre_unité>*:/*<chemin>*
3. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle 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 passerelle 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 qui doivent être traités simultanément. La valeur par défaut est 3.
6. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous voulez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.
7. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous voulez que la passerelle soit mise hors ligne (automatiquement) lorsque le nombre de relances a été épuisé. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.

   Si vous sélectionnez **Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la passerelle n'a pas été mise en ligne manuellement.
8. Dans la zone **Utiliser un nom de fichier unique**, laissez la case cochée si vous voulez que le document conserve son nom d'origine lorsqu'il est envoyé. Dans le cas contraire, décochez-la, ce qui indiquera à WebSphere Partner Gateway d'attribuer in nom au fichier.
9. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs», à la page 151.Sinon, cliquez sur **Sauvegarder**.

Configuration d'une passerelle FTPS

Pour créer des passerelles FTPS, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
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 participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Dans la page Liste des passerelles, procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **FTPS** dans la liste des **transferts**.
2. Dans la zone **Adresse**, entrez l'URI de la destination du document. Cette zone doit être renseignée.

   Le format est : ftp://<*nomserveur_ftp*>:<*numéroport*>

   Exemple :

   ```
   ftp://ftpserver1.ibm.com:2115
   ```

   Si vous ne définissez pas de numéro de port, le port FTP standard est utilisé.
3. Entrez éventuellement un nom d'utilisateur et un mot de passe s'ils sont obligatoires pour accéder au serveur HTTP sécurisé.
4. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle 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 passerelle 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**, indiquez le nombre de documents qui doivent être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous voulez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous voulez que la passerelle soit mise hors ligne (automatiquement) lorsque le nombre de relances a été épuisé. Dans le cas contraire, sélectionnez **Non**. Par défaut, **Non** est sélectionné.

   Si vous sélectionnez **Mise en file d'attente automatique**, tous les documents restent en file d'attente tant que la passerelle n'a pas été mise en ligne manuellement.
9. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion pourra rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
10. Dans la zone **Utiliser un nom de fichier unique**, laissez la case cochée si vous voulez que le document conserve son nom d'origine lorsqu'il est envoyé. Dans le cas contraire, décochez-la, ce qui indiquera à WebSphere Partner Gateway d'attribuer in nom au fichier.
11. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs», à la page 151.Sinon, cliquez sur **Sauvegarder**.

Configuration d'une passerelle de script FTP

Une passerelle de script FTP s'exécute d'après la planification que vous avez définie. Le comportement d'une passerelle de script FTP est régi par un script de commande FTP.

Création du script FTP

Pour utiliser une passerelle 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 passerelles 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 envoyer tous les fichiers vers le répertoire sur le serveur.

   ```
   open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD% %BCGOPTIONx%
   cd %BCGOPTIONx%
   mput *
   quit
   ```

   Lorsque la passerelle 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 passerelle de script FTP, comme indiqué dans la table suivante :

Tableau 17. Mappage des paramètres de script et des informations des zones de passerelle de script FTP

Paramètre de script	**Informations des zones de la passerelle 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

  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 crée un répertoire sur le serveur FTP.

- mput

Cette commande utilise un seul argument, qui décrit un ou plusieurs fichiers à transférer sur le système éloigné. Cet argument peut contenir les caractères génériques standard ('*' et '?') pour identifier plusieurs fichiers.

- 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 passerelle FTP doit être :

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

- quit, bye

  Cette commande arrêtre 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 supprime 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.

Passerelles de script FTP

Si vous pensez utiliser des passerelles de script FTP, procédez comme suit :

Pour créer des passerelles de script FTP, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
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 participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Créer**.

Détails sur la passerelle

Dans la page Liste des passerelles, procédez comme suit :

1. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
2. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
4. Entrez éventuellement une description de la passerelle.

Configuration de la passerelle

Dans la section **Configuration de la passerelle**, procédez comme suit :

1. Sélectionnez **Script FTP** dans la liste des **transferts**.

2. Entrez l'adresse IP du serveur FTP auquel vous voulez envoyer des documents. La valeur indiquée ici remplacera %BCGSERVERIP% lorsque le script FTP sera exécuté.
3. 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.
4. Si la cible est en mode sécurisé, utilisez la valeur par défaut **Oui** pour **Mode FTPS**. Sinon, cliquez sur **Non**.
5. Envoyez le script en procédant comme suit :
   a. Cliquez sur **Télécharger le fichier de script**.
   b. Entrez le nom du fichier contenant le script de traitement des documents, ou utilisez **Parcourir** pour accéder au fichier.
   c. Cliquez sur **Charger le fichier** pour charger le fichier de script dans la zone de texte **Fichier de script actuellement chargé**.
   d. Si ce fichier de script est bien celui que vous voulez utiliser, cliquez sur **Enregistrer**.
   e. Cliquez sur **Fermer la fenêtre**.
6. Dans la zone **Nombre de relances**, indiquez le nombre de fois que la passerelle doit tenter d'envoyer un document avant d'abandonner. La valeur par défaut est 3.
7. Dans la zone **Intervalle de relance**, indiquez le délai d'attente que la passerelle doit observer avant de tenter de renvoyer le document. La valeur par défaut est 300 secondes.
8. Dans **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion pourra rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
9. Dans la zone **Verrouiller l'utilisateur**, indiquez si la passerelle demandera un verrouillage pour qu'aucune autre instance d'une passerelle 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 transfert globaux, de la façon indiquée à la section «Définition des valeurs de transfert globales», à la page 136.

Attributs définis par l'utilisateur

Si vous souhaitez préciser des attributs supplémentaires, procédez comme suit. 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%
          mput *
          quit
```

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

Planification

Dans la section Planification de la page, procédez comme suit :

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 gateway ne soit interrogé (ou acceptez la valeur par défaut).
   - Si vous avez sélectionné **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 passerelle 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 une date 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. **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.
2. Pour configurer l'étape Preprocess ou Postprocess de la passerelle, voir «Configuration de récupérateurs».Sinon, cliquez sur **Sauvegarder**.

Configuration de récupérateurs

Comme indiqué au Chapitre 1, «Introduction», vous pouvez modifier deux points de configuration pour une passerelle, Preprocess et Postprocess.

Aucun récupérateur n'étant fourni par défaut pour le Preprocess ou le Postprocess, aucun récupérateur n'est indiqué par défaut dans la **Liste des récupérateurs disponibles**. Si vous avez téléchargé un récupérateur, vous pouvez le sélectionner et le déplacer dans la **liste des récupérateurs configurés**.

Pour appliquer un récupérateur écrit par l'utilisateur à ces points de configuration, vous devez d'abord télécharger le récupérateur, comme décrit dans la section «Téléchargement de récupérateurs définis par l'utilisateur», à la page 38. (Sélectionnez **Passerelle** au lieu de **Cible** pour l'étape 2, à la page 38). Ensuite, procédez comme suit :

1. Sélectionnez **preprocess** ou **postprocess** dans la liste des **récupérateurs de point de configuration**.
2. Sélectionnez le récupérateur dans la **Liste des récupérateurs disponibles** et cliquez sur **Ajouter**.
3. Si vous voulez modifier les attributs du récupérateur, sélectionnez-le dans la **liste des récupérateurs configurés** puis cliquez sur **Configurer**. La liste d'attributs modifiables s'affiche. Apportez les modifications nécessaires et cliquez sur **Définir valeurs**.
4. Cliquez sur **Enregistrer**.

Vous pouvez modifier davantage la **liste des récupérateurs configurés** de la façon suivante :

- Supprimez un récupérateur en le sélectionnant dans la liste des **récupérateurs configurés** et en cliquant sur **Supprimer**. Le récupérateur passe dans la liste des **récupérateurs disponibles**.
- Pour modifier l'ordre du récupérateur dans la liste, sélectionnez-le dans la liste et cliquez sur le bouton de **déplacement vers le haut** ou **déplacement vers le bas**.

Configuration d'une passerelle pour un transfert défini par l'utilisateur

Si vous entendez télécharger un transfert défini par l'utilisateur, effectuez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Passerelles**.
3. Cliquez sur **Gérer les types de transfert**.
4. Entrez le nom d'un fichier XML définissant le mode de transfert (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 transfert 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 transferts, vous pouvez également supprimer un type de transfert défini par l'utilisateur. Vous ne pouvez pas supprimer un transfert fourni par WebSphere Partner Gateway. Vous ne pouvez pas non plus supprimer un transfert défini par l'utilisateur une fois qu'il a été utilisé pour la création d'une passerelle.
8. Cliquez sur **Créer**
9. Entrez un nom pour identifier la passerelle. Cette zone doit être renseignée.
10. Indiquez éventuellement l'état de la passerelle. L'état par défaut est **Activé**. Une passerelle activée est prête à envoyer des documents. Une passerelle désactivée ne peut pas envoyer de documents.
11. Indiquez éventuellement si la passerelle est en ligne ou hors ligne. Par défaut, elle est en ligne (**Connecté**).
12. Entrez éventuellement une description de la passerelle.
13. Complétez les zones (qui seront uniques à chaque transfert défini par l'utilisateur) et cliquez sur **Enregistrer**.

Spécification d'une passerelle par défaut

Une fois que vous avez créé des passerelles pour le Gestionnaire de communauté ou le participant, indiquez-en une comme passerelle par défaut.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère de recherche pour afficher la liste de tous les participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Passerelles**.
5. Cliquez sur **Afficher les passerelles par défaut**.

La liste des passerelles définies pour le participant s'affiche.

6. Dans la liste **Production**, sélectionnez la passerelle par défaut pour ce participant. Vous pouvez également définir des passerelles par défaut pour d'autres types de passerelles, tels que **Test**.
7. Cliquez sur **Sauvegarder**.

Chapitre 11. Création de participants et de leurs capacités B2B

Créez un profil de participant pour chacun de ceux avec lesquels vous échangerez des documents. Définissez ensuite leurs capacités B2B (les participants peuvent se charger eux-mêmes de cette étape).

Ce chapitre contient les rubriques suivantes :

Création des profils des participants

Pour créer un participant, vous devez être en mesure de fournir des informations le concernant, à savoir :

- l'adresse IP du participant ;
- l' ID Métier utilisé par le participant. 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 choisi par le participant pour identifier la société.

Pour chaque participant que vous souhaitez ajouter à la communauté du concentrateur, effectuez la procédure suivante :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Créer**.
3. Pour **Nom de connexion de l'entreprise**, saisissez le nom que le participant indiquera dans la zone Société lors de la connexion au concentrateur.
4. Pour **Nom affiché du participant**, entrez le nom de la société ou tout autre nom descriptif pour le participant. Il s'agit du nom affiché dans la liste **Recherche du participant**.
5. Sélectionnez le type du participant. WebSphere Partner Gateway n'accepte qu'un seul Gestionnaire de communauté et qu'un seul Opérateur de communauté, aussi le choix est limité à **Participant de communauté**.
6. Sélectionnez l'état du participant. Lors de la création d'un participant, il est probable que vous voudrez utiliser la valeur par défaut, **Activé**.
7. Indiquez éventuellement le type de la société dans la zone **Fournisseur**.
8. Entrez éventuellement le site Web du participant.
9. Sous **ID Métier**, cliquez sur **Nouveau**.
10. 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 participant.

    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 métier à un participant. Dans certains cas, plusieurs ID métier 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 Gestionnaire de communauté et les participants impliqués dans ce type de flot 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.

11. Vous pouvez éventuellement entrer une adresse IP pour le participant en procédant comme suit :
    a. Sous **Adresse IP**, cliquez sur **Nouveau**.
    b. Spécifiez le type de passerelle.
    c. Entrez l'adresse IP du participant.
12. Cliquez sur **Sauvegarder**.
13. Vous obtiendrez un mot de passe qui sera utilisé par le participant pour se connecter au concentrateur. Notez-le. Vous l'indiquerez à l'utilisateur d'administration du participant.

Lorsque vous créez un participant, vous créez en réalité son utilisateur d'administration. Les utilisateurs d'administration peuvent créer des utilisateurs individuels au sein de leur organisations ou, en tant qu'Administrateur du concentrateur, vous pouvez créer les utilisateurs pour les participants.

Lorsque vous avez créé un profil pour un participant, établissez les passerelles qui seront utilisées par le concentrateur pour envoyer des documents au participant. Consultez les sections suivantes pour paramétrer des passerelles pour les participants :

- «Définition des valeurs de transfert globales», à la page 136

  Remarque : Ces valeurs concernent uniquement la passerelle de script FTP.
- «Configuration d'une passerelle HTTP», à la page 138
- «Configuration d'une passerelle HTTPS», à la page 139
- «Configuration d'une passerelle FTP», à la page 140
- «Configuration d'une passerelle SMTP», à la page 142
- «Configuration d'une passerelle JMS», à la page 143
- «Configuration d'une passerelle fichier-répertoire», à la page 145
- «Configuration d'une passerelle FTPS», à la page 146
- «Configuration d'une passerelle de script FTP», à la page 148

Configuration des capacités B2B

Chaque participant a des capacités B2B qui définissent les types de documents qu'il peut envoyer et recevoir.

En tant qu'administrateur du concentrateur, vous pouvez définir les capacités B2B de vos participants. Vous pouvez également leur laisser le soin d'effectuer cette opération. Dans ce chapitre, vous apprendrez comment exécuter cette tâche pour les participants.

La fonction Capacités B2B vous permet d'associer les capacités B2B d'un participant à une définition de flot de documents.

Pour définir les capacités B2B de chaque participant, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère de recherche pour afficher la liste de tous les participants.
3. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du participant.
4. Cliquez sur **Capacités B2B**. La page des capacités B2B s'affiche. Dans la partie de droite apparaissent les regroupements, les protocoles et les flots de documents pris en charge par le système en tant que définitions du flot de documents.
5. Cliquez sur l'icône **Role inactif**, sous la colonne **Définition de la source** pour les regroupements de la partie droite qui contiennent des documents à envoyer aux participants ou au Gestionnaire de communauté.
6. Si les participants 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 du flot de documents est activée.

   Remarque : La sélection de la Définition de la source sera la même pour toutes les actions d'un processus PIP à double sens même si la requête provient d'un participant et la confirmation associée d'un autre. Cela vaut également pour la colonne Définition de la cible.
7. Cliquez sur l'icône **Développer** au niveau **Regroupement** pour développer un noeud jusqu'au niveau Définition du flot de documents approprié, ou sélectionnez un nombre de **0 à 4**, ou cliquez sur **Tous** pour développer toutes les définitions de flot de documents affichées, jusqu'au niveau sélectionné.
8. Sélectionnez à nouveau **Définition de la source**, **Définition de la cible** ou les deux rôles à la fois pour les niveaux inférieurs **Protocole** et **Flot de documents**, pour chaque définition de flot de documents prise en charge par votre système.

   Si une définition est activée au niveau **Flot de documents**, les définitions **Action** et **Activité** (s'il en existe) seront activées automatiquement.
9. Cliquez éventuellement sur **Activé** sous la colonne **Activé** pour mettre une définition du flot 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 regroupement est désactivé, toutes les définitions de flot de documents de niveau inférieur de ce même noeud sont également désactivées, même si leur état respectif était Activé. Si une définition du flot de documents de niveau inférieur est désactivée, toutes les définitions de niveau supérieur appartenant au même contexte restent activées. Lorsqu'une définition de flot de documents est désactivée, les connexions et attributs existants continuent de fonctionner. La définition de flot de documents désactivée ne fait que limiter la création de nouvelles connexions.

10. Cliquez éventuellement sur l'icône **Edition** si vous souhaitez modifier l'un des attributs d'un protocole, d'un regroupement, d'un flot 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**.

Chapitre 12. Gestion des connexions

Une fois que vous avez créé les capacités B2B des participants, établissez des connexions entre le Gestionnaire de communauté et eux. Ce chapitre contient les rubriques suivantes :

- «Vue d'ensemble»
- «Activation des connexions de participants»
- «Spécification ou modification des attributs», à la page 160

Vue d'ensemble

Configurez une connexion entre les participants pour chaque type de document qui sera échangé. Vous pourrez par exemple avoir plusieurs connexions depuis le Gestionnaire de communauté vers le même participant, car le regroupement, le protocole, le flot de documents, l'action ou la mappe seront différents.

Lorsque vous activez les connexions, vous pouvez préciser les attributs des participants source et cible. Tout attribut défini au niveau de la connexion est prioritaire sur les attributs définis au niveau des capacités B2B (pour un participant particulier) ou au niveau de la définition du flot de documents.

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 112 pour plus d'informations.

Activation des connexions de participants

Les connexions de participants contiennent les informations nécessaires à l'échange de chaque flot de documents. Un document ne peut pas être acheminé tant qu'il n'existe pas de connexion entre le Gestionnaire de communauté et un de ses participants.

Le système crée automatiquement des connexions entre le Gestionnaire de communauté et les participants en fonction de leurs capacités B2B.

Vous devez rechercher ces connexions puis les activer.

Lors de la sélection d'une source et d'une cible, veillez à respecter les recommandations suivantes :

- La source et la cible doivent être uniques.
- Evitez de coupler une passerelle de production et une passerelle de test lors de la sélection d'une source et d'une cible ; à défaut, une erreur se produira.
- La source et la cible doivent être des passerelles de production ou de test.

Pour rechercher des connexions et les activer, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Connexions du participant**. La page Gestion des connexions s'affiche.

2. Sous **Source**, sélectionnez une source. Par exemple, si vous configurez un échange émis par le Gestionnaire de communauté, sélectionnez le Gestionnaire de communauté.
3. Sous **Cible**, sélectionnez une cible. Par exemple, si vous configurez un échange qui sera reçu par un participant, sélectionnez ce participant.

   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 contient le regroupement, le protocole et le flot de documents 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».

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

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 Gestionnaire de communauté envoie un document regroupé en tant que Aucun à un participant. Le participant va recevoir le document regroupé en tant que AS. Il est possible que le Gestionnaire de communauté ait plusieurs ID Métier. 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 **Aucun**.
   c. Sélectionnez dans la liste **Mettre à jour** l'ID AS qui doit être envoyé au participant.
   d. Cliquez sur **Enregistrer**.

   Remarque : Si vous avez indiqué précédemment un ID AS (sur la page des capacités B2B, par exemple), la valeur entrée supplante toute valeur antérieure.

   Un autre exemple de configuration d'attribut consiste à entrer une valeur pour l'adresse lorsque vous recevez des documents regroupés en tant que AS à partir d'un participant. L'adresse indique où le MDN est fourni.

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 **Passerelles** pour consulter ou modifier la passerelle 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 définis au niveau de la connexion sont prioritaires sur les attributs définis au niveau du protocole ou du flot de documents.

Chapitre 13. Configuration de la sécurité pour les échanges entrants et sortants

Avec WebSphere Partner Gateway, vous pouvez installer et utiliser plusieurs types de certificats pour les transactions entrantes et sortantes. Ce chapitre contient les rubriques suivantes :

Sécurité, termes et concepts

Cette section fournit une présentation générale des types de sécurité, des outils utilisés pour générer et télécharger les certificats, ainsi que les types de magasins de données installés par WebSphere Partner Gateway.

Mécanismes et protocoles de sécurité utilisés dans WebSphere Partner Gateway

Cette section présente la couche SSL, les signatures numériques et le chiffrement.

Couche SSL

WebSphere Partner Gateway peut utiliser la couche SSL pour sécuriser les documents entrants et sortants. Un document entrant est celui envoyé au concentrateur. Un document sortant est celui envoyé à partir du concentrateur.

SSL est un protocole couramment utilisé pour la gestion de la sécurité sur Internet. La couche SSL sécurise les connexions en permettant à deux applications reliées par une liaison réseau de s'identifier l'une l'autre et en assurant la confidentialité et l'intégrité des données.

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 numériques, se mettent d'accord sur les algorithmes de chiffrement à utiliser et génèrent des clés de chiffrement pour le reste de la session.

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 accepte également les algorithmes AES et DES. Vous pouvez définir ces algorithmes dans le fichier bcg.properties ou à l'aide de l'API SecurityService. Pour plus de détails sur le fichier bcg.properties, consultez le *Guide de l'administrateur*. Consulter le *Programmer Guide* pour plus d'informations sur SecurityService.

Le protocole SSL fournit les dispositifs de sécurité suivants :

- authentification du serveur, signifiant que le serveur utilise son certificat numérique pour s'authentifier auprès des clients ;
- authentification du client, une étape facultative au cours de laquelle il peut être demandé aux clients de s'authentifier auprès du serveur en fournissant leur propre certificat numérique.

Signature numérique

La signature numérique est la méthode pour assurer l'irréfutabilité. Cela signifie qu'un participant ne peut pas nier être à l'origine d'un message et l'avoir envoyé. Cela assure également que le participant ne peut pas nier avoir reçu un message.

Une signature numérique permet à l'expéditeur de signer un message afin de pouvoir vérifier qu'il est bien à l'origine de l'envoi. Elle permet également de s'assurer que le message n'a pas été modifié depuis qu'il a été signé.

WebSphere Partner Gateway prend en charge les formats de signature numérique PKCS#7 SignedData, selon les protocoles métier.

Chiffrement

WebSphere Partner Gateway utilise un système de chiffrement à clé publique pour sécuriser les communications entre les participants et le concentrateur. Le chiffrement à clé publique utilise une paire de clés mathématiquement liées. Un document chiffré avec la première clé ne peut être déchiffré qu'avec la seconde, et réciproquement.

Chaque participant d'un système de clé publique dispose d'une paire de clés. L'une des clés est maintenue secrète, il s'agit de la clé privée. clé privée. L'autre clé est distribuée à quiconque la demande, il s'agit de la clé publique. WebSphere Partner Gateway utilise une clé publique de participant pour chiffrer un document. La clé privée est utilisée pour le déchiffrer.

Utilitaire iKeyman

Comme décrit dans les sections suivantes, l'outil IBM de gestion des clés (iKeyman) est utilisé pour créer des bases de données de clés, des paires de clés publiques et privées et des demandes de certificats. Vous pouvez également utiliser iKeyman pour créer des certificats auto-signés. L'utilitaire iKeyman se trouve dans le répertoire /<*ProductDir*>/was/bin, créé par WebSphere Partner Gateway au cours de l'installation.

Vous pouvez également utiliser iKeyman pour générer une demande de certificat auprès d'une autorité de certification.

Console de communauté

Vous utiliserez la Console de communauté pour installer tous les certificats client, de signature et de chiffrement pour le stockage de WebSphere Partner Gateway. Vous pouvez également utiliser la Console de communauté pour installer les certificats racine et intermédiaires d'autorité de certification.

Remarque : Lorsque le certificat d'un participant expire, la responsabilité lui incombe d'obtenir un nouveau certificat. La Console de communauté inclut des fonctions d'alerte d'expiration pour les certificats stockés dans WebSphere Partner Gateway.

Magasins de clés et magasins de relations de confiance

Lors de l'installation de WebSphere Partner Gateway, un magasin de clés et un magasin de relations de confiance sont également installés pour le Réceptionnaire et la Console.

- 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 de CA et auto-signés de vos participants. La clé publique est stockée comme un certificat de signataire. Pour une autorité de certification commerciale, le certificat de CA racine est ajouté. Le fichier de magasin de relations de confiance peut être accessible à un plus large public. Il contient tous les certificats dignes de confiance.

Par défaut, les deux magasins de clés et les deux magasins de relations de confiance sont créés dans le répertoire *<ProductDir>*/common/security/keystore, sous les noms suivants :

- receiver.jks
- receiverTrust.jks
- console.jks
- consoleTrust.jks

Modification du mot de passe par défaut

Le mot de passe par défaut permettant d'accéder aux quatre magasins est WebAS. L'application WebSphere Application Server est configurée pour utiliser ces quatre magasins. Vous pouvez utiliser l'utilitaire iKeyman pour changer le mot de passe. Vous pouvez aussi utiliser la commande Unix suivante pour modifier le mot de passe du fichier de magasin de clés :

```
/<ProductDir>/console/was/java/bin/keytool
 -storepasswd -new $NEW_PASSWORD$ -keystore $KEYSTORE_LOCATION$
 -storepass $CURRENT_PASSWORD$ -storetype JKS
```

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 Réceptionnaire 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 d'ajout.
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**.

Hiérarchies de certificats

Une hiérarchie de certificats se compose des certificats d'un participant et de tout certificat utilisé pour les authentifier. Par exemple, si un CA a été utilisé pour créer le certificat du participant, ce CA peut avoir lui-même avoir été certifié par un autre CA. 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 des relations de confiance et le certificat du participant (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 participant.

Certificat principal et certificat secondaire

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. 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 participant
- Certificat de signature de l'opérateur du concentrateur
- Certificat client SSL pour l'opérateur du concentrateur

Modification de la puissance du chiffrement

Prenez note des limitations importantes formulées ci-dessous, concernant l'utilisation de certificats de 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 de chiffrement symétriques, tels que DES3. 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.

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/142/.
2. Décompressez le fichier dans un dossier temporaire
3. Copiez les fichiers local_policy.jar et US_export_policy.jar depuis ce dossier temporaire.
4. Passez dans le répertoire <*ProductDir*>\was\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. Collez les fichiers copiés à l'étape 3 dans le dossier où vous êtes, <*ProductDir*>\was\java\jre\lib\security.
7. Redémarrez le serveur.

Ces étapes s'appliquent à toutes les instances configurées de WebSphere Application Server.

Création et installation de certificats 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 la couche SSL, ni vous, ni vos participants n'avez besoin de certificat SSL pour les communications entrantes ou sortantes.

Négociation SSL

Chaque session SSL commence par une négociation.

Lorsqu'un client (le participant ou le Gestionnaire de communauté) initie un échange de message, le processus est le suivant :

1. Le client envoie un message de salutation ″hello″ avec ses capacités 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.

Certificats SSL entrants

Cette section explique comment configurer l'authentification du serveur et du client pour les demandes de connexion entrantes émises par les participants.

Authentification serveur

WebSphere Application Server utilise le certificat SSL lorsqu'il reçoit des demandes de connexion de participants via SSL. Il s'agit du certificat que le réceptionnaire présente pour identifier le concentrateur auprès du participant. 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 pour générer un certificat et une paire de clés. Pour plus d'informations sur l'utilisation d'iKeyman, 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 participants. Si vous disposez de plusieurs réceptionnaires ou consoles, copiez le magasin de clés résultant sur chaque instance. Si le certificat est auto-signé, fournissez-le aux participants. Pour obtenir ce certificat, utilisez l'utilitaire iKeyman afin d'extraire le certificat public dans un fichier.

Utilisation 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 le répertoire /<*ProductDir*>/was/bin. Si c'est la première fois que vous utilisez iKeyman, supprimez le certificat "fictif" (dummy) se trouvant dans le magasin de clés.
2. Utilisez iKeyman pour générer un certificat auto-signé et une paire de clés pour le magasin de clés du réceptionnaire ou de la console.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.

   Enregistrez le magasin de clés dans un fichier JKS, PKCS12 ou JCEK.
4. Installez le fichier dans le magasin de clés du réceptionnaire ou de la console pour lequel il a été créé.
5. Distribuez le certificat à vos participants. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos participants doivent vous appeler et vous demander le mot de passe correspondant au fichier compressé.

Utilisation 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 /<*ProductDir*>/was/bin.
2. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le réceptionnaire.
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 l'autorité de certification à tous les participants.

Authentification client

Si vous souhaitez authentifier les participants qui envoient des documents, procédez comme suit.

Installation du certificat du client : Pour l'authentification client, utilisez la procédure ci-dessous.

1. Procurez-vous un certificat pour votre participant.
2. Installez le ou les certificats dans le magasin de clés de relations de confiance à l'aide de iKeyman.
3. Placez la ou les CA associées dans le magasin de clé correspondant.

Remarque : Si vous ajoutez plusieurs participants à la communauté de votre concentrateur, vous pouvez utiliser iKeyman pour ajouter leurs certificats au magasin de relations de confiance. Si un participant quitte la communauté, vous pouvez utiliser iKeyman pour supprimer ses certificats du magasin de relations de confiance.

Configuration de l'authentification du client : 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 redémarrez le serveur bcgreceiver pour que ces modifications prennent effet.

Validation du certificat du client : 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 Métier contenus dans les documents entrants. Pour pouvoir utiliser cette fonction, créez le profil du participant, importez le certificat client et marquez-le comme SSL.

1. Importez le certificat du client.
   a. Cliquez sur **Administrateur du compte > Profils > Participant de communauté** et recherchez le profil du participant.
   b. Cliquez sur **Certificats**.
   c. Cliquez sur **Charger le certificat**.
   d. Sélectionnez **Client SSL** comme type de certificat.
   e. Tapez une description du certificat (obligatoire).
   f. Faites passer l'état sur **Activé**.
   g. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
   h. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
   i. Si vous souhaitez sélectionner un autre type de passerelle que **Production** (valeur par défaut), faites-le.
   j. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.
2. Mettez à jour la passerelle du client.
   a. Cliquez sur **Administrateur du compte > Profils > Participant de communauté** et recherchez le profil du participant.
   b. Cliquez sur **Passerelles**.
   c. Sélectionnez la passerelle HTTPS précédemment créée. Si vous n'avez pas encore créé la passerelle HTTPS, consultez la section «Configuration d'une passerelle HTTPS», à la page 139.
   d. Cliquez sur l'icône **Edition** pour modifier la passerelle.
   e. Sélectionnez **Oui** pour **Valider le certificat client SSL**.
   f. Cliquez sur **Enregistrer**.

Certificat SSL pour les communications sortantes

Si votre communauté n'utilise pas la couche SSL, vous n'avez pas besoin de certificat SSL pour les communications entrantes ou sortantes.

Authentification serveur

Si la couche SSL est utilisée pour envoyer des documents sortants à vos participants, WebSphere Partner Gateway leur demande un certificat côté serveur. Le même certificat de CA peut être utilisé pour plusieurs participants. 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 participant 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 **Certificats**.
2. Cliquez sur **Charger les certificats**.
3. Sélectionnez **Racine et intermédiaire** 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. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

Remarque : Il est inutile d'effectuer les étapes précédentes si le certificat de CA est déjà installé.

Authentification client

Si une authentification SSL client est requise, le participant 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 participant. S'il s'agit d'un certificat signé par une autorité de certification, il doit être envoyé aux participants, de sorte qu'ils puissent l'ajouter à leurs certificats dignes de confiance.

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 ou n'est pas utilisable.

Utilisation d'un certificat auto-signé : 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 participants. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos participants 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.
   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 type de passerelle que **Production** (valeur par défaut), faites-le.
   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) : 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 réceptionnaire.
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 de signature de l'autorité de certification à tous les participants.

Ajout d'un liste de retrait 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 participants qui ont révoqué des certificats avant leur date d'expiration prévue. Les participants 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.

Les listes de retrait de certificats sont à l'emplacement suivant : /*<répertoire de données partagées>*/security/crl. WebSphere Partner Gateway utilise le paramètre bcg.CRLDir dans le fichier bcg.properties pour déterminer l'emplacement du répertoire CRL.

Créez un fichier .crl contenant les certificats révoqués et placez-le dans le répertoire de la liste de retrait de certificats.

Par exemple, dans le fichier bcg.properties, utilisez le paramètre suivant :

```
bcg.CRLDir=/<répertoire de données partagées>/security/crl
```

Activation de l'accès aux points de distribution des CRL

Les CA se chargent de maintenir et mettre à jour les CRL. Ces listes de retrait de certificats sont en général conservées dans un point de distribution de CRL. Les CRL servent à vérifier si un certificat est retiré.

Le script bcgSetCRLDP.jacl peut servir pour activer et désactiver la vérification du point de distribution de CRL lors de la vérification des certificats retirés. S'il vous faut accéder aux points de distribution de CRL lors de cette vérification, activez leur utilisation. Si les certificats que vous avez installés contiennent une extension CRL DP, vous pouvez activer l'utilisation des points de distribution de CRL, afin qu'ils soient accessibles pour la vérification des certificats retirés. Si vous avez téléchargé toutes les CRL requises dans le répertoire défini par la propriété bcg.CRLDir de bcg.properties, vous pouvez envisager de désactiver l'utilisation des points de distribution de CRL. Si les CRL courantes risquent de ne pas être disponibles dans le répertoire bcg.CRLDir, vous avez intérêt à activer l'utilisation des points de distribution de CRL.

Les points de distribution de CRL accessibles par HTTP et LDAP sont pris en charge. Vous pouvez également configurer des serveurs proxy pour l'accès à ces points.

Remarque : Pour Windows, utilisez `bcgwsadmin.bat` au lieu de `./bcgwsadmin.sh` dans les commandes indiquées dans cette section.

Pour activer l'utilisation des points de distribution de CRL, lancez la commande suivante depuis le répertoire <*ProductDir*>/bin :

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install
 <nomdenoeud> <NomDeServeur> CRLDP
```

où :

<server_root>
Est le répertoire racine du serveur (par exemple `/opt/ibm/receiver/was/profiles/bcgreceiver`)

<NomDeServeur>
Peut être `bcgdocmgr`, `bcgreceiver` ou `bcgconsole`. La commande doit être lancée depuis le *<server_root>* correspondant.

Pour désactiver l'utilisation des points de distribution de CRL, lancez la commande suivante depuis le répertoire *<ProductDir>*/bin :

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl uninstall
<nomdenoeud> <NomDeServeur> CRLDP
```

Pour activer l'utilisation des points de distribution de CRL, avec un serveur proxy, lancez la commande suivante depuis le répertoire *<ProductDir>*/bin :

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl install
 <nomdenoeud> <NomDeServeur> CRLDP
<hôteProxy> <portProxy>
```

Pour indiquer que vous ne voulez pas utiliser de serveur proxy, lancez la commande suivante depuis le répertoire *<ProductDir>*/bin :

```
./bcgwsadmin.sh -f <ProductDir>/scripts/bcgSetCRLDP.jacl
 uninstall <nomdenoeud> <NomDeServeur> PROXY
```

Si vous avez un exit utilisateur de Réceptionnaire, et qu'il utilise l'API SecurityService, les paramètres ci-dessus s'appliquent également au serveur bcgreceiver. Pour lancer les commandes ci-dessus depuis le Réceptionnaire, remplacez `bcgdocmgr` par `bcgreceiver`.

Création et installation de certificats de signature

Cette section apporte des informations sur les certificats de signature, utilisés dans un objectif d'irréfutabilité et pour la vérification du signataire.

Certificat de signature de communication entrante

Le Gestionnaire de documents utilise le certificat signé du participant pour vérifier la signature de l'expéditeur lorsque vous recevez des documents. Les participants vous envoient leurs certificats de signature auto-signés au format X.509 DER. En retour, vous installez les certificats des participants via la Console de communauté sous leur profil respectif.

Pour installer le certificat, utilisez la procédure ci-dessous.

1. Recevez le certificat de signature X.509 du participant au format DER.
2. Installez-le via la Console de communauté sous le profil du participant.
   a. Cliquez sur **Administrateur du compte > Profils > Participant de communauté** et recherchez le profil du participant.
   b. Cliquez sur **Certificats**.
   c. Cliquez sur **Charger les certificats**.
   d. Sélectionnez **Signature numérique** comme type de certificat.
   e. Tapez une description du certificat (obligatoire).
   f. Faites passer l'état sur **Activé**.
   g. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
   h. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.

i. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

3. Si le certificat a été signé par une autorité de certification 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.
   a. 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 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.
4. Activez la signature au niveau regroupement (niveau le plus élevé), participant 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 participant, cliquez sur **Administrateur du compte > Connexions du participant** et sélectionnez les participants. Cliquez sur **Attributs**, puis éditez l'attribut (par exemple **AS signé**).

Certificat de signature de communication sortante

Le Gestionnaire de documents utilise ce certificat lorsqu'il envoie des documents signés aux participants. 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 ou n'est pas utilisable.

Utilisation d'un certificat auto-signé

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 participants. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos participants 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 d'auto-signature et la paire de clés privées sous forme de fichier PKCS12 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**.

      Remarques :

      1) Le fichier PKCS12 envoyé ne doit contenir qu'une seule clé privée et le certificat associé.
      2) Vous pouvez également télécharger le certificat codé au format DER et la clé privée codée en PKCS#8.
   c. Sélectionnez **Signature numérique** 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 un mot de passe.
   i. Si vous avez deux certificats numériques, indiquez s'il s'agit du certificat principal ou secondaire en sélectionnant **Principal** ou **Secondaire** dans la liste **Utilisation du certificat**.
   j. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.
7. Répétez l'étape 6 si le participant dispose d'un second certificat de chiffrement.

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.

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 réceptionnaire.
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 signature de l'autorité de certification à tous les participants.

Création et installation de certificats de chiffrement

Cette section apporte des informations sur les certificats de chiffrement.

Certificat de chiffrement de communication entrante

Ce certificat est utilisé par le concentrateur pour déchiffrer les fichiers codés, reçus de participants. 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 participants. Si un participant envoie un message AS2 chiffré en utilisant le mauvais certificat, le déchiffrage échoue. Toutefois, aucun MDN n'est retourné au participant pour indiquer l'échec. Pour que votre participant puisse recevoir des MDN dans ce cas-là, créez une connexion vers le participant avec la définition de flot de documents suivante :

- Regroupement : **AS**
- Protocole : **Binaire**
- Flot de documents : **Binaire**

Utilisation d'un certificat auto-signé

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 participants. Ils doivent importer le fichier dans leur produit B2B pour l'utiliser comme certificat de chiffrement. Conseillez-leur de l'utiliser lorsqu'ils désirent envoyer des fichiers chiffrés au Gestionnaire de communauté. Si votre certificat est signé par une autorité de certification, fournissez également le certificat de CA.
5. Utilisez iKeyman pour enregistrer le certificat auto-signé et la paire de clés privées sous forme de fichier PKCS12.
6. Installez le certificat d'auto-signature et la paire de clés privées sous forme de fichier PKCS12 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**.

      Remarques :

      1) Le fichier PKCS12 envoyé ne doit contenir qu'une seule clé privée et le certificat associé.
      2) Vous pouvez également télécharger le certificat codé au format DER et la clé privée codée en PKCS#8.
   c. Sélectionnez **Chiffrement** 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 un mot de passe.
   i. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

7. Activez le chiffrement au niveau regroupement (niveau le plus élevé), participant 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 participant, cliquez sur **Administrateur du compte > Connexions du participant** et sélectionnez les participants. Cliquez sur **Attributs**, puis éditez l'attribut (par exemple, **AS chiffré**).

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 réceptionnaire.
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 signature de l'autorité de certification à tous les participants.

Certificat de chiffrement de communication sortante

Ce certificat est utilisé lorsque le concentrateur envoie des documents chiffrés aux participants. WebSphere Partner Gateway chiffre les documents à l'aide des clés publiques des participants et ces derniers déchiffrent les documents avec leurs clés privées.

Le participant peut disposer de plus d'un certificat de chiffrement. L'un est le certificat principal, utilisé par défaut. L'autre est le certificat secondaire, utilisé si le certificat principal expire ou n'est pas utilisable.

1. Procurez-vous le certificat de chiffrement de votre participant. Le certificat doit être au format X.509 DER. Notez que WebSphere Partner Gateway n'accepte que les certificats X5.09.
2. Installez-le via la Console de communauté sous le profil du participant.
   a. Cliquez sur **Administrateur du compte > Profils > Participant de communauté** et recherchez le profil du participant.
   b. Cliquez sur **Certificats**.
   c. Cliquez sur **Charger le certificat**.
   d. Sélectionnez **Chiffrement** comme type de certificat.
   e. Tapez une description du certificat (obligatoire).
   f. Faites passer l'état sur **Activé**.
   g. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
   h. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
   i. Si le participant a deux certificats de chiffrement, indiquez s'il s'agit du certificat principal ou secondaire en sélectionnant **Principal** ou **Secondaire** dans la liste **Utilisation du certificat**.
   j. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.
3. Répétez l'étape 2 si le participant dispose d'un second certificat de chiffrement.

4. Si le certificat a été signé par une autorité de certification 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.
   a. 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 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.
5. Activez le chiffrement au niveau regroupement (niveau le plus élevé), participant 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 participant, cliquez sur **Administrateur du compte > Connexions du participant** et sélectionnez les participants. 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 arriver à expiration ou être retirés. Dans ces cas, l'événement correspondant (`Certificat retiré ou arrivé à expiration`) est également visible dans l'Afficheur d'événements. Notez que ces deux événements peuvent être séparés par d'autres. Pour ouvrir l'Afficheur d'événements, cliquez sur **Afficheurs > Afficheur d'événements**.

Configuration de la couche SSL de communication entrante pour la console et le réceptionnaire

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 la couche SSL de la console et du réceptionnaire 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 Réceptionnaire : <*ProductDir*>/common/security/keystore/receiver.jks et <*ProductDir*>/common/security/keystore/receiverTrust.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 est doit être choisi parmi l'un des formats suivants : JKS, JCEK ou PKCS12. Saisissez cette valeur en majuscules, exactement comme indiqué ;
- le chemin d'accès au fichier script nommé bcgssl.jacl.

2. Ouvrez une fenêtre de Console de communauté et passez dans /<*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 : Répétez ces étapes pour la console, en remplaçant **receiver** par **console** dans le chemin d'accès.

Présentation des certificats

Le tableau 18 résume l'utilisation des certificats dans WebSphere Partner Gateway. L'emplacement des certificats est indiqué entre parenthèses "( )".

Tableau 18. Informations récapitulatives concernant les certificats

Mode de livraison des messages (voir la note 1)	Certificat d'opérateur du concentrateur	Obtenir le certificat et la CA du participant	CA (voir note 2)	Envoyez le certificat au participant (voir note 3)	Commentaires
SSL entrant	S'installe sur le SSL WebSphere Application côté serveur. (Dans le magasin de clés de WebSphere Application Server.)	N/A	Ne sert que si l'authentification du client est utilisée. (Mettre le CA ou le certificat d'auto-signature dans le magasin de relations de confiance de WebSphere Application Server.)	Le certificat d'opérateur de concentrateur est auto-signé, ou le certificat racine de CA est authentifié par l'autorité de certification.	

Tableau 18. Informations récapitulatives concernant les certificats (suite)

Mode de livraison des messages (voir la note 1)	Certificat d'opérateur du concentrateur	Obtenir le certificat et la CA du participant	CA (voir note 2)	Envoyez le certificat au participant (voir note 3)	Commentaires
SSL sortant	Si l'authentification du client est utilisée. (WebSphere Partner Gateway)	Certificat participant côté serveur ou certificat racine de CA, s'il est authentifié par la CA.	WebSphere Partner Gateway	Certificat d'opérateur de concentrateur, s'il est auto-signé, ou clé publique en cas de signature de tierce partie.	
Chiffrement entrant	Clé privée (WebSphere Partner Gateway)	N/A	N/A	Certificat d'opérateur du concentrateur	Pour déchiffrer le message
Signature entrante	N/A	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
Chiffrement sortant	N/A	Utiliser le certificat obtenu du participant. (Le certificat est installé dans le profil du participant)	CA du certificat client, s'il n'est pas auto-signé	N/A	Pour le chiffrement des messages sortants
Signature sortante	Clé privée (WebSphere Partner Gateway)	N/A	N/A	Facultatif, dépend du partenaire ; fournir la clé publique à WebSphere Partner Gateway	
Certificat pour validation DUNS	N/A	Charger dans le profil du participant	Charger le même certificat (celui dans la colonne à gauche) dans le profil d'opérateur du concentrateur, en tant que certificat de CA		Valide que ce certificat est bien pour cet ID DUNS lors du contrôle SSL

Remarques :

1. Un message entrant est un message qui arrive dans WebSphere Partner Gateway, en provenance d'un participant. Un message sortant quitte WebSphere Partner Gateway, vers un participant.
2. Si le certificat est émis par une CA, il faut obtenir et conserver le certificat de cette autorité de certification. Ceci s'applique pour le certificat de l'opérateur du concentrateur ou pour le certificat du participant.
3. Si une clé privée est impliquée, ce certificat lui correspond.

Chapitre 14. Parachèvement de la configuration

Ce chapitre décrit les opérations supplémentaires que vous pouvez effectuer pour configurer le concentrateur. Il contient les rubriques suivantes :

Activation d'API

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*.

Cette procédure vise à activer des API XML pour que les participants puissent les appeler via le serveur WebSphere Partner Gateway.

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**.

Définition des files d'attente utilisées pour les événements

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 n'indiquez pas de valeur dans les zones **Regroupements d'URL fournisseur** ou **URL du fournisseur JMS**, les valeurs par défaut se trouvant dans la section des propriétés MQ du fichier bcg.properties sont utilisées. Ces valeurs par défaut utilisent les liaisons JMS générées au moment de l'installation. Si vous avez opté pour les valeurs par défaut, les liaisons JMS utilisent le port 9999 sur le serveur MQ, désigné au cours de l'installation.

Pour indiquer un autre ensemble de liaisons JMS, modifiez les **Regroupements d'URL du fournisseur** afin qu'ils pointent vers un répertoire contenant un fichier de liaisons JMS que vous avez vous-même préparé. Modifiez également le nom de la **fabrique de connexion de file d'attente** et le **nom de file d'attente** afin qu'ils correspondent aux noms que vous avez choisis dans vos liaisons JMS. Procédez ainsi si vous souhaitez publier les événements dans une file d'attente sur un autre serveur MQ que celui spécifié au cours de l'installation.

Pour indiquer où les événements doivent être livrés, procédez comme suit :

1. Dans le menu principal, cliquez sur **Administration du système > Traitement de l'événement > Information de livraison d'événement**.
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.
   - 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 **Modules 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

Lorsqu'un événement se produit dans WebSphere Partner Gateway, un code d'événement est généré. Dans 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 des noms d'événement de la page 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 :

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 Caractéristiques du code événement s'affiche.
   b. Sélectionnez **Alerte possible**.
   c. Cliquez sur **Sauvegarder**.

Mise à jour d'un transfert défini par l'utilisateur

Comme décrit au Chapitre 5, «Définition des cibles» et au Chapitre 10, «Création de passerelles», à la page 135, vous pouvez télécharger un fichier XML décrivant un transfert défini par l'utilisateur. Vous utiliserez pour cela **Gérer les types de transferts**. Une fois le fichier XML envoyé, le transfert peut être utilisé lors de la définition d'une cible ou d'une passerelle.

Le fichier XML qui décrit le transfert défini par l'utilisateur inclut les attributs du transfert. Ces attributs sont affichés (dans la section **Attributs de transport personnalisés**) sur la page de la cible ou de la passerelle lorsque vous spécifiez un transfert défini par l'utilisateur. Par exemple, un transfert défini par l'utilisateur pour une passerelle peut inclure l'attribut GatewayRetryCount.

L'auteur du fichier XML décrivant le transfert 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 transferts** pour envoyer le fichier. Toute modification apportée aux attributs apparaît dans la page de la passerelle ou de la cible.

Annexe A. Exemples simple

La présente annexe propose des exemples de configuration du concentrateur. Elle 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 193
- «Extension de la configuration de base», à la page 199

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 Annexe B, «Exemples d'EDI», à la page 205.

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 métier).

Configuration de base – Echange de documents EDI avec passe-système

Dans cet exemple, la configuration du concentrateur est relativement simple—deux cibles sont définies : une pour les documents entrant dans le concentrateur émis par un participant, et une autre pour les documents entrant dans le concentrateur en provenance du système dorsal du Gestionnaire de communauté). Les échanges définis dans cet exemple utilisent les définitions de flot de documents fournies par WebSphere Partner Gateway ; autrement dit, les connexions qui sont créées sont basées sur ces flots. Cet exemple ne fait appel à aucun format XML.

Cet exemple illustre un échange entre une application dorsale du Gestionnaire de communauté et un participant (Partenaire B).

Configuration du concentrateur

La première étape de configuration du concentrateur consiste à créer les deux cibles.

- Une cible HTTP (appelée “CibleHttp”) pour recevoir via HTTP (du Partenaire B) les documents qui doivent être envoyés au système dorsal du Gestionnaire de communauté.
- Une cible Fichier-répertoire (appelée “CibleSystèmeFichiers”) pour extraire des documents du système de fichiers (à partir du système dorsal du Gestionnaire de communauté) et devant être envoyés au Partenaire B.

Définition des cibles

Pour créer une cible pour la réception de documents sur HTTP :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Cliquez sur **Créer la cible**.
3. Dans la zone Nom de la cible, entrez **CibleHttp**.
4. Dans la liste Transfert, sélectionnez **HTTP/S**.
5. En ce qui concerne le type de passerelle, 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 une cible afin d’interroger un répertoire dans le système de fichiers. La création de la cible entraîne celle, automatique, d’un nouveau répertoire dans le système de fichiers.

Pour créer la cible dans le système de fichiers, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles**.
2. Cliquez sur **Créer la cible**.
3. Dans la zone Nom de la cible, entrez **CibleSystèmeFichiers**.
4. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
5. En ce qui concerne le Type de passerelle par défaut, utilisez la valeur par défaut, à savoir, **Production**.
6. Dans la zone Répertoire principal du document, tapez **\temp\CibleSystèmeFichiers**

   Remarque : Le répertoire CibleSystèmeFichiers 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 flots de documents et des interactions

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 la section Annexe B, «Exemples d’EDI», à la page 205 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 regroupement, du Gestionnaire de communauté vers le Partenaire B.
- envoi d'un document EDI-X12, regroupé AS2, du Partenaire B vers le Gestionnaire de communauté ;

Du fait du regroupement et des protocoles mis en oeuvre, il n'est pas utile de créer une nouvelle définition de flot de documents. Les regroupements, protocoles et flots de documents sont ceux prédéfinis dans le système.

Toutefois, vous devez définir des interactions basées sur ces flots de documents prédéfinis.

Créez la première interaction, dont la source est un document au format ISA conforme au standard EDI-X12 sans regroupement, et la cible un document ISA conforme au standard EDI-X12 avec regroupement AS.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Dans la colonne **Source**, développez :
   a. **Regroupement : Aucun**
   b. **Protocole : EDI-X12**
4. Cliquez sur **Flot de documents : ISA**
5. Dans la colonne **Cible**, développez:
   a. **Regroupement : AS**
   b. **Protocole : EDI-X12**
6. Cliquez sur **Flot 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 regroupement AS, et la cible un document ISA conforme au standard EDI-X12 sans regroupement :

1. Cliquez sur **Création d'une interaction**.
2. Dans la colonne **Source**, développez :
   a. **Regroupement :AS**
   b. **Protocole : EDI-X12**
3. Cliquez sur **Flot de documents : ISA**
4. Dans la colonne **Cible**, développez:
   a. **Regroupement : Aucun**
   b. **Protocole : EDI-X12**
5. Cliquez sur **Flot de documents :ISA**
6. Dans la liste des **actions**, sélectionnez **Passe-système**.
7. Cliquez sur **Sauvegarder**.

Création de participants et de connexions de participants

Dans cet exemple, un participant externe est créé, en plus du Gestionnaire de communauté. Les passerelles pour les participants comprennent des transferts standard. En outre, aucun point de configuration n'est défini pour les passerelles.

Création des participants

Créez deux nouveaux participants. Pour définir le Gestionnaire de communauté :

1. Cliquez sur **Administrateur du compte** dans le menu principal. La page Recherche du participant 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 participant**, tapez : **Gest Com**.
5. Pour le **Type de participant**, sélectionnez **Gestionnaire de communauté**
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 > Participant de communauté**.
2. Cliquez sur **Créer**.
3. Dans la zone **Nom de connexion de l'entreprise**, tapez **partenaireB**
4. Dans la zone **Nom affiché du participant**, tapez : **Partenaire B**
5. Pour le **Type de participant**, sélectionnez **Participant de communauté**
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 Gestionnaire de communauté et le Partenaire B pour le concentrateur.

Les étapes suivantes consistent à configurer les passerelles pour le Gestionnaire de communauté et le Partenaire B.

Création des passerelles

Avant de créer une passerelle fichier-répertoire pour le Gestionnaire de communauté, vous devez créer la structure de répertoire utilisée par cette passerelle. Créez un nouveau répertoire PasserelleSystèmeFichiers sur l'unité principale. Ce répertoire sera utilisé par le Gestionnaire de communauté pour stocker les fichiers reçus des participants.

Pour le Gestionnaire de communauté, la passerelle représente le point d'entrée dans le système dorsal.

Pour créer une passerelle pour le Gestionnaire :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez **Gest Com** en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Passerelles** dans la barre de navigation horizontale.
5. Cliquez sur **Créer**.
6. Dans la zone **Nom de la passerelle**, tapez **PasserelleSystèmeFichiers**
7. Pour **Transfert**, sélectionnez **Répertoire de fichiers**.
8. Dans la zone **Adresse**, tapez **file://C:\PasserelleSystèmeFichiers**
9. Cliquez sur **Sauvegarder**.

Ensuite, définissez cette passerelle nouvellement créée comme passerelle par défaut du Gestionnaire de communauté.

1. Cliquez sur **Liste** pour dresser la liste de toutes les passerelles configurées pour le Gestionnaire de communauté.
2. Cliquez sur **Afficher les passerelles par défaut**.
3. Dans la liste **Production**, sélectionnez **PasserelleSystèmeFichiers**.
4. Cliquez sur **Sauvegarder**.

Créez une passerelle pour le Partenaire B :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**, puis sélectionnez **Partenaire B** en cliquant sur l'icône **Afficher les détails**.
3. Cliquez sur **Passerelles** dans la barre de navigation horizontale.
4. Cliquez sur **Créer**.
5. Dans la zone **Nom de la passerelle**, tapez **PasserelleHttp**
6. Sélectionnez le mode de **Transfert 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 participant se connectant à son système.

Vous devez à nouveau définir une passerelle par défaut pour ce participant.

1. Cliquez sur **Liste** puis sur **Afficher les passerelles par défaut**.
2. Dans la liste **Production**, sélectionnez **PasserelleHttp**.
3. Cliquez sur **Sauvegarder**.

Définition des capacités B2B

L'étape suivante consiste à définir les capacités B2B du Gestionnaire de communauté.

1. Dans le menu principal, cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez **Gest Com** en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Capacités B2B** dans la barre de navigation horizontale.
5. Définissez la source et la cible pour Regroupement : Aucun, Protocole : EDI-X12 et Flot de documents : ISA en suivant les étapes suivantes :
   a. Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : Aucun**.
   b. Cliquez sur l'icône **Rôle inactif** sous **Définir la cible** pour **Regroupement : Aucun**.
   c. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**.
   d. Cliquez sur l'icône **Rôle inactif** de **Protocole : EDI-X12 (TOUT)** 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 **Flot de documents : ISA** pour la source et la cible.

Ensuite, définissez les capacités B2B du Partenaire B.

1. Dans le menu principal, cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**.
3. Sélectionnez le Partenaire B en cliquant sur l'icône **Afficher les détails**.
4. Cliquez sur **Capacités B2B** dans la barre de navigation horizontale.
5. Sélectionnez Définition de la source et Définition de la cible pour Regroupement : AS, Protocole : EDI-X12 et Flot de documents : ISA en effectuant les opérations suivantes :
   a. Cliquez sur l'icône **Rôle inactif** sous **Définir la source** pour **Regroupement : AS**.
   b. Cliquez sur l'icône **Rôle inactif** sous **Définir la cible** pour **Regroupement : AS**.
   c. Cliquez sur l'icône **Développer** en regard de **Regroupement : AS**.
   d. Cliquez sur l'icône **Rôle inactif** de **Protocole : EDI-X12 (TOUT)** 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 **Flot de documents : ISA** pour la source et la cible.

Définition des connexions des participants

Définissez la connexion des participants pour les documents EDI sans regroupement envoyés par le Gestionnaire de communauté au Partenaire B.

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
2. Dans la liste **Source**, sélectionnez **Gest Com**.
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) Regroupement : **Aucun (N/A)**
      2) Protocole : **EDI-X12 (TOUT)**

3) Flot de documents : **ISA (TOUT)**

b. **Cible**

1) Regroupement : **AS (N/A)**

2) Protocole : **EDI-X12 (TOUT)**

3) Flot de documents : **ISA (TOUT)**

Ensuite, définissez la connexion pour les documents EDI encapsulés dans le regroupement AS2 envoyés sans regroupement au Gestionnaire de communauté 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 du participant**.
2. Dans la liste **Source**, sélectionnez **Partenaire B**.
3. Dans la liste **Cible**, sélectionnez **Gest Com**.
4. Cliquez sur **Rechercher**.
5. Cliquez sur **Activation** pour la connexion comportant les détails suivants :

   a. **Source**

   1) Regroupement : **AS (N/A)**

   2) Protocole : **EDI-X12 (TOUT)**

   3) Flot de documents : **ISA (TOUT)**

   b. **Cible**

   1) Regroupement : **Aucun (N/A)**

   2) Protocole : **EDI-X12 (TOUT)**

   3) Flot de documents : **ISA (TOUT)**

Ensuite, sélectionnez Attributs en regard de la zone **Regroupement : AS (N\A)** pour le Partenaire B.

1. Modifiez les attributs de Regroupement : AS (N\A) en faisant défiler la page et en cliquant sur l'icône **Développer** en regard de **Regroupement : 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

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 Réceptionnaire, receiver.jks. Dans la barre de menus, sélectionnez **Key Database File Open**. Dans le cas d'une installation par défaut, receiver.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 receiver.jks. Ce mot de passe est WebAS.
4. Si vous ouvrez le fichier receiver.jks pour la première fois, supprimez le certificat "fictif" (dummy).

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 Réceptionnaire 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 Réceptionnaire 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 transfert 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 > Participant de communauté**.
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 passerelle du Partenaire B de sorte qu'elle utilise le protocole HTTP sécurisé.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté** 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 **Passerelles** dans la barre de navigation horizontale. Ensuite, sélectionnez HttpGateway en cliquant sur l'icône **Afficher les détails**.
4. Modifiez-le en cliquant sur l'icône **Edition**.
5. Sélectionnez la valeur de transfert **HTTPS/1.1**

6. Modifiez la valeur de l'adresse comme suit : **https://<***IP_address***>: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

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 > Participant de communauté** 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 Type de passerelle associé à la valeur **Production**.
12. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

La procédure de configuration requise pour permettre à un participant 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 participant. Pour cela, vous devez charger le certificat public dans le concentrateur.

1. Dans le menu principal, cliquez sur **Administrateur du compte > Profils > Participant de communauté**.

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 paramètre Type de passerelle sur **Production**.
13. Cliquez sur **Télécharger**, puis sur **Sauvegarder**.

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 Gestionnaire de communauté et le Partenaire B.

Pour modifier cette connexion dans la Console de communauté, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Connexions du participant** 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, notez que la valeur courante de l'attribut **AS chiffré** est **Non**. Modifiez cette valeur en cliquant sur l'icône **Développer** en regard de **Regroupement : 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

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 participant, en vue de l'utilisation de 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 partenaireBSignature.der à la disposition du concentrateur.

Pour charger le certificat numérique dans le concentrateur, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté** 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 participant utilise le certificat public pour authentifier les transactions signées qui sont envoyées au concentrateur.

Le concentrateur quant à lui utilisera la clé privée pour signer numériquement les transactions sortantes envoyées au participant. 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 Gestionnaire de communauté et le Partenaire B, en vue de permettre l'envoi d'une transaction AS2 signée.

Pour modifier les attributs de la connexion des participants, procédez comme suit :

1. Cliquez sur **Administrateur du compte > Connexions du participant** dans la barre de navigation horizontale.
2. Sélectionnez **Gest Com** 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 **Regroupement : 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 participant 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 Gestionnaire de communauté appelé Gest Com, avec un ID DUNS de 123456789 et une passerelle fichier-répertoire), et décrit la procédure à suivre pour ajouter la prise en charge de :

- mode de transfert FTP ;
- documents XML personnalisés ;
- fichiers binaires (sans regroupement)

Création d'une cible FTP

La cible 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 19, avant de créer une cible FTP, vous devez disposer d'un serveur FTP configuré ainsi que d'un répertoire FTP.

Dans cet exemple, on suppose que le seveur 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 > Cibles**.
2. Cliquez sur **Créer la cible**.
3. Entrez les informations suivantes :
   a. Nom de la cible : **Réceptionnaire_FTP**
   b. Transfert : **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 Gestionnaire de communauté.

Création d'une interaction pour les documents binaires

Par défaut, WebSphere Partner Gateway fournit quatre interactions impliquant des documents binaires. Toutefois, il ne propose pas d'interaction pour les documents binaires en regroupement de type Aucun et destinés à un participant dont les documents sont également regroupés en tant que Aucun. Cette section vous indique comment créer l'interaction nécessaire pour permettre aux documents binaires de transiter par le système.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.

2. Cliquez sur **Gestion des interactions**.
3. Cliquez sur **Création d'une interaction**.
4. Au niveau du paramètre **Source**, sélectionnez **Regroupement : Aucun Protocole : Binaire (1.0) Flot de documents : Binaire (1.0)**.
5. Au niveau du paramètre **Cible**, sélectionnez **Regroupement : Aucun Protocole : Binaire (1.0) Flot de documents : Binaire (1.0)**.
6. Dans la liste des **actions**, sélectionnez **Passe-système**.
7. Cliquez sur **Sauvegarder**.

Mise à jour des capacités B2B pour le Gestionnaire de communauté

Cette section explique comment configurer le Gestionnaire de communauté pour qu'il accepte des documents binaires.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**.
3. Cliquez sur l'icône **Afficher les détails** en regard de **Gest Com**.
4. Cliquez sur **Capacités B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**.
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** de **Flot de documents : Binaire (1.0)** sous **Définition de la cible**.

Mise à jour des capacités B2B du Partenaire B

Cette section explique comment configurer le partenaire A pour lui permettre d'envoyer des documents binaires.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**.
3. Cliquez sur l'icône **Afficher les détails** en regard du Partenaire B.
4. Cliquez sur **Capacités B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : Aucun** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**.
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** de **Flot de documents : Binaire (1.0)** sous **Définition de la source**.

Création d'une nouvelle connexion de participants

Cette section explique comment configurer une nouvelle connexion de participant entre le Gestionnaire de communauté et le Partenaire B pour des documents binaires.

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
2. Sélectionnez **Partenaire B** dans la liste **Source**.

3. Sélectionnez **Gest Com** dans la liste **Cible**.
4. Cliquez sur **Rechercher**.
5. Localisez la connexion **Aucun (N/A), Binaire (1.0), Binaire (1.0)** à **Aucun (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 au «Création de documents XML personnalisés», à la page 86, 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>
        <From>987654321</From>
       <To>123456789</To>
   </Tester>
```

Le Gestionnaire de documents utilise le code 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 participant d'origine et du participant de destination.

Création d'un format de définition de protocole CustomXML

La première étape consiste à créer le nouveau protocole CustomXML que vous allez échanger.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Création d'une définition du flot de documents**.
3. Sélectionnez **Protocole** dans la liste **Type de flot de documents**.
4. Entrez les informations suivantes :
   a. Code : **CustomXML**
   b. Version : **1.0**
   c. Description : **CustomXML**
5. Réglez le paramètre **Niveau du document** sur **Non**.
6. Réglez le paramètre **Etat** sur **Activé**.
7. Réglez le paramètre **Visibilité : Opérateur de communauté** sur **Oui**.
8. Réglez le paramètre **Visibilité : Gestionnaire de communauté** sur **Oui**.
9. Réglez le paramètre **Visibilité : Participant de communauté** sur **Oui**.
10. Sélectionnez les éléments suivants :
    a. Regroupement : **AS**
    b. Regroupement : **Aucun**
    c. Regroupement : **Intégration dorsale**
11. Cliquez sur **Sauvegarder**.

Création de la définition de document Testeur_XML

La deuxième étape consiste à créer une définition de flot de documents pour le nouveau protocole.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.

2. Cliquez sur **Création d'une définition du flot de documents**.
3. Sélectionnez **Flot de documents** dans la liste **Type de flot de documents**.
4. Entrez les informations suivantes :
   a. Code : **Testeur_XML**
   b. Version : **1.0**
   c. Description : **Testeur_XML**
5. Réglez le paramètre **Niveau du document** sur **Oui**.
6. Réglez le paramètre **Etat** sur **Activé**.
7. Réglez le paramètre **Visibilité : Opérateur de communauté** sur **Oui**.
8. Réglez le paramètre **Visibilité : Gestionnaire de communauté** sur **Oui**.
9. Réglez le paramètre **Visibilité : Participant de communauté** sur **Oui**.
10. Cliquez sur l'icône **Développer** en regard de **Regroupement : AS** et sélectionnez **Protocole : CustomXML**.
11. Cliquez sur l'icône **Développer** en regard de**Regroupement : Aucun** et sélectionnez **Protocole : CustomXML**.
12. Cliquez sur l'icône **Développer** en regard de **Regroupement : Intégration dorsale** et sélectionnez **Protocole : CustomXML**.
13. Cliquez sur **Sauvegarder**.

Création du format XML Testeur_XML

Enfin, vous devez créer le format XML associé au nouveau protocole.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Formats XML**.
2. Cliquez sur **Création du format XML**.
3. Sélectionnez **CustomXML 1.0** dans la liste des **Formats d'acheminement**.
4. Sélectionnez **XML** dans la liste **Type de fichiers**.
5. Sélectionnez **Code racine** dans la liste **Type d'identificateur** et indiquez la valeur **Testeur**.
6. Sélectionnez **Chemin d'accès à l'élément** dans la liste **ID Métier source** et indiquez la valeur **/Testeur/From**.
7. Sélectionnez **Chemin d'accès à l'élément** dans la liste **ID Métier cible** et tapez la valeur **/Testeur/To**.
8. Sélectionnez **Constante** dans la liste **Flot de documents source** et indiquez la valeur **XML_Testeur**.
9. Sélectionnez **Constante** pour **Version du flot de documents source**, et indiquez la valeur **1.0**.
10. Cliquez sur **Sauvegarder**.

Création d'une interaction pour les documents XML Testeur_XML

Maintenant que vous disposez d'un nouveau protocole et d'un flot de documents, vous pouvez configurer une interaction.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**.
3. Cliquez sur **Création d'une interaction**.
4. Au niveau du paramètre **Source**, sélectionnez les éléments suivants :
   a. Regroupement : **Aucun**
   b. Protocole : **CustomXML (1.0)**

c. Flot de documents : **Testeur_XML (1.0)**

5. Au niveau du paramètre **Cible**, sélectionnez les éléments suivants :
   a. Regroupement : **Aucun**
   b. Protocole : **CustomXML (1.0)**
   c. Flot de documents : **Testeur_XML (1.0)**
6. Dans la liste des **actions**, sélectionnez **Passe-système**.
7. Cliquez sur **Sauvegarder**.

Mise à jour des capacités B2B pour le Gestionnaire de communauté

Pour permettre l'échange du document XML personnalisé, vous devez mettre à jour les capacités B2B des participants.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**.
3. Cliquez sur l'icône **Afficher les détails** en regard de **Gest Com**.
4. Cliquez sur **Capacités B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**.
7. Cliquez sur l'icône **Rôle inactif** de **Protocole : CustomXML (1.0)** sous **Définition de la cible**.
8. Cliquez sur l'icône **Développer** en regard de **Protocole : CustomXML (1.0)**.
9. Enfin, cliquez sur l'icône **Rôle inactif** de **Flot de documents : XML_Testeur (1.0)** sous **Définition de la cible**.

Mise à jour des capacités B2B du Partenaire B

La mise à jour des capacités B2B du Partenaire B permet l'échange du nouveau format XML personnalisé.

1. Cliquez sur **Administrateur du compte > Profils > Participant de communauté**.
2. Cliquez sur **Rechercher**.
3. Cliquez sur l'icône **Afficher les détails** en regard du Partenaire B.
4. Cliquez sur **Capacités B2B**.
5. Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : Aucun** pour l'activer.
6. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**.
7. Cliquez sur l'icône **Rôle inactif** de **Protocole : CustomXML (1.0)** sous **Définition de la source**.
8. Cliquez sur l'icône **Développer** en regard de **Protocole : CustomXML (1.0)**.
9. Enfin, cliquez sur l'icône **Rôle inactif** de **Flot de documents : XML_Testeur (1.0)** sous **Définition de la source**.

Création d'une nouvelle connexion de participants

Enfin, créez une nouvelle connexion de participants.

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
2. Sélectionnez **Partenaire B** dans la liste **Source**.
3. Sélectionnez **Gest Com** dans la liste **Cible**.
4. Cliquez sur **Rechercher**.

5. Localisez la connexion **Aucun (N/A), CustomXML (1.0), XML_Testeur(1.0)** vers **Aucun (N/A), CustomXML(1.0), XML_Testeur (1.0)**, puis cliquez sur **Activation** pour l'activer.

Annexe B. 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'Annexe A, «Exemples simple», à la page 187. De nouvelles cibles, passerelles et profils sont créés.

Remarque : Un exemple d'EDI traversant le concentrateur (sans désenveloppement ni transformation) est proposé en Annexe A, «Exemples simple».

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 :

- «Exemple EDI vers ROD»
- «Exemple EDI vers XML», à la page 218
- «Exemple de document XML vers EDI», à la page 224
- «Exemple ROD vers EDI», à la page 231

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 métier).

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 Gestionnaire de communauté.

Désenveloppement et transformation d'un EDI

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 Gestionnaire de communauté. 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

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 flot de documents

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 flot de documents auxquelles cette mappe est associée s'affichent :

Tableau 19. Définition de flot de document associée à la mappe

Source	Cible
Regroupement : N/A Protocole : X12V5R1 (ALL) Flot de documents : 850 (TOUT)	Regroupement : Aucun Protocole : DEMO850CL_DICTIONARY(TOUT) Flot de documents : 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 flot de documents (DEMO850CLSUW).

Configuration de la cible

Cette section explique comment créer une cible de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles** puis sur **Créer cible**.
2. Dans la zone Nom de la cible, entrez **CibleFichierEDI**.
3. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
4. Dans Chemin principal, entrez **/Data/Manager/editarget**
5. Cliquez sur **Sauvegarder**.

Le participant de la communauté envoie l'EDI à cette cible.

Création des interactions

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 du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Sous **Source**, développez **Regroupement : Aucun** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
4. Sous **Cible**, développez **Regroupement : N/A** et **Protocole : EDI-X12** puis sélectionnez **Flot 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 **Enregistrer**.

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 du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Sous **Source**, développez **Regroupement : N/A** et **Protocole : X12V5R1** puis sélectionnez **Flot de documents : 850**.
4. Sous **Source**, développez **Regroupement : Aucun** et **Protocole : DEMO850CL_DICTIONARY** puis sélectionnez **Flot 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 conversion EDI**.
7. Cliquez sur **Enregistrer**.

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 participants

Dans cet exemple, vous avez deux participants : le Gestionnaire de communauté (Gestionnaire) et un participant (TP1).

Créez le profil du Gestionnaire de communauté :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du participant, tapez **Gestionnaire**
4. Pour Type de participant, sélectionnez **Gestionnaire de communauté**.
5. Cliquez sur **Nouveau** pour ID métier 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 métier et tapez `01-000000000` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Créez le second participant :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du participant, tapez **TP1**
4. Pour Type de participant, sélectionnez **Participant de communauté**.
5. Cliquez sur **Nouveau** pour ID métier 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 métier et tapez `01-000000001` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Création des passerelles

Créez des passerelles fichier-répertoire pour tous les participants de l'exemple. Créez d'abord une passerelle pour le Gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.
   a. Dans Nom, tapez **PasserelleFichierGestionnaire**.
   b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file:///Data/Manager/filegateway**
   d. Cliquez sur **Enregistrer**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du Gestionnaire de communauté.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4.
8. Cliquez sur **Enregistrer**.

Ensuite, créez une passerelle pour le participant.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Sélectionnez l'autre participant créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **PasserelleFichierTP1**.
   b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file:///Data/TP1/filegateway**

d. Cliquez sur **Enregistrer**.

5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du participant.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4, à la page 208.
8. Cliquez sur **Enregistrer**.

Configuration des capacités B2B

Activez les capacités B2B des deux participants de cet échange. Dans cet exemple, l'EDI est émis par le participant de la communauté (TP1) et sera transmis au Gestionnaire de communauté.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du participant source de cet exemple (**TP1**).
3. Cliquez sur **Capacités B2B**.
4. Activez deux ensembles de capacités pour le participant source.
   a. Tout d'abord, activez la définition de flot de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : Aucun** pour l'activer.
      2) Développez **Regroupement : Aucun**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : ISA (TOUT)**.
   b. Ensuite, activez la définition de flot de documents représentant la transaction 850 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, pour l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : X12V5R1**.
      4) Développez **Protocole X12V5R1 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : 850**.
5. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du participant cible de cet exemple (**Gestionnaire**).
7. Cliquez sur **Capacités B2B**.
8. Activez deux ensembles de capacités pour le participant cible.
   a. Tout d'abord, activez la définition de flot de documents représentant l'enveloppe :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.

3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
4) Développez **Protocole : EDI-X12 (TOUT)**.
5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents : ISA (TOUT)**.

b. Ensuite, activez la définition de flot de documents représentant le document transformé :
1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
2) Développez **Regroupement : Aucun**.
3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : DEMO850CL_DICTIONARY (TOUT)**.
4) Développez **Protocole : DEMO850CL_DICTIONARY (TOUT)**.
5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents : DEMO850CLSUW(TOUT)**.

Activation des connexions

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
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 20. Connexion de l'enveloppe

Source	Cible
Regroupement : Aucun (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)	Regroupement : N/A (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente la transaction 850 vers le document transformé :

Tableau 21. Connexion de la transaction EDI vers le document ROD

Source	Cible
Regroupement : N/A (N/A) Protocole : X12V5R1 Flot de documents : 850 (TOUT)	Regroupement : Aucun (N/A) Protocole : DEMO850CL_DICTIONARY(TOUT) Flot de documents : DEMO850CLSUW (TOUT)

Ajout d'attributs

Définissez les attributs qui autorisent les documents ayant le même ID :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**.
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 flot de documents de la page. Sur la ligne **Autoriser les documents avec des ID en double** de la liste, sélectionnez **Oui**.
5. Cliquez sur **Enregistrer**.

A ce stade, si TP1 envoie un EDI contenant une transaction 850 au Gestionnaire de communauté, l'EDI sera désenveloppé et générera une transaction 850. Cette dernière sera alors transformée dans le type de document DEMO850CLSUW et le document résultant sera envoyé à la passerelle du Gestionnaire de communauté.

Ajout d'un TA1 à un échange

Dans X12, TA1 est un segment optionnel utilisé pour accuser 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

Pour associer la mappe à une définition de flot 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 de regroupement disponible sur le système.
3. Créez l'association à la définition du flot de documents en procédant comme suit :
   a. Cochez la case en regard de **Regroupement : 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 **Flot de documents : ISA (TOUT)**.
   d. Cliquez sur **Enregistrer**.

Vous avez créé une association entre la mappe &WDI_TA1_ACK1 et la définition de flot de documents pour l'enveloppe.

Création d'interactions

Créez une interaction qui représente la transaction TA1.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Sous **Source**, développez **Regroupement : N/A** et **Protocole : &X44TA1** puis sélectionnez **Flot de documents : TA1**.
4. Sous **Source**, développez **Regroupement : N/A** et **Protocole : &X44TA1** puis sélectionnez **Flot de documents : TA1**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Enregistrer**.

Créez une interaction dont une source représente l'enveloppe 850 qui contiendra le TA1.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.

2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Sous **Source**, développez **Regroupement : N/A** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
4. Sous **Source**, développez **Regroupement : Aucun** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Enregistrer**.

Activation des capacités B2B

Ensuite, vous ajoutez les interactions nouvellement créées aux capacités B2B des participants.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du participant source de cet exemple (**Gestionnaire**).

   Remarque : Gardez en mémoire que le TA1 circule du participant qui reçoit le document ROD vers le participant qui l'a envoyé. Dans cet exemple, le Gestionnaire est la source du TA1 et le TP1 du participant en est la cible.
3. Cliquez sur **Capacités B2B**.
4. Activez deux ensembles de capacités pour le participant source.
   a. Tout d'abord, activez la capacité pour le TA1.
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : &X44TA1**.
      4) Développez **Protocole : &X44TA1**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : TA1 (TOUT)**.
   b. Ensuite, activez la capacité pour l'enveloppe :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : EDI-X12**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : ISA (TOUT)**.
5. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du participant cible de cet exemple (**TP1**).
7. Cliquez sur **Capacités B2B**.
8. Activez deux ensembles de capacités pour le participant cible.
   a. Tout d'abord, activez la définition de flot de documents représentant le TAI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : N/A**, afin de l'activer.

2) Développez **Regroupement : N/A**.
3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : &X44TA1 (TOUT)**.
4) Développez **Protocole : &X44TA1 (TOUT)**.
5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents : TA1 (TOUT)**.

b. Ensuite, activez la définition de flot de documents représentant l'enveloppe EDI :
1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
2) Développez **Regroupement : Aucun**.
3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
4) Développez **Protocole : EDI-X12 (TOUT)**.
5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents :ISA (TOUT)**.

Création du profil d'enveloppe

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 EDI :
   - ISA01: **01**
   - ISA02: **ISA0000002**
   - ISA03: **02**
   - ISA04: **ISA0000004**
   - ISA11: \
   - ISA12: **00501**
   - ISA15: **T**
7. Cliquez sur **Enregistrer**.

Activation des connexions de participants

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
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 22. Connexion TA1

Source	Cible
Regroupement : N/A (N/A) Protocole : &X44TA1 (TOUT) Flot de documents : TA1 (TOUT)	Regroupement : N/A (N/A) Protocole : &X44TA1 (TOUT) Flot de documents : TA1 (TOUT)

6. Activez la connexion qui représente l'enveloppe :

Tableau 23. Connexion de l'enveloppe

Source	Cible
Regroupement : N/A (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)	Regroupement : Aucun (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)

Configuration des attributs

Pour préciser les attributs du profil de l'enveloppe :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Sélectionnez **TP1** dans la liste.
3. Cliquez sur **Capacités B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Regroupement : Aucun**.
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 **Enregistrer**.
8. Cliquez de nouveau sur **Capacités B2B**.
9. Cliquez sur l'icône **Développer** en regard de **Regroupement : 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 **Enregistrer**.

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 flot décrit dans «Exemple EDI vers ROD», à la page 205. 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 211, 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 205.

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 «Accusés de réception fonctionnels», à la page 128 pour connaître la liste des mappes fournies avec WebSphere Partner Gateway.

Création des associations

Pour associer la mappe à une définition de flot 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 de regroupement disponible sur le système.
3. Créez l'association avec la définition du flot de documents en procédant comme suit :
   a. Cochez la case en regard de **Regroupement : 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 **Flot de documents : 850**.
   d. Cliquez sur **Enregistrer**.

Vous avez associé cette mappe 997 d'accusé de réception fonctionnel au protocole X12.

Création d'interactions

Créez une interaction qui représente l'accusé de réception 997.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Sous **Source**, développez **Regroupement : N/A** et **Protocole : &DT99724**, puis sélectionnez **Flot de documents : 997**.
4. Sous **Cible**, développez **Regroupement : N/A** et **Protocole : &DT99724**, puis sélectionnez **Flot de documents : 997**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Enregistrer**.

Créez une interaction qui représente l'enveloppe.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Développez **Regroupement : N/A** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
4. Développez **Regroupement : Aucun** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Passe-système**.
6. Cliquez sur **Enregistrer**.

Activation des capacités B2B

Ensuite, vous ajoutez les interactions nouvellement créées aux capacités B2B des participants.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du participant source de cet exemple (**Gestionnaire**).

   Remarque : Gardez en mémoire que l'accusé de réception fonctionnel circule du participant qui reçoit le document ROD vers le participant qui l'a envoyé. Dans cet exemple, le Gestionnaire est la source de l'accusé de réception fonctionnel et le TP1 du participant en est la cible.
3. Cliquez sur **Capacités B2B**.
4. Activez deux ensembles de capacités pour le participant source.
   a. Tout d'abord, activez la capacité pour le FA.
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : &DT99724**.
      4) Développez **Protocole : &DT99724**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : 997 (TOUT)**.
   b. Ensuite, activez la capacité pour l'enveloppe :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : EDI-X12**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : ISA (TOUT)**.
5. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du participant cible de cet exemple (**TP1**).
7. Cliquez sur **Capacités B2B**.
8. Activez deux ensembles de capacités pour le participant cible.
   a. Tout d'abord, activez la définition de flot de documents représentant le 997 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : &DT99724 (TOUT)**.
      4) Développez **Protocole : &DT99724 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents : 997 (TOUT)**.

b. Ensuite, activez la définition de flot de documents représentant l'enveloppe EDI :
   1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
   2) Développez **Regroupement : Aucun**.
   3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
   4) Développez **Protocole : EDI-X12 (TOUT)**.
   5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents :ISA (TOUT)**.

Création du profil d'enveloppe

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 **Enregistrer**.

Activation des connexions de participants

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
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 24. Connexion de l'accusé de réception fonctionnel

Source	Cible
Regroupement : N/A (N/A) Protocole : &DT99724 (TOUT) Flot de documents : 997 (TOUT)	Regroupement : N/A (N/A) Protocole : &DT99724 (TOUT) Flot de documents : 997 (TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente l'enveloppe EDI renvoyée à l'émetteur de l'échange :

Tableau 25. Connexion de l'enveloppe

Source	Cible
Regroupement : N/A (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)	Regroupement : Aucun (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)

Configuration des attributs

Tout d'abord, précisez la mappe d'accusé de réception fonctionnel à utiliser :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Sélectionnez **TP1** dans la liste.
3. Cliquez sur **Capacités B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Regroupement : 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 **Capacités B2B**.
8. Cliquez sur l'icône **Développer** en regard de **Regroupement : 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 **Enregistrer**.

Dans cette série de tâches, vous avez ajouté un accusé de réception fonctionnel EDI-X12 997 à l'échange, afin que lorsque le Gestionnaire de communauté 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 Gestionnaire de communauté.

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 Gestionnaire de communauté. 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

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 flot de documents

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 flot de documents auxquelles cette mappe est associée s'affichent :

Tableau 26. Définition de flot de document associée à la mappe

Source	Cible
Regroupement : N/A Protocole : X12V5R1 Flot de documents : 879 (TOUT)	Regroupement : Aucun Protocole : FVT-XML-TEST (TOUT) Flot de documents : 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 de la cible

Cette section explique comment créer une cible de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles** puis sur **Créer cible**.
2. Dans la zone Nom de la cible, entrez **CibleFichierEDI**.
3. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
4. Dans Chemin principal, entrez **/Data/Manager/editarget**
5. Cliquez sur **Sauvegarder**.

Le participant de la communauté envoie l'EDI à cette cible.

Création des interactions

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 du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Développez **Regroupement : Aucun** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
4. Développez **Regroupement : N/A** et **Protocole : EDI-X12** puis sélectionnez **Flot 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 **Enregistrer**.

Créez une interaction dont une source représente la transaction 879 et une cible le document transformé.

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Développez **Regroupement : N/A** et **Protocole : X12V5R1** puis sélectionnez **Flot de documents : 879**.
4. Développez **Regroupement : Aucun** et **Protocole : FVT-XML-TEST** puis sélectionnez **Flot 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 conversion EDI**.
7. Cliquez sur **Enregistrer**.

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 participants

Dans cet exemple, vous avez deux participants : le Gestionnaire de communauté (Gestionnaire) et un participant (TP1).

Créez le profil du Gestionnaire de communauté :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du participant, tapez **Gestionnaire**
4. Pour Type de participant, sélectionnez **Gestionnaire de communauté**.
5. Cliquez sur **Nouveau** pour ID métier 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 métier et tapez `01-000000000` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Créez le second participant :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du participant, tapez **TP1**
4. Pour Type de participant, sélectionnez **Participant de communauté**.
5. Cliquez sur **Nouveau** pour ID métier 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 métier et tapez `01-000000001` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Création des passerelles

Créez des passerelles fichier-répertoire pour tous les participants de l'exemple. Créez d'abord une passerelle pour le Gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.
   a. Dans Nom, tapez **PasserelleFichierGestionnaire**.
   b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file:///Data/Manager/filegateway**
   d. Cliquez sur **Enregistrer**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du Gestionnaire de communauté.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4.
8. Cliquez sur **Enregistrer**.

Ensuite, créez une passerelle pour le participant.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.

2. Sélectionnez l'autre participant créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **PasserelleFichierTP1**.
   b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file:///Data/TP1/filegateway**
   d. Cliquez sur **Enregistrer**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du participant.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4.
8. Cliquez sur **Enregistrer**.

Configuration des capacités B2B

Activez les capacités B2B des deux participants de cet échange. Dans cet exemple, l'EDI est émis par le participant de la communauté (TP1) et sera transmis au Gestionnaire de communauté.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du participant source de cet exemple (**TP1**).
3. Cliquez sur **Capacités B2B**.
4. Activez deux ensembles de capacités pour le participant source.
   a. Tout d'abord, activez la définition de flot de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : Aucun** pour l'activer.
      2) Développez **Regroupement : Aucun**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : ISA (TOUT)**.
   b. Ensuite, activez la définition de flot de documents représentant la transaction :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : X12V5R1**.
      4) Développez **Protocole X12V5R1 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : 879**.
5. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du participant cible de cet exemple (**Gestionnaire**).

7. Cliquez sur **Capacités B2B**.
8. Activez deux ensembles de capacités pour le participant cible.
   a. Tout d'abord, activez la définition de flot de documents :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents : ISA (TOUT)**.
   b. Ensuite, activez la définition de flot de documents représentant le document transformé :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
      2) Développez **Regroupement : Aucun**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : FVT-XML-TEST (TOUT)**.
      4) Développez **Protocole : FVT-XML-TEST (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents :WWRE_ITEMCREATIONINTERNAL (TOUT)**.

Activation des connexions

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
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 27. Connexion de l'enveloppe

Source	Cible
Regroupement : Aucun (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)	Regroupement : N/A (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente la transaction 879 vers le document transformé :

Tableau 28. Connexion de la transaction EDI vers le document XML

Source	Cible
Regroupement : N/A (N/A) Protocole : X12V5R1 (ALL) Flot de documents : 879 (TOUT)	Regroupement : Aucun (N/A) Protocole : FVT-XML-TEST (TOUT) Flot de documents : WWRE_ITEMCREATIONINTERNAL (TOUT)

A ce stade, si TP1 a envoyé un EDI contenant une transaction 879 au Gestionnaire de communauté, l'EDI sera désenveloppé et générera une transaction 879. Celle-ci sera transformée et le document résultant envoyé à la passerelle du Gestionnaire de communauté.

Exemple de document XML vers EDI

Cette section fournit un exemple d'envoi de document XML par le Gestionnaire de communauté au concentrateur, qui le transforme en transaction EDI enveloppée dans un EDI et l'envoie au participant.

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 participant. 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

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 flot de documents

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 flot de documents auxquelles cette mappe est associée s'affichent :

Tableau 29. Définitions de flot de documents associées à la mappe

Source	Cible
Regroupement : Aucun Protocole : FVT-XML-TEST (TOUT) Flot de documents : ICGCPO (TOUT)	Regroupement : N/A Protocole : MX12V3R1 (TOUT) Flot de documents : 850 (TOUT)

La mappe S_DT_XML_TO_EDI a été définie pour transformer un document XML en transaction EDI.

Configuration de la cible

Cette section explique comment créer une cible de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles** puis sur **Créer cible**.
2. Dans la zone Nom de la cible, entrez **CibleFichierXML**.
3. Dans la liste Transfert, 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 récupérateurs disponibles et cliquez sur **Ajouter** pour le déplacer dans la liste des récupérateurs configurés.
7. Cliquez sur **Sauvegarder**.

Le Gestionnaire de communauté envoie le document XML à cette cible.

Création des interactions

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 **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Développez **Regroupement : Aucun** et **Protocole : FVT-XML-TEST** puis sélectionnez **Flot de documents : ICGCPO**.
4. Développez **Regroupement : N/A** et **Protocole : MX12V3R1**, puis sélectionnez **Flot 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 **Enregistrer**.

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 **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.

3. Développez **Regroupement : N/A** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
4. Développez **Regroupement : Aucun** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
5. Dans la liste des actions, sélectionnez **Passe-système**.

   Remarque : Aucune transformation ne se produit dans cette interaction.
6. Cliquez sur **Enregistrer**.

Création des participants

Dans cet exemple, vous avez deux participants : le Gestionnaire de communauté (Gestionnaire) et un participant (TP1).

Créez le profil du Gestionnaire de communauté :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du participant, tapez **Gestionnaire**
4. Pour Type de participant, sélectionnez **Gestionnaire de communauté**.
5. Cliquez sur **Nouveau** pour ID métier 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 Métier et tapez `01-000000000` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Créez le second participant :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du participant, tapez **TP1**
4. Pour Type de participant, sélectionnez **Participant**.
5. Cliquez sur **Nouveau** pour ID métier 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 métier et tapez `01-000000001` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Création des passerelles

Créez des passerelles fichier-répertoire pour tous les participants de l'exemple. Créez d'abord une passerelle pour le Gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.

a. Dans Nom, tapez **PasserelleFichierGestionnaire**.
b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
c. Dans Adresse, tapez : **file:///Data/Manager/filegateway**
d. Cliquez sur **Enregistrer**.

5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du Gestionnaire de communauté.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4, à la page 226.
8. Cliquez sur **Enregistrer**.

Ensuite, créez une passerelle pour le participant.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Sélectionnez l'autre participant créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **PasserelleFichierTP1**.
   b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file:///Data/TP1/filegateway**
   d. Cliquez sur **Enregistrer**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du participant.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4.
8. Cliquez sur **Enregistrer**.

Configuration des capacités B2B

Activez les capacités B2B des deux participants de cet échange. Dans cet exemple, le document XML est émis par le Gestionnaire de communauté et sera transmis au participant.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du participant source de cet exemple (**GestCom**).
3. Cliquez sur **Capacités B2B**.
4. Activez trois ensembles de capacités pour le participant source.
   a. Activez la définition de flot de documents représentant le document XML :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : Aucun** pour l'activer.
      2) Développez **Regroupement : Aucun**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : FVT-XML-TEST (TOUT)**.
      4) Développez **Protocole : FVT-XML-TEST (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : ICGCPO (TOUT)**.

b. Ensuite, activez la définition de flot de documents représentant le document transformé :
   1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
   2) Développez **Regroupement : N/A**.
   3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : MX12V3R1 (TOUT)**.
   4) Développez **Protocole : MX12V3R1 (TOUT)**.
   5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : 850**.

c. Ensuite, activez la définition de flot de documents représentant l'enveloppe EDI :
   1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
   2) Développez **Regroupement : N/A**.
   3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
   4) Développez **Protocole EDI-X12 (TOUT)**.
   5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : ISA (TOUT)**.

5. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du participant cible de cet exemple (**TP1**).
7. Cliquez sur **Capacités B2B**.
8. Activez deux ensembles de capacités pour le participant cible.
   a. Tout d'abord, activez la définition de flot de documents représentant la transaction EDI 850 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : MX12V3R1 (TOUT)**.
      4) Développez **Protocole : MX12V3R1 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents : 850 (TOUT)**.

   b. Ensuite, activez la définition de flot de documents :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
      2) Développez **Regroupement : Aucun**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole : EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents :ISA (TOUT)**.

Création du profil d'enveloppe

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: **U**
   - ISA12: **00301**
   - ISA15: **T**
7. Cliquez sur **Enregistrer**.

Création du format XML

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 **Code 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 Flot de documents source, sélectionnez **Constante** et tapez **ICGCPO**.
9. Dans Version du flot de documents source, sélectionnez **Constante** et tapez **TOUT**.
10. Cliquez sur **Enregistrer**.

Activation des connexions

Activez les connexions du participant :

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
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 30. Connexion de transaction de document XML vers EDI

Source	Cible
Regroupement : Aucun (N/A) Protocole : FVT-XML-TEST (TOUT) Flot de documents : ICGCPO (TOUT)	Regroupement : N/A (N/A) Protocole : MX12V3R1 (TOUT) Flot de documents : 850 (TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente l'enveloppe EDI :

Tableau 31. Connexion de l'enveloppe EDI

Source	Cible
Regroupement : N/A (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)	Regroupement : Aucun (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)

Configuration des attributs

Configurez les attributs Capacités B2B du participant cible (TP1) et du participant source (Gestionnaire) :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur **Afficher les détails** en regard de **TPI** pour le sélectionner.
3. Cliquez sur **Capacités B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Regroupement : 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 **Enregistrer**.
8. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
9. Cliquez sur Afficher les détails en regard de **Gestionnaire** pour le sélectionner.
10. Cliquez sur **Capacités B2B**.
11. Cliquez sur l'icône **Développer** en regard de **Regroupement : 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 **Enregistrer**.

A ce stade, si le participant source (le Gestionnaire de communauté) a envoyé un document XML au participant, ce document sera transformé (au niveau du concentrateur) en transaction EDI, puis envoyé à la passerelle du participant.

Exemple ROD vers EDI

Cette section fournit un exemple d'envoi de document XML par le Gestionnaire de communauté au concentrateur, qui le transforme en transaction EDI enveloppée dans un EDI et l'envoie au participant.

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 participant. 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

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 flot de documents

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 flot de documents auxquelles cette mappe est associée s'affichent :

Tableau 32. Définitions de flot de documents associées à la mappe

Source	Cible
Regroupement : Aucun Protocole : ROD-TO-EDI_DICT (TOUT) Flot de documents : DTROD-TO-EDI_ROD (TOUT)	Regroupement : N/A Protocole : X12V5R1 (TOUT) Flot de documents : 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 de la cible

Cette section explique comment créer une cible de répertoire de système de fichiers pour le concentrateur :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Cibles** puis sur **Créer cible**.
2. Dans la zone Nom de la cible, entrez **CibleFichierROD**.
3. Dans la liste Transfert, 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 récupérateurs disponibles et cliquez sur **Ajouter** pour le déplacer dans la liste des récupérateurs configurés.
7. Sélectionnez **com.ibm.bcg.edi.receiver.preprocesshandler.RODSplitterHandler** dans la liste des récupérateurs configurés et cliquez sur **Configurer**.
8. Ajoutez les valeurs de la table ci-dessous :

Tableau 33. Attributs Récupérateur du processus de fractionnement ROD

Zone	Valeur
Nom du regroupement d'origine	Aucun
Version du regroupement d'origine	N/A
Nom du protocole d'origine	ROD-TO-EDI_DICT
Version du protocole d'origine	TOUT
Code processus De	DTROD-TO-EDI_ROD
Version processus De	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 Gestionnaire de communauté envoie le document ROD à cette cible.

Création des interactions

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 **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Développez **Regroupement : Aucun** et **Protocole : ROD-TO-EDI_DICT** puis sélectionnez **DTROD-TO-EDI_ROD**.
4. Développez **Regroupement : N/A** et **Protocole : X12V5R1** puis sélectionnez **Flot 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 **Enregistrer**.

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 **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur **Gestion des interactions**, puis sur **Création d'une interaction**.
3. Développez **Regroupement : N/A** et **Protocole : EDI-X12** puis sélectionnez **Flot de documents : ISA**.
4. Développez **Regroupement : Aucun** et **Protocole : EDI-X12** puis sélectionnez **Flot 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 **Enregistrer**.

Création des participants

Dans cet exemple, vous avez deux participants : le Gestionnaire de communauté (Gestionnaire) et un participant (TP1).

Créez le profil du Gestionnaire de communauté :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez : **GestionnaireCom**
3. Pour Nom affiché du participant, tapez **Gestionnaire**
4. Pour Type de participant, sélectionnez **Gestionnaire de communauté**.
5. Cliquez sur **Nouveau** pour ID métier 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 métier et tapez `01-000000000` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Créez le second participant :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Créer**.
2. Pour Nom de connexion de l'entreprise, tapez **TP1**
3. Pour Nom affiché du participant, tapez **TP1**
4. Pour Type de participant, sélectionnez **Participant de communauté**.
5. Cliquez sur **Nouveau** pour ID métier 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 métier et tapez `01-000000001` pour ID de forme libre.
7. Cliquez sur **Enregistrer**.

Création des passerelles

Créez des passerelles fichier-répertoire pour tous les participants de l'exemple. Créez d'abord une passerelle pour le Gestionnaire :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** en regard du Profil du gestionnaire.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister sur le système de fichiers.
   a. Dans Nom, tapez **PasserelleFichierGestionnaire**.
   b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file:///Data/Manager/filegateway**
   d. Cliquez sur **Enregistrer**.
5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du Gestionnaire de communauté.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4.
8. Cliquez sur **Enregistrer**.

Ensuite, créez une passerelle pour le participant.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Sélectionnez l'autre participant créé pour cet exemple, en cliquant sur l'icône **Afficher les détails** en regard de **TP1**.
3. Cliquez sur **Passerelles** puis sur **Créer**.
4. Entrez les valeurs suivantes pour la passerelle. Rappelez-vous que le répertoire de fichiers (le chemin entier) doit déjà exister.
   a. Dans Nom, tapez **PasserelleFichierTP1**.
   b. Dans la liste Transfert, sélectionnez **Répertoire de fichiers**.
   c. Dans Adresse, tapez : **file:///Data/TP1/filegateway**

d. Cliquez sur **Enregistrer**.

5. Cliquez sur **Liste** pour afficher la liste de toutes les passerelles du participant.
6. Cliquez sur **Afficher les passerelles par défaut**.
7. Dans la liste **Production**, sélectionnez la passerelle créée à l'étape 4, à la page 234.
8. Cliquez sur **Enregistrer**.

Configuration des capacités B2B

Activez les capacités B2B des deux participants de cet échange. Dans cet exemple, le document ROD est émis par le Gestionnaire de communauté et sera transmis au participant.

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Cliquez sur l'icône **Afficher les détails** du participant source de cet exemple (**Gestionnaire**).
3. Cliquez sur **Capacités B2B**.
4. Activez deux ensembles de capacités pour le participant source.
   a. Tout d'abord, activez la définition de flot de documents représentant le document ROD :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : Aucun** pour l'activer.
      2) Développez **Regroupement : Aucun**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : ROD-TO-EDI_DICT (TOUT)**.
      4) Développez **Protocole : ROD-TO-EDI_DICT (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : DTROD-TO-EDI_ROD (TOUT)**.
   b. Ensuite, activez la définition de flot de documents représentant l'enveloppe EDI :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir source** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.
      3) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Protocole : EDI-X12 (TOUT)**.
      4) Développez **Protocole EDI-X12 (TOUT)**.
      5) Cliquez sur l'icône **Role inactif** sous **Définir source** pour **Flot de documents : ISA (TOUT)**.
5. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
6. Cliquez sur l'icône **Afficher les détails** du participant cible de cet exemple (**TP1**).
7. Cliquez sur **Capacités B2B**.
8. Activez deux ensembles de capacités pour le participant cible.
   a. Tout d'abord, activez la définition de flot de documents représentant la transaction EDI 850 :
      1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : N/A**, afin de l'activer.
      2) Développez **Regroupement : N/A**.

3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : X12V5R1 (TOUT)**.
4) Développez **Protocole X12V5R1 (TOUT)**.
5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents : 850 (TOUT)**.

b. Ensuite, activez la définition de flot de documents représentant l'enveloppe EDI :
1) Cliquez sur l'icône **Rôle inactif** sous **Définir cible** pour **Regroupement : Aucun** pour l'activer.
2) Développez **Regroupement : Aucun**.
3) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Protocole : EDI-X12 (TOUT)**.
4) Développez **Protocole : EDI-X12 (TOUT)**.
5) Cliquez sur l'icône **Role inactif** sous **Définir cible** pour **Flot de documents :ISA (TOUT)**.

Création du profil d'enveloppe

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 **Enregistrer**.

Activation des connexions

Pour activer les connexions :

1. Cliquez sur **Administrateur du compte > Connexions du participant**.
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 34. Connexion ROD vers EDI

Source	Cible
Regroupement : N/A (N/A) Protocole : ROD-TO-EDI_DICT (TOUT) Flot de documents : DTROD-TO-EDI_ROD (TOUT)	Regroupement : Aucun (N/A) Protocole : X12V5R1 (TOUT) Flot de documents : 850 (TOUT)

6. Cliquez sur **Activation** pour la connexion qui représente l'enveloppe :

Tableau 35. Connexion de l'enveloppe

Source	Cible
Regroupement : Aucun (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)	Regroupement : N/A (N/A) Protocole : EDI-X12 (TOUT) Flot de documents : ISA (TOUT)

Configuration des attributs

Pour préciser les attributs du profil de l'enveloppe :

1. Cliquez sur **Administrateur de compte > Profils > Participant de communauté** puis sur **Rechercher**.
2. Sélectionnez **TP1** dans la liste.
3. Cliquez sur **Capacités B2B**.
4. Cliquez sur l'icône **Développer** en regard de **Regroupement : 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 **Enregistrer**.

A ce stade, si le Gestionnaire de communauté envoie un document ROD au concentrateur, le document sera transformé en transaction 850, qui sera ensuite enveloppée et envoyée à la passerelle du participant.

Annexe C. Informations complémentaires sur RosettaNet

La présente annexe apporte des informations complémentaires sur la prise en charge RosettaNet. Elle contient les rubriques suivantes :

Désactivation des PIP

Une fois qu'un regroupement 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 participants, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Développez l'arborescence des définitions de flot de documents pour accéder au flot de documents du PIP que vous souhaitez désactiver.
3. Dans la colonne Etat du regroupement, cliquez sur **Activé**. La colonne Etat affiche maintenant **Désactivé**, et WebSphere Partner Gateway ne peut pas utiliser la définition de flot de documents pour le PIP.

Pour désactiver une communication PIP avec un participant donné, désactivez la connexion au participant défini pour le processus PIP.

Notification d'échec

Cette section apporte des informations sur la notification d'échec.

PIP 0A1

Si un échec se produit au cours du traitement d'un message PIP, WebSphere Partner Gateway utilise le processus PIP 0A1 pour signaler l'échec au participant 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 participant. 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 participant. Le processus PIP 0A1 identifie la condition d'exception afin de permettre au participant de compenser l'échec du processus PIP 3A4.

Pour assurer la notification d'échec, téléchargez un regroupement 0A1 et servez-vous en pour créer une connexion PIP au participant.

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

Pour la prise en charge de RosettaNet, une définition de flot de documents de type action possède un jeu particulier d'attributs. 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 regroupements 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 flot de documents d'action, procédez comme suit :

1. Cliquez sur **Administrateur du concentrateur > Configuration du concentrateur > Définition du flot de documents**.
2. Cliquez sur les icônes **Développer** pour développer un noeud jusqu'au niveau de définition du flot de documents 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 RosettaNets**. 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 36. 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 participant ou système dorsal qui envoie le message
Vers le service	Contient le nom du service de composant réseau du participant ou système dorsal qui reçoit le message
A partir du rôle	Contient le nom de rôle du participant ou système dorsal qui envoie le message

Tableau 36. Attributs RosettaNet (suite)

Attribut RosettaNet	Description
Vers le rôle	Contient le nom de rôle du participant ou système dorsal qui reçoit le message
Code 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 flot de documents.
6. Cliquez sur **Sauvegarder**.

Création de regroupements de flot de documents PIP

RosettaNet ajoutant des processus PIP de temps en temps, il peut s'avérer nécessaire de créer vos propres regroupements 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 regroupement de flot de documents PIP pour PIP 5C4 V01.03.00. WebSphere Partner Gateway fournit un regroupement de flot 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 regroupement de flot de documents PIP est la même 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 regroupement de flot de documents PIP comprend les procédures suivantes :

- Création des fichiers XSD
- Création du fichier XML

- Création des regroupements

Création de fichiers XSD

Un regroupement de flot 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 252.

Pour créer les fichiers XSD pour le regroupement de flot 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 **Finish**.
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 regroupement de flot de documents PIP basé sur une autre version du regroupement 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 regroupement de flot 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 regroupement de flot 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 regroupement de flot 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"
```

Le 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

Le 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 regroupement de flot de documents PIP sur la base d'une autre version du regroupement 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 regroupement de flot 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 regroupement de flot 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 regroupement de flot 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"
```

Le 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

Le figure 38, à la page 247 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 regroupement de flot de documents PIP sur la base d'une autre version du regroupement 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 regroupement de flot de documents PIP de la version que vous remplacez. 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 regroupement de flot 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 regroupement de flot 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"
```

Le 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

Le 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

Après avoir créé les fichiers XSD pour votre regroupement de flot de documents PIP, vous pouvez créer le fichier XML du regroupement RNIF et le fichier XML du regroupement d'intégration dorsale. Par exemple, ces regroupements 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 regroupement RNIF :

1. Extrayez le fichier XML d'un fichier de regroupement de flot de documents PIP RNIF. Si vous effectuez une mise à niveau, extrayez le fichier de la version précédente du regroupement (par exemple, BCG_Package_RNIFV02.00_5C4V01.02.zip). Si vous créez un nouveau regroupement, extrayez le fichier à partir d'un regroupement de flot de documents PIP semblable à celui que vous créez. Par exemple, si vous créez un regroupement pour prendre en charge un processus PIP à deux actions, copiez le fichier XML à partir d'un autre regroupement 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 37. 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/A	N/A
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/A	N/A
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/A	N/A

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 38. Informations de mise à jour PIP 5C4 à partir de la spécification PIP

Informations à mettre à jour	Description	Valeur dans le regroupement 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/A

5. Mettez à jour les valeurs d'attribut du regroupement. 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 regroupement d'intégration dorsale, passez directement à l'étape 6, à la page 251.

Tableau 39. Mises à jour d'attributs PIP 5C4

Informations à mettre à jour	Description	Valeur dans le regroupement 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 (son ATTRIBUTEKEY est NonRepudiationRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
NonRepudiationOf Receipt	Spécifié au tableau 3-3	N	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (son ATTRIBUTEKEY est NonRepudiationOfReceipt) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY
DigitalSignature Required	Spécifié au tableau 5-1	O	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (son ATTRIBUTEKEY est DigitalSignatureRequired) ns1:AttributeValue AttributePickListItem ATTRVALUEKEY

Tableau 39. Mises à jour d'attributs PIP 5C4 (suite)

Informations à mettre à jour	Description	Valeur dans le regroupement 5C4	Chemin d'accès à l'élément dans le fichier XML
TimeToAcknowledge	Spécifié au tableau 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (son ATTRIBUTEKEY est TimeToAcknowledge) ns1:AttributeValue ATTRVALUE
TimeToPerform	Spécifié au tableau 3-3	2 (120 min)	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (son ATTRIBUTEKEY est TimeToPerform) ns1:AttributeValue ATTRVALUE
RetryCount	Spécifié au tableau 3-3	3	ns1:Package ns1:Protocol ns1:Process ns1:Attribute (son ATTRIBUTEKEY est 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 regroupement d'intégration dorsale, répétez les étapes 1 à 6 avec les différences suivantes :

- A l'étape 1, à la page 249, extrayez le fichier XML à partir du regroupement d'intégration dorsale (par exemple BCG_Package_RNSC1.0_RNIFV02.00_5C4V01.02.zip).
- N'effectuez pas l'étape 5, à la page 250.

Après avoir créé les fichiers XML et XSD, vous pouvez créer les regroupements de flot de documentation PIP.

Création du regroupement

Pour créer un regroupement RNIF, procédez comme suit :

1. Créez un répertoire GuidelineMaps et copiez-y les fichiers XSD du regroupement.
2. Créez un répertoire Packages et copiez-y le fichier XML RNIF.
3. Allez dans le répertoire parent et créez un regroupement de flot de documents PIP (fichier ZIP) contenant les répertoires GuidelineMaps et Packages. Vous devez conserver l'arborescence des répertoires dans le fichier ZIP.

Pour créer un regroupement d'intégration dorsale, suivez les étapes 1 à 3, mais utilisez le fichier XML d'intégration dorsale au lieu du fichier RNIF.

Après avoir créé le regroupement PIP, vous pouvez le télécharger en suivant la procédure de la section «Regroupements de flot de documents RNIF et PIP», à la page 69.

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 regroupement de flot 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 regroupements de flot de documents PIP», à la page 241 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 regroupement de flot 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″.

Contenu du regroupement de flot de documents PIP

Les sections suivantes décrivent les regroupements de flot de documents PIP fournis par WebSphere Partner Gateway pour chaque PIP. Chaque regroupement contient un fichier XML inclus dans un répertoire Packages et plusieurs fichiers XSD dans un répertoire GuidelineMaps, qui sont communs à tous les regroupements de flot 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 regroupement

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 40. 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 regroupement

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 41. 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 regroupement

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 42. 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 regroupement

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 43. 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
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 regroupement

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 44. 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 regroupement

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 45. 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

Tableau 45. Fichiers ZIP et XML de 3A2 Request Price and Availability (suite)

Nom du fichier ZIP	Nom du fichier 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 regroupement

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 46. 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 regroupement

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 47. 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
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 regroupement

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 48. 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 regroupement

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 49. 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 regroupement

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 50. 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 regroupement

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 51. 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 regroupement

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 52. 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 regroupement

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 53. 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 regroupement

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 54. 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 regroupement

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 55. 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 regroupement

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 56. 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

Tableau 56. Fichiers ZIP et XML de 3B11 Notify of Shipping Order (suite)

Nom du fichier ZIP	Nom du fichier 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 regroupement

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 57. 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 regroupement

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 58. 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 regroupement

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 59. 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

Tableau 59. Fichiers ZIP et XML du PIP 3B14 Request Shipping Order Cancellation (suite)

Nom du fichier ZIP	Nom du fichier 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 regroupement

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 60. 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 regroupement

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 61. 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
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 regroupement

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 62. 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 regroupement

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 63. 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 regroupement

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 64. 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 regroupement

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 65. 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

Tableau 65. Fichiers ZIP et XML de 3C7 Notify of Self-Billing Invoice (suite)

Nom du fichier ZIP	Nom du fichier 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 regroupement

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 66. 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

Tableau 66. Fichiers ZIP et XML de 3D8 Distribute Work in Process (suite)

Nom du fichier ZIP	Nom du fichier 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 regroupement

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 67. 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 regroupement

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 68. 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 regroupement

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 69. 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
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 regroupement

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 70. 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 regroupement

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 71. 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 regroupement

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 72. 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

Tableau 72. Fichiers ZIP et XML de 4B3 Notify of Consumption (suite)

Nom du fichier ZIP	Nom du fichier 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 regroupement

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 73. 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 regroupement

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 74. 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 regroupement

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 75. 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 regroupement

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 76. 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 regroupement

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 77. 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 regroupement

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 78. 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 regroupement

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 79. 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 regroupement

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 80. 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 regroupement

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 81. 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 regroupement

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 82. 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 regroupement

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 83. 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

Annexe D. Attributs

Cette annexe décrit les attributs que vous pouvez définir depuis la Console de communauté. Il concerne les attributs suivants :

Attributs d'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 84 dresse la liste des attributs généraux pour lesquels des valeurs par défaut sont fournies.

Tableau 84. Attributs généraux

Nom de la zone	Obligatoire ?	Description	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

Tableau 84. Attributs généraux (suite)

Nom de la zone	Obligatoire ?	Description	par défaut
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.	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.

Attributs des groupes : Le tableau 85 indique les attributs de groupe pour lesquels des valeurs par défaut sont fournies.

Tableau 85. Attributs des groupes

Nom de la zone	Obligatoire ?	Description	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 UCS

Cette section indique si les valeurs par défaut s'appliquent à un groupe, une transaction ou un EDI UCS.

Attributs généraux : Le tableau 86 indique les attributs généraux pour lesquels des valeurs par défaut sont fournies.

Tableau 86. Attributs généraux

Nom de la zone	Obligatoire ?	Description	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

Tableau 86. Attributs généraux (suite)

Nom de la zone	Obligatoire ?	Description	par défaut
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 87 indique les attributs de groupe pour lesquels des valeurs par défaut sont fournies.

Tableau 87. Attributs des groupes

Nom de la zone	Obligatoire ?	Description	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 88, à la page 298 indique les attributs généraux pour lesquels des valeurs par défaut sont fournies.

Tableau 88. Attributs généraux

Nom de la zone	Obligatoire ?	Description	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
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 89 indique les attributs de groupe pour lesquels des valeurs par défaut sont fournies.

Tableau 89. Attributs des groupes

Nom de la zone	Obligatoire ?	Description	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 90 indique les attributs de messages pour lesquels des valeurs par défaut sont fournies.

Tableau 90. Attributs de messages

Nom de la zone	Obligatoire ?	Description	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 flots de documents

Cette section décrit les attributs de définition de flot de documents 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 91 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 sépérateurs et délimiteurs sont indiqués dans le tableau 91.

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 91. Attributs de profil d'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)

Tableau 91. Attributs de profil d'enveloppe (suite)

Attribut	Terme X12	Terme EDIFACT	Description
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)
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 91, à la page 299.

Un message EDI est composé de plusieurs segments disposés dans un ordre particulier. Un 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 EDI

Cette section indique quels autres attributs d'EDI peuvent être définis au niveau de la définition du flot de documents ou de la connexion.

Tableau 92. Autres attributs d'EDI

Attribut	Obligatoire	Description	Restrictions	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.	Limité au protocole ou à la connexion	Oui

Tableau 92. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	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 d'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 92. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	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 92. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	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 92. Autres attributs d'EDI (suite)

Attribut	Obligatoire	Description	Restrictions	par défaut
Supprimer une erreur	Non	Cet attribut est utilisé dans le traitement polymorphique. 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 d'utilisation 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 réceptionnaire 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 réceptionnaire d'application de groupe	Non	Le code qui sert à identifier le format de l'identificateur du réceptionnaire d'application de groupe.		
Mot de passe d'application de groupe	Non	Cet attribut définit les informations de sécurité.		

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 93. 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 94 répertorie d'autres propriétés du client Data Interchange Services et les attributs WebSphere Partner Gateway qui leur sont associés.

Tableau 94. 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 réceptionnaire de l'EDI
IchgRcvrId	ID du réceptionnaire de l'EDI
IchgDate	Date de l'EDI
IchgTime	Heure de l'EDI
IchgPswd	Mot de passe de l'EDI
IchgUsgInd	Indicateur d'utilisation EDI
IchgAppRef	Référence de l'application EDI.
IchgVerRel	Version et édition de l'EDI.

Tableau 94. Propriétés de client Data Interchange Services et attributs associés (suite)

Propriété du client Data Interchange Services	Supplante l'attribut WebSphere Partner Gateway
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 réceptionnaire 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 95. Attributs AS

Attribut	Obligatoire	Description	Restrictions	par défaut
Heure d'accuser réception	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 un MDN n'est pas reçu. Cet attribut est associé à l'attribut Heure d'accuser 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
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

Tableau 95. Attributs AS (suite)

Attribut	Obligatoire	Description	Restrictions	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
Chiffrement AS	Non	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 AS 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 valides sont Oui et Non. **Oui** Le chiffrement est obligatoire. **Non** Le chiffrement n'est pas obligatoire.	Limité au protocole ou à la connexion	Non
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 un MDN. **Non** Un MDN n'est pas obligatoire.	Limité au protocole ou à la connexion	Oui
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 un 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". Uniquement pour AS1, cet attribut est utilisé en association avec l'attribut AS MDN asynchrone, dans le format mailto:xxx@company.com.	Limité au protocole ou à la connexion	

Tableau 95. Attributs AS (suite)

Attribut	Obligatoire	Description	Restrictions	par défaut
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 un MDN asynchrone. Cet attribut est utilisé en association avec l'attribut AS MDN asynchrone.	Limité au protocole ou à la connexion	
AS MDN asynchrone	Non	Indique si le MDN doit être retourné 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 signé	Non	Indique si la demande exige le retour d'un MDN signé. 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** Un MDN signé est exigé **Non** Un MDN signé n'est pas exigé Si cet attribut est défini sur Oui, le MDN envoyé par le partenaire doit être signé. Si cet attribut est défini sur Non, le MDN peut être signé ou non.	Limité au protocole ou à la connexion	Non
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 signés, la valeur sert à renseigner l'en-tête "Disposition-notification-options: signed-receipt-micalg".	Limité au protocole ou à la connexion	sha1

Tableau 95. Attributs AS (suite)

Attribut	Obligatoire	Description	Restrictions	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
ID métier de l'AS	Non	L'ID métier de l'AS à utiliser dans l'en-tête "AS2-To". En l'absence de valeur, WebSphere Partner Gateway utilise l'ID métier du réceptionnaire qui a servi dans le document source. **Remarque :** L'en-tête "AS2-From" sera renseigné à partir du document source original qui est arrivé dans WebSphere Partner Gateway et qui est en cours d'envoi en tant qu'AS.	Limité au protocole ou à la connexion	

Attributs RosettaNet

Cette section apporte des informations sur les attributs RosettaNet.

Tableau 96. Attributs RosettaNet

Attribut	Obligatoire	Description	Restrictions	par défaut
Heure d'accuser 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 96. Attributs RosettaNet (suite)

Attribut	Obligatoire	Description	Restrictions	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'accuser 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 le document original 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
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.	
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 qui identifie la chaîne d'approvisionnement pour la fonction du participant. Les valeurs possibles sont : • Composants électroniques • Technologie d'informations • Technologie de semiconducteurs	Limité au protocole ou à la connexion	

Tableau 96. Attributs RosettaNet (suite)

Attribut	Obligatoire	Description	Restrictions	par défaut
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 s'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 possibles sont : **Aucun** Le chiffrement n'est pas obligatoire. **Données utile** 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.	Aucun

Attribut Intégration dorsale

Cette section apporte des informations sur l'attribut associé au regroupement d'Intégration dorsale.

Tableau 97. Attribut Intégration dorsale

Attribut	Description	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

Annexe E. 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 ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense CEDEX
France

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

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. IBM DECLINE TOUTE RESPONSABILITE, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE VALEUR MARCHANDE OU D'ADAPTATION A VOS BESOINS. 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. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis 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
U.S.A

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.

Ces informations peuvent 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. Ces noms sont fictifs et toute ressemblance avec des noms ou adresses de personnes ou de sociétés réelles serait purement fortuite.

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.

LICENCE SUR LES DROITS D'AUTEUR

Le présent document peut contenir 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.

WebSphere Partner Gateway comprend du code nommé ICU4J dont la licence vous a été fournie par IBM conformément aux dispositions des Conditions internationales d'utilisation des logiciels IBM, soumises aux dispositions relatives aux Composants exclus. Toutefois, IBM est tenu de vous informer des remarques suivantes :

COPYRIGHT ET AUTORISATION

Copyright (c) 1995-2003 International Business Machines Corporation and others

All rights reserved.

Il est ainsi autorisé, gratuitement, à toute personne recevant une copie de ce logiciel ainsi que les fichiers de documentation qui s'y rapportent, d'utiliser ce dernier sans restriction, ni limitation de droits d'utilisation du logiciel, de copier, de modifier, de fusionner, de publier, de distribuer et/ou de vendre des copies du logiciel et d'autoriser les personnes à qui ce logiciel est remis d'en faire autant, à condition que les remarques concernant le copyright et la remarque concernant l'autorisation apparaissent sur toutes les copies du logiciel et sur la documentation qui s'y rapporte.

CE LOGICIEL EST FOURNI "EN L'ETAT", SANS GARANTIE D'AUCUNE SORTE, EXPLICITE OU IMPLICITE, Y COMPRIS, ENTRE AUTRE, DES GARANTIES DE VALEUR MARCHANDE, DE COMPATIBILITE POUR UNE UTILISATION PARTICULIERE ET LE RESPECT DES DROITS APPLICABLES AUX FOURNISSEURS TIERS. EN AUCUN CAS, LE OU LES DETENTEURS DU COPYRIGHT INCLUS DANS CETTE REMARQUE NE SONT EN DROIT D'EMETTRE AUCUNE RECLAMATION CONCERNANT DES DOMMAGES INDIRECTS, PROVOQUANT LA PERTE D'INFORMATIONS OU DE PROFITS, QUE CE SOIT DANS LE CADRE D'UNE DELEGATION, D'UNE NEGLIGENCE OU D'UNE ERREUR DE TRAITEMENT, LIES A L'UTILISATION OU LA MANIPULATION DE CE LOGICIEL.

A l'exception de ce qui est mentionné dans cette remarque, le nom d'un détenteur de copyright ne doit jamais être utilisé dans un contexte publicitaire ou de promotion de vente, d'utilisation ou autres objets liés à ce logiciel sans autorisation écrite préalable du détenteur du copyright.

Informations sur l'interface de programmation

Les informations sur l'interface de programmation ont pour objectif de vous aider à créer des logiciels d'application utilisant ce programme. Les interfaces de programmation génériques vous permettent de créer des logiciels d'application qui obtiennent les services des outils de ce programme. Cependant, ces informations peuvent également contenir des informations sur le diagnostic, la modification et le réglage. Les informations sur le diagnostic, la modification et le réglage vous permettent de déboguer vos logiciels d'application.

Avertissement : N'utilisez pas ces informations sur le diagnostic, la modification et le réglage comme interface de programmation car elles sont susceptibles de changer.

Marques 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 :

i5/OS
IBM
Le logo IBM
AIX
CICS
CrossWorlds
DB2
DB2 Universal Database
Domino
IMS
Informix
iSeries
Lotus
Lotus Notes
MQIntegrator
MQSeries
MVS
OS/400
Passport Advantage
SupportPac
WebSphere
z/OS

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'Intel Corporation aux Etats-Unis et/ou dans certains autres pays.

Java et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains 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 et Advanced Edition inclut un logiciel développé par le projet Eclipse (www.eclipse.org).

IBM WebSphere Partner Gateway Enterprise et Advanced Editions, version 6.0.

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