IBM WebSphere Partner Gateway Enterprise et Advanced Editions

Guide du Partenaire

Version 6.1.1

IBM WebSphere Partner Gateway Enterprise et Advanced Editions

Guide du Partenaire

Version 6.1.1

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 107.

Première édition - mars 2008

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Information produit

IBM WebSphere Partner Gateway est un système de traitement de document électronique servant à gérer une communauté d'échange B2B (business-to-business). Le B2B a évolué ces dernières années afin de permettre l'exécution de nombreux types de transactions commerciales automatiques (par exemple, les bons de commande et les factures) de manière rapide, pratique et économique.

Ce guide fournit aux partenaires de la communauté toutes les informations dont ils ont besoin pour configurer la console et exécuter les tâches quotidiennes.

Public concerné

Les parties impliquées dans une transaction ou une communauté de concentrateur IBM WebSphere Partner Gateway sont le partenaire interne, l'administrateur du concentrateur et les partenaires externes. Chacune de ces parties est composée d'utilisateurs administratifs disposant de différents niveaux de privilèges. Ces utilisateurs administratifs ajouteront des utilisateurs réguliers disposant de privilèges d'accès à la console spécifiques.

Conventions typographiques

Ce document utilise les conventions typographiques suivantes :

Convention	Description
`Police monospace`	Le texte dans cette police indique qu'il s'agit de texte que vous tapez, de valeurs pour des arguments ou des options de commande, d'exemples et d'exemples de code ou d'informations que le système imprime à l'écran (texte de message ou invite).
Gras	Le texte en gras correspond aux commandes de l'interface graphique (par exemple, les noms des boutons en ligne, les noms ou les options de menu) et aux en-têtes de colonne dans des tables et du texte.
Italique	Le texte en italique correspond aux emphases, aux titres de manuels, à de nouveaux termes et aux termes définis dans le texte, aux noms de variables ou aux lettres de l'alphabet utilisées comme lettres.
`Police monospace en italique`	Le texte en police monospace italique correspond aux noms de variables dans du texte en police monospace.
Texte en couleur souligné	Le texte en couleur souligné indique une référence croisée. Cliquez sur le texte pour naviguer jusqu'à l'objet de la référence.
Texte avec contour bleu	(Dans les fichiers PDF uniquement) Un texte encadré de bleu indique une référence croisée. Cliquez sur le texte avec contour pour atteindre l'objet de référence. Cette convention est l'équivalent de celle des fichiers PDF ("Texte en couleur souligné") mentionnée dans ce tableau.
{INSTALL DIR}	Représente le répertoire dans lequel le produit est installé.
UNIX: / Windows:	Les paragraphes commençant par l'un de ces éléments signalent des remarques présentant des différences entre systèmes d'exploitation.

“ “ (guillemets)	(Dans les fichiers PDF uniquement) Les guillemets entourent les références croisées aux autres sections du document.
{ }	Dans une ligne de syntaxe, les accolades encadrent un jeu d’options parmi lesquelles vous pouvez en choisir une seule.
[ ]	Dans une ligne de syntaxe, les crochets entourent des paramètres facultatifs.
...	Dans une ligne de syntaxe, les points de suspension indiquent une répétition du paramètre précédent. Par exemple, `option[,...]` signifie que vous pouvez entrer plusieurs options séparées par des virgules.
< >	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.
\, /	Sous Windows, les barres obliques inversées (\) sont utilisées pour séparer les composants dans les chemins d’accès aux répertoires. Pour les installations UNIX, remplacez les barres obliques inverses par des barres obliques standard (/).

Documents associés

L’ensemble de la documentation disponible pour ce produit comprend des informations exhaustives sur l’installation, la configuration, l’administration et l’utilisation de WebSphere Partner Gateway Enterprise Edition et WebSphere Partner Gateway Advanced Edition.

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

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

Remarque : Des informations importantes concernant ce produit sont disponibles dans les notes Technical Support Technotes and Flashes publiées postérieurement à ce document. Vous trouverez ces informations sur le site Web de support de WebSphere Partner Gateway à l’adresse suivante :

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

Sélectionnez le domaine de composant qui vous intéresse et parcourez la section Technotes and Flashes.

Nouveautés de cette version

Cette section décrit les nouvelles fonctionnalités d'IBM WebSphere Partner Gateway.

Nouveautés de l'édition 6.1.1

WebSphere Partner Gateway V6.1.1 prend en charge les nouvelles fonctions suivantes :

- Dans les versions précédentes, la prise en charge de l'authentification standard était uniquement disponible pour les messages de services Web. Cette fonction a été étendue à tous les protocoles. Il est conseillé d'utiliser une connexion sécurisée HTTP, soit HTTPS et non HTTP.
- Prise en charge de la compression et de la décompression de données fournie pour les messages RNIF, à l'exception de la signature et du chiffrement.
- Prise en charge de la validation des éléments SOAP Body et SOAP Envelope. Par ailleurs, il est possible de désenvelopper un élément SOAP Envelope.
- Le délai d'attente maximum synchrone et les connexions maximales synchrones peuvent être contrôlés localement pour chaque récepteur HTTP.
- Le serveur FTP est intégré à WebSphere Partner Gateway pour prendre en charge le protocole AS3, la destination FTP d'écriture de script, le récepteur FTP d'écriture de script, le récepteur et la destination FTP/FTPS.
- Un document en erreur peut être envoyé au partenaire à l'origine de l'échange, au partenaire récepteur ou aux deux. Le flux de document en erreur peut être configuré dans la console de WebSphere Partner Gateway et être envoyé au format de WebSphere Partner Gateway ou des services Web.
- Les performances de l'utilitaire de création d'archives ont été améliorées.
- La prise en charge de plusieurs partenaires internes est assurée.
- Il est désormais possible d'envoyer une nouvelle fois plusieurs documents entrants ou sortants simultanément.
- La prise en charge du mode FIPS est offerte. Possibilité de configurer le produit pour l'exécuter en mode FIPS ou en mode par défaut.
- Fonctionnalités Supprimer et Emplacement d'utilisation fournies pour la destination, les mappes de validation, les définitions de document, les interactions et les utilisateurs.
- La prise en charge de la compression des fichiers volumineux est assurée pour les documents AS2 et AS3.
- La prise en charge du chiffrement et de la signature numérique est assurée.
- Les dépendances du type de configuration pour la migration comprennent également les codes événement et les notifications d'alertes. Aussi, la fonction de migration des partenaires a été enrichie pour permettre la prise en charge de l'importation/exportation des définitions d'événements donnant lieu à des alertes.
- La prise en charge du chargement de plusieurs certificats est assurée. Nouvel assistant inclus dans la console pour télécharger et configurer les certificats.
- Le produit prend désormais en charge AIX 6.1, RHEL (32 et 64 bits), SLES 10 (64 bits) et Windows Server 2003 64 bits.

Nouveautés de la version 6.1

WebSphere Partner Gateway V6.1 prend en charge les nouvelles fonctions suivantes :

- Nouveaux protocoles de gestion : AS3, SOAP avec pièces jointes, CIDX et prise en charge de ebMS (ebXML Message Service) 2.0
- Prise en charge améliorée des documents XML personnalisés : meilleure organisation, prise en charge complète des expressions XPath, zones de recherche, attributs définis par l'utilisateur et prise en charge synchronisée
- Prise en charge d'IPv6 et fonction améliorées de création de scripts FTP pour la prise en charge d'AS3
- Réorganisation des attributs de définition de document
- Nouveaux attributs de définition de document pour les exits utilisateur.
- Irréfutabilité configurable par type de document et par niveau de partenaire d'échanges
- L'afficheur de documents dispose de nouvelles zones de recherche définies par l'utilisateur.
- Prise en charge améliorée de l'afficheur AS avec états de retour MDN
- Assistant de configuration EDI et assistant d'importation EIF (auparavant fourni dans le pack de support GA02)
- Nouveau mode de notification d'alerte permettant d'envoyer des notifications à toutes les parties concernées (partenaires source et cible ou tous les contacts inscrits), ce qui réduit les opérations de configuration
- Fonction de renvoi et droits Gateway disponibles pour tous les utilisateurs (autres que l'administrateur du concentrateur)
- Nouveau groupe d'utilisateurs permettant à plusieurs utilisateurs d'assumer la fonction d'administrateur du concentrateur
- Prise en charge LDAP pour l'authentification d'ouverture de session
- Utilisation des fonctions de consignation et de traçage WebSphere Application Server pour les composants WebSphere Partner Gateway
- Les données de configuration du fichier de propriétés sont désormais stockées et gérées de manière centralisée par la console WebSphere Partner Gateway
- WebSphere MQ n'est plus obligatoire ; WebSphere Platform Messaging est utilisé pour les communications internes
- Archivage sélectif en fonction du type de document et/ou de partenaire
- Migration de la configuration WebSphere Partner Gateway en exportant et en important les définitions d'une instance WebSphere Partner Gateway à une autre
- Option d'installation simplifiée sur une seule machine (mode simple)
- WebSphere Application Server Network Deployment est désormais utilisé pour les déploiements sur plusieurs machines, ce qui permet la mise en cluster et une gestion centrale de l'infrastructure
- Prise en charge de l'utilisation de WebSphere Process Server Version 6.1 en tant que système d'intégration backend

Remarques :

1. L'API d'administration XML est dépréciée dans la version 6.1.
2. WebSphere Partner Gateway Version 6.1 ne prend pas en charge l'algorithme RC5.

Chapitre 1. Introduction

Communauté du concentrateur

La communauté de concentrateur d'IBM WebSphere Partner Gateway est composée des trois entités suivantes, connectées à un concentrateur central pour échanger en temps réel des documents de gestion : l'administrateur du concentrateur, le partenaire interne et les partenaires externes.

Administrateur du concentrateur

L'administrateur de concentrateur est une société responsable de la gestion des opérations quotidiennes de la communauté du concentrateur. Il gère l'infrastructure matérielle et logicielle de la communauté du concentrateur 24h/24 et 7j/7. Ses responsabilités comprennent :

- l'identification et la résolution des incidents ;
- la vérification de la configuration de la communauté de concentrateur pour tous les partenaires externes ;
- l'assistance à la configuration de nouveaux partenaires externes à la communauté de concentrateur et
- la planification stratégique de l'expansion future afin de s'assurer que la communauté de concentrateur fonctionne au maximum de ses capacités.

La fonction d'administrateur du concentrateur peut être déléguée à une tierce partie au sein de la communauté du concentrateur, ou accomplie par le partenaire interne ayant acheté WebSphere Partner Gateway.

Partenaire interne

Le partenaire interne est la principale société et le principal moteur de la communauté de concentrateur. Elle est responsable de l'achat et de la construction de la communauté de concentrateur, y compris de la définition des processus de commerce électronique échangés entre elle et les partenaires externes.

Le partenaire interne peut également choisir d'être administrateur du concentrateur.

Partenaires externes

Les partenaires externes sont les sociétés effectuant des transactions commerciales avec le partenaire interne via la communauté du concentrateur. Ils doivent accomplir un processus de configuration pour se connecter à la communauté de concentrateur. Une fois connectés, ils peuvent échanger des document de gestion électroniques avec le partenaire interne.

Icônes de la Console de communauté

Les icônes présentées dans le tableau ci-dessous sont spécifiques à la Console de communauté WebSphere Partner Gateway.

Tableau 1. Icônes de la console de la communauté

Icône	Nom de l'icône
	Réduire
	Copier
	Créer un rôle. Le rôle est inactif.
	Le dossier contient des données
	Activer
	Supprimer
	Afficher le document brut
	Document en cours de progression
	Le traitement du document a échoué
	Le traitement du document a abouti
	Télécharger une mappe
	Editer
	Edition des valeurs d'attribut
	Sortir de l'édition
	Edition des valeurs d'attribut RosettaNet
	Développer
	Exporter des informations
	Exporter l'état
	Destination désactivée
	Masquer les critères de recherche
	Modifier
	Le dossier ne contient pas de donnée
	Ouvrir l'agenda
	Activer / désactiver le classement des documents
	Pause

Tableau 1. Icônes de la console de la communauté (suite)

Icône	Nom de l'icône
	Imprimer
	Saisie requise
	Démarrer
	Arrêter le traitement ; le document est en cours, option utilisateur pour demander au serveur d'arrêter le traitement du document
	Flux de données synchrone ; aucune icône n'est affichée pour les transactions asynchrones
	Charger une mappe
	Afficher les caractéristiques
	Afficher la configuration de l'attribut de définition de document
	Afficher le système d'aide
	Afficher les membres
	Afficher le document d'origine
	Afficher les autorisations
	Afficher les appartenances au groupe
	Afficher les erreurs de validation
	Cas d'emploi

Utilisation de la Console de communauté

Après avoir configuré WebSphere Partner Gateway, vous utiliserez régulièrement deux outils de la console : l'Afficheur d'événements et l'Analyse du document.

Utilisez l'Afficheur d'événements, dans le module Afficheurs, pour rechercher des événements. La plupart des documents sont renvoyés plusieurs fois : si un document échoue et génère une alerte, vous devez donc examiner le problème et faire les corrections nécessaires pour éviter ce genre d'échecs à l'avenir.

Vous pouvez localiser un événement spécifique et en rechercher la cause. L'Afficheur d'événements vous permet de rechercher des événements par heure, date, type d'événement, nom d'événement et emplacement de l'événement. L'administrateur du concentrateur peut également effectuer une recherche par partenaire, par IP source et par IP événement.

Remarque : Les utilisateurs n'auront pas tous accès au Débogage des événements.

Les données générées par l'Afficheur d'événements aident à identifier l'événement et le document qui l'a créé. Vous pouvez également afficher le document de base, qui identifie la zone, la valeur et la cause de l'erreur.

Le deuxième outil le plus utilisé est la fonction Analyse du document du module Outils. Elles sert à rechercher le nombre de documents qui ont été reçus, de ceux en cours et de ceux terminés, ainsi que le nombre de documents qui ont échoué et de ceux qui ont abouti. Utilisez cet outil pour retrouver les documents spécifiques ayant échoué et pour comprendre la cause de cet échec.

Les modules de l'Administrateur du compte de la console sont principalement utilisés lors de la configuration de WebSphere Partner Gateway puis pour la maintenance.

Chapitre 2. Configuration de votre environnement WebSphere Partner Gateway

La présente section décrit les tâches que doivent effectuer les partenaires externes pour préparer WebSphere Partner Gateway pour les utilisateurs et l'environnement du partenaire externe.

Pour configurer WebSphere Partner Gateway pour votre entreprise, vous devez effectuer les opérations suivantes à partir de la Console de communauté dans l'ordre indiqué ci-dessous.

1. «Connexion à la Console de communauté»
2. «Vérification de votre profil partenaire», à la page 6
3. «Création d'une destination», à la page 7
4. «Examen des fonctions B2B», à la page 7
5. «Chargement de certificats numériques», à la page 9
6. «Création de groupes de console», à la page 29
7. «Création d'utilisateurs», à la page 30
8. «Configuration de l'utilisateur FTP», à la page 31
9. «Création des informations de contact», à la page 33
10. «Création d'alertes et ajout de contacts», à la page 34
11. «Création d'une adresse», à la page 40

Connexion à la Console de communauté

Cette section décrit la marche à suivre pour afficher la Console de communauté et s'y connecter. La résolution d'écran recommandée est de 1024 x 768.

Remarque : La Console de communauté de WebSphere Partner Gateway requiert l'activation des cookies pour permettre la conservation des informations de session. Aucune information personnelle n'est stockée dans le cookie ; en outre, ces informations sont effacées dès que le navigateur est fermé.

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

   http://<*nom_hôte*>.<*domaine*>:58080/console (non sécurisé)

   https://<*nom_hôte*>.<*domaine*>:58443/console (sécurisé)

   où <*nom_hôte*> et <*domaine*> correspondent au nom et à l'emplacement de l'ordinateur hébergeant le composant Console de communauté.

   Remarque : Ces URL partent du principe que les numéros de port par défaut sont utilisés. Si vous avez modifié les numéros de port par défaut, remplacez-les par les valeurs indiquées.

Dans la plupart des cas, votre administrateur de concentrateur vous a communiqué le nom d'utilisateur, le mot de passe initial et le nom de connexion de l'entreprise à utiliser pour vous connecter à la Console de communauté. Vous aurez besoin de ces informations pour la procédure qui suit. Si vous ne les avez pas reçues, contactez votre administrateur du concentrateur.

Pour se connecter à la Console de communauté (ces instructions s'adressent aux partenaires internes ainsi qu'aux partenaires externes) :

1. Saisissez le **Nom d'utilisateur** de votre entreprise.
2. Saisissez le **Mot de passe** de votre entreprise.
3. Saisissez le **Nom de connexion de l'entreprise**, par exemple, IBM.
4. Cliquez sur **Connexion**. A l'occasion de votre première connexion, vous devez créer un nouveau mot de passe.
5. Saisissez un nouveau mot de passe, puis saisissez-le une deuxième fois dans la zone de texte Vérifier.
6. Cliquez sur **Sauvegarder**. Le système affiche l'écran de saisie initial de la console.

Remarque : Si WebSphere Partner Gateway est configuré en utilisant le protocole LDAP, il vous faudra entrer le nom d'utilisateur et le mot de passe LDAP. Le nom de connexion de l'entreprise n'est pas pertinent dans ce cas de figure, c'est pourquoi vous ne serez pas invité à le saisir. Par ailleurs, le système ne vous invitera pas à modifier votre mot de passe.

Vérification de votre profil partenaire

Utilisez la fonction Administration du compte pour les partenaires pour afficher et éditer les informations identifiant votre entreprise dans le système.

Les partenaires peuvent éditer tous les attributs de leur profil, excepté le Nom de connexion de l'entreprise. Les partenaires peuvent également ajouter et supprimer des ID entreprise, ID de messagerie lié à tout ID entreprise, et des adresses IP. Les adresses IP ou les noms d'hôte peuvent être entrés pour les Modes de fonctionnement suivants : Production, Test, Gestionnaire CPS et Partenaire CPS.

Cette fonction propose également une option pour restaurer tous les mots de passe des utilisateurs. Vous pouvez utiliser cette fonction si vous pensez que les mots de passe des utilisateurs sont compromis.

Affichage et édition de votre profil partenaire

1. Cliquez sur **Administrateur du compte** > **Profils** > **Partenaire**.
2. Cliquez sur l'icône Mon profil pour modifier celui-ci. Le système affiche l'écran Caractéristiques du partenaire.
3. Editez votre profil si nécessaire (certaines valeurs ne peuvent pas être éditées). Pour l'explication des valeurs, voir le tableau 2, à la page 7.

Tableau 2. Valeurs sur les écrans Partenaires

Valeur	Description
Nom de connexion de l'entreprise	Identifie le partenaire dans le système. Quinze (15) caractères maximum. Ne peut comprendre les caractères spéciaux suivants : , . ! # ; : \ / & ?. Les partenaires ne peuvent pas éditer cette valeur.
Nom d'affichage du partenaire	Nom choisi par le partenaire pour le représenter vis-à-vis de la communauté de concentrateur. Trente (30) caractères maximum.
Type de partenaire	Type de partenaire - partenaire externe ou partenaire interne. Les partenaires peuvent éditer cette valeur uniquement si la propriété bcg.allow.partner.type.edit est définie sur True. Par défaut, cette propriété est définie sur False.
Etat	Activé ou Désactivé. S'il est désactivé, le partenaire n'est pas visible dans les critères de recherche et les listes déroulantes.
Type de fournisseur	Identifie le rôle du partenaire. Par exemple : Fabricant du contrat ou Grossiste.
Site Web	Identifie le site Web du partenaire.
ID entreprise	Numéro DUNS, DUNS+4 ou à format libre utilisé par le système pour l'acheminement. Vous pouvez ajouter des numéros ID entreprise supplémentaires. • Les numéros DUNS doivent comporter neuf chiffres. • Les numéros DUNS+4 doivent comporter treize chiffres. • Les numéros ID à format libre peuvent comporter jusqu'à 60 caractères alpha-numériques et spéciaux. **Remarque :** Les ID entreprise EDI doivent comporter un préfixe contenant n'importe quel qualificatif utilisé dans le document EDI. Le format est le suivant : qualificatif EDI plus ″-″ et l'ID. Par exemple, un EDI X12 utilisant un numéro DUNS serait 01-123456789.
ID de messagerie	ID de messagerie valide de chaque ID entreprise. Vous pouvez ajouter des ID de messagerie supplémentaires pour tous les ID entreprise. Cette zone n'est pas visible si aucun ID entreprise n'est renseigné.
Adresse IP ou nom hôte	• Mode de fonctionnement. Par exemple, Partenaire CPS. • Adresse IP ou nom d'hôte du partenaire.

4. Cliquez sur **Sauvegarder**.

Création d'une destination

Vous devez créer et gérer une destination par défaut. Si vous ne le faites pas, vous ne pourrez pas créer de connexions. Pour plus d'informations sur la création de destinations, voir Chapitre 3, «Création de destinations», à la page 43.

Examen des fonctions B2B

Remarque : Dans les petites installations, ce processus peut être exécuté par l'administrateur du concentrateur.

Utilisez cette fonction pour afficher et éditer toutes les fonctions B2B prédéfinies du concentrateur et pour activer des fonctions B2B locales supplémentaires, si nécessaire.

Une fonction B2B est un type spécifique de processus métier pouvant être échangé entre vous et d'autres membres de la communauté. Les fonctions B2B ou de

traitement de documents sont définies avec les définitions de types de type. Une définition de type de documents apporte au système toutes les informations nécessaires à la réception, au traitement et à l'acheminement de documents entre les membres de la communauté.

Chaque fonction comporte jusqu'à cinq définitions de type de document différentes :

Package. Il s'agit des formats d'empaquetage des documents utilisés pour leur transmission sur Internet. Par exemple, RNIF, AS1, AS2 et AS3.

Protocole. Identifie la structure et l'emplacement des informations dans le document. Le système a besoin de ces informations pour traiter et acheminer le document.

Type de document. Identifie le processus métier qui sera traité entre le partenaire interne et ses partenaires externes.

Activité. La fonction métier remplie par le processus.

Action. Les documents individuels composant un processus métier complet. Les documents sont traités entre le partenaire interne et le partenaire externe.

Chaque définition de type de document contient des attributs (c'est-à-dire des informations) qui définissent sa fonctionnalité. Un attribut est une information associée à un type de document spécifique. Le système utilise ces informations pour différentes fonctions telles que la validation des documents ou la vérification du chiffrement.

Révision et édition des fonctions B2B :

1. Cliquez sur **Administrateur du compte** > **Profils** > **B2B Fonctions**. Le système affiche l'écran des fonctions B2B.
   - Si un dossier apparaît à côté d'un package et que la colonne Activé affiche le mot Activé, cela signifie que l'administrateur du concentrateur a activé cette fonctionnalité pour vous.
   - Une marque en dessous de Définition de la source ou de Définition de la cible indique que vous pouvez utiliser cette fonctionnalité dans ce rôle (c-à-d. en tant que source, cible ou les deux).
   - L'icône Créer un rôle sous Définition de la source ou Définition de la cible indique que cette fonctionnalité n'est pas activée dans ce rôle (c'est-à-dire, en tant que source, cible ou les deux).
   - La colonne Activé affiche l'état du package : Activé ou Désactivé.

   Remarque : La fonctionnalité de cible, de source ou des deux doit être définie avant que vous puissiez l'activer.
2. Définissez votre fonction pour initier (**Définition de la source**), recevoir (**Définition de la cible**) ou initier et recevoir le contexte du type de document. Dans un PIP bidirectionnel, la Définition de la source et la Définition de la cible sont les mêmes pour toutes les actions, bien que la demande et la confirmation qui y correspond proviennent de deux partenaires différents.
3. Définissez votre fonction pour initier (**Définition de la source**), recevoir (**Définition de la cible**) ou initier et recevoir pour chaque définition de type de document de niveau inférieur.

4. Cliquez sur l'icône Editer pour afficher, et si vous le souhaitez, modifier les définitions de type de document de niveau inférieur (Protocole ou Type de document, par exemple). Vous pouvez aussi modifier les attributs de la définition d'un type de document (par exemple l'Heure d'exécution ou le Nombre de relances). Lorsque vous utilisez cet écran pour la première fois, les attributs sont définis globalement. Vous pouvez toutefois les réinitialiser localement, si vous le souhaitez. La définition d'un attribut au niveau local remplace la définition de votre environnement, mais pas la définition globale.
   - Si vous effectuez une modification, à quelque niveau que ce soit, elle se propage à tous les niveaux inférieurs.
   - Vous avez la possibilité de sélectionner et éditer un dossier individuel situé sous un package. Ce genre de modification ne se propage pas aux niveaux inférieurs.
   - Vous pouvez annuler l'option intégrée "tout sélectionner" en désélectionnant du bas vers le haut.
   - Les signaux, par exemple les accusés de réception, sont spécifiques à RosettaNet. Il y a trois signaux en dessous de chaque action : Accuser réception, Exception générale et Exception d'accusé de réception. Vous pouvez définir des attributs pour les signaux.
   - Irréfutabilité requise
   - ID entreprise de l'AS

   Si vous avez modifié un attribut, cliquez sur **Sauvegarder**.

Chargement de certificats numériques

Un certificat numérique est un justificatif d'identification en ligne similaire au passeport ou au permis de conduire d'un chauffeur. Un certificat numérique peut être utilisé pour identifier un individu ou une organisation.

Il s'agit de calculs basés sur un document électronique avec une cryptographie de clé publique. Au cours de ce processus, la signature numérique est liée au document signé ainsi qu'au signataire et ne peut pas être reproduite. Depuis que la loi sur les signatures numériques a été votée, les transactions électroniques signées numériquement ont la même valeur juridique que les transactions signées avec un stylo.

WebSphere Partner Gateway utilise les certificats numériques pour vérifier l'authenticité des transactions de documents de gestion entre le partenaire interne et les partenaires externes. Ils servent aussi au chiffrement et au déchiffrement.

Vous pouvez spécifier un certificat principal et un secondaire pour les documents entrants afin de vous assurer que l'échange de documents n'est pas interrompu. Le certificat principal est utilisé pour toutes les transactions. Le secondaire est utilisé si le principal est expiré ou révoqué.

Les certificats numériques sont chargés et identifiés pendant le processus de configuration.

Si un certificat a expiré ou est révoqué, il est désactivé et apparaît comme tel dans la console. Si le certificat principal a expiré ou est révoqué, il est désactivé et le certificat secondaire sera défini comme principal. Un événement est généré lorsqu'un certificat a expiré ou est révoqué.

L'option Utilisation du certificat est disponible en fonction du type de certificat sélectionné. Dans le profil de l'Opérateur de concentrateur, l'Utilisation du certificat peut être définie pour un certificat de signature numérique ou un certificat client SSL. Dans le profil partenaire, l'Utilisation du certificat peut être définie pour le certification de chiffrement. Si le même certificat doit être utilisé pour des objectifs différents, par exemple, pour la signature numérique et le chiffrement dans le profil de l'opérateur du concentrateur, il doit être chargé deux fois, une fois pour la signature numérique et une deuxième fois pour le certificat de chiffrement. Cependant, si le certificat est utilisé pour une signature numérique ou un client SSL, les cases correspondantes peuvent être cochées dans la même entrée de certificat.

Ces certificats peuvent également être chargés deux fois, une fois pour la signature numérique et une deuxième fois pour le client SSL. Si tel est le cas, le même modèle doit être appliqué pour les certificats secondaires. Par exemple, si les certificats principaux ont été chargés comme certificats distincts pour la signature numérique et pour le client SSL, des certificats secondaires doivent également être chargés comme entrées de certificats distinctes (même si le certificat peut être le même).

Pour la création et la validation complète de certpath, vous devez charger tous les certificats dans la hiérarchie de certificats. Par exemple, si la hiérarchie de certificats contient les certificats A -> B -> C -> D, où A -> B signifie que A est l'émetteur de B, alors les certificats A, B, et C doivent être chargés en tant que certificats racines. Si l'un des certificats n'est pas disponible, la valeur certpath ne sera pas créée et la transaction n'aboutira pas. Les certificats de CA peuvent être obtenus à partir des référentiels de certificats maintenus par les autorités de certification ou à partir du partenaire ayant fourni le certificat. Les certificats racine peuvent uniquement être chargés dans le profil Opérateur de concentrateur.

Remarque : Avant de pouvoir utiliser les procédures dans les sections suivantes, les certificats doivent être chargés dans le système. Pour plus d'informations sur le chargement des certificats, voir le manuel *Hub Configuration Guide*.

Vous pouvez créer des alertes d'expiration de certificat qui vous informeront lorsqu'un certificat sera sur le point d'expirer. Pour plus d'informations, voir «Création d'alertes et ajout de contacts», à la page 34. Les certificats expirés sont sauvegardés dans la base de données IBM WebSphere Partner Gateway. Ils ne peuvent pas être supprimés du système.

Dispositions du certificat

Autorité de certification (AC). Autorité émettant et gérant des justificatifs de sécurité et des clés publiques pour le chiffrement de message. Lorsqu'un individu ou une entreprise requiert un certificat numérique, une AC et une autorité d'enregistrement contrôlent les informations qui leur sont données par l'individu ou l'entreprise. Si les informations soumises sont vérifiées par l'autorité d'enregistrement, l'AC émet un certificat.

VeriSign et Thawte sont des exemples d'AC.

Certificat numérique. Le certificat numérique est la version électronique de la carte d'identité. Il établit votre identité lorsque vous effectuez des transactions B2B sur Internet. Les certificats numériques s'obtiennent auprès d'une autorité de certification (AC) et comportent trois éléments :

- La partie publique de votre paire de clé publique et privée.
- Des informations vous identifiant.
- La signature numérique d'une entité fiable (AC) attestant de la validité du certificat.

Signature numérique. Code numérique créé avec une clé privée. Les signatures numériques permettent aux membres de la communauté de concentrateur d'authentifier les transmissions grâce à la vérification de la signature. Lorsque vous signez un fichier, un code numérique spécifique au contenu du fichier et à votre clé privée est créé. Votre clé publique sert à vérifier votre signature.

Chiffrement. Méthode de codage des informations rendant celles-ci illisibles, excepté pour le destinataire prévu qui doit les déchiffrer pour les lire.

Déchiffrement. Méthode de décodage des informations chiffrées qui les rend à nouveau lisibles. La clé privée du destinataire sert au déchiffrement.

Clé. Code numérique servant à chiffrer, signer, déchiffrer et vérifier les fichiers. Les clés peuvent se présenter en paires, comprenant un clé privée et une clé publique.

Irréfutabilité. Empêche la dénégation d'actions ou d'engagements déjà entrepris. Pour les transactions électroniques B2B, les signatures numériques servent à valider l'expéditeur et à horodater la transaction. Cela empêche les parties prenantes de prétendre que la transaction n'était pas valide ou autorisée.

Clé privée. Partie secrète d'une paire de clés. Cette clé sert à signer et à déchiffrer les informations. Vous seul avez accès à votre clé privée. Elle sert aussi à générer une signature numérique unique basée sur le contenu du document.

Clé publique. Partie publique d'une paire de clés. Cette clé sert à chiffrer les informations et à vérifier les signatures. Une clé publique peut être distribuée aux autres membres de la communauté de concentrateur. Le fait de connaître la clé publique d'une personne ne permet pas de découvrir la clé privée correspondante.

Clé auto-signée. Clé publique ayant été signée par la clé privée correspondante pour preuve du droit de propriété.

Certificat X.509. Certificat numérique servant à prouver l'identité et le droit de propriété d'une clé publique sur un réseau de communication. Il comporte le nom et la signature numérique de l'émetteur (c-à-d. l'AC) ainsi que les informations d'identification de l'utilisateur.

Votre certificat identifie la période pendant laquelle il est valide et votre organisation.

Types de certificats et formats pris en charge

Tous les certificats doivent être au format DER ou ASCII PEM (Privacy Enhanced Mail). Ils peuvent être convertis d'un format à l'autre.

Il existe différents types de certificats :

- **Certificat client SSL (partenaires externes et partenaire interne)**. Certificat de transport. Si votre transport de communication sortante est HTTPS, vous aurez besoin d'un certificat de Client SSL. Dans la plupart des cas, le certificat de Client SSL doit être signé par une AC. Si le certificat est utilisé dans un environnement de test, il peut être auto-signé.

  Vous devez charger le certificat sur WebSphere Partner Gateway via la console et en envoyer une copie à l'Opérateur du concentrateur.
- **Certificat de Client SSL**. Active l'authentification de serveur SSL. L'AC du certificat du serveur SSL doit être échangée entre les partenaires.
- **Certificat de chiffrement (partenaires externes et partenaire interne)**. Si les membres de la communauté de concentrateur chiffrent des fichiers, la partie du certificat de chiffrement correspondant à la clé publique doit être envoyée aux membres de la communauté de concentrateur. La partie du certificat de chiffrement correspondant à la clé publique doit être envoyée au niveau de l'opérateur de concentrateur via la console. Vous devez envoyer la partie du certificat de partenaire correspondant à la clé publique à WebSphere Partner Gateway via la console et envoyer une copie du certificat à l'Opérateur de concentrateur.
- **Certificat de signature numérique (partenaires externes et partenaire interne)**. Si les membres de la communauté de concentrateur signent les documents, la partie publique du certificat de signature doit être envoyée au concentrateur au niveau du partenaire en tant que certificat de signature. Si le gestionnaire de concentrateur doit signer les documents qu'il envoie aux membres de la communauté de concentrateur, vous devez envoyer la partie publique du certificat du gestionnaire de concentrateur aux membres de la communauté. Le certificat de signature du concentrateur doit être envoyé via la console à l'opérateur de concentrateur.
- **Certificat VTP (partenaire interne)**. Ce certificat est utilisé par le Gestionnaire de documents de WebSphere Partner Gateway pour la fonction de simulateur du partenaire externe. Il est copié sur le système de fichiers plutôt que chargé via la console.

  Les certificats VTP copiés sur le système de fichiers sont actifs pour tous les partenaires créés par le biais de la console. Ils servent à valider les documents signés reçus par le simulateur du partenaire externe. En outre, les certificats copiés sur le système de fichiers ne sont pas visualisables via la console.

Serveur SSL et authentification client

Si l'authentification client n'est pas obligatoire :

- Si le certificat du serveur Web de la communauté de concentrateur est un certificat d'auto-signature, les partenaires doivent en avoir une copie.
- Si le certificat du serveur Web de la communauté de concentrateur provient d'une autorité de certification, les partenaires doivent avoir une copie des certificats intermédiaire et racine de l'AC.

Si l'authentification client est obligatoire :

- Si le certificat du serveur Web de la communauté de concentrateur est un certificat d'auto-signature, les partenaires doivent en avoir une copie.

- Si le certificat du serveur Web de la communauté de concentrateur provient d'une autorité de certification, les partenaires doivent avoir une copie des certificats intermédiaire et racine de l'AC.
- Le serveur cible doit avoir une copie du certificat du partenaire s'il est auto-signé et chargé dans le fichier de clés sécurisé.
- Le serveur cible doit avoir une copie du certificat des autorités de certification s'il est authentifié par une AC et chargé dans le fichier de clés sécurisé.

Remarque : Les versions précédentes de WebSphere Partner Gateway ne prenaient pas en charge le format d'adresse IPv6. WebSphere Partner Gateway 6.1 prend en charge ce format. Vérifiez qu'au moins un de vos serveurs est configuré pour prendre en charge le format d'adresse IPv6. La configuration pour le format IPv6 n'est nécessaire que sur le serveur.

Configuration de certificats SSL pour les communications entrantes

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

Une demande de connexion entrante est générée lorsque le partenaire envoie un document à WebSphere Partner Gateway. Si votre communauté n'utilise pas la couche SSL, vous n'avez pas besoin de certificat SSL pour les communications entrantes ou sortantes.

Remarque : Pour les communications FTPS entrantes, WebSphere Partner Gateway utilise un serveur FTP fourni par le client : la configuration nécessaire pour les communications SSL entrantes dépend donc du serveur FTP utilisé par le client.

Etape 1 : Obtention d'un certificat SSL : WebSphere Application Server utilise le certificat SSL lorsqu'il reçoit des demandes de connexion de partenaires via SSL. Il s'agit du certificat que le récepteur présente pour identifier le concentrateur auprès du partenaire. Ce certificat serveur peut être auto-signé ou signé par une autorité de certification. Dans la plupart des cas, vous utilisez un certificat d'une autorité de certification pour augmenter la sécurité. Vous pouvez utiliser un certificat d'auto-signature dans un environnement de test. Utilisez iKeyman ou la console d'administration de WebSphere Application Server pour générer un certificat et une paire de clés. Pour plus d'informations sur l'utilisation de iKeyman ou la console d'administration de WebSphere Application Server, reportez-vous à la documentation disponible auprès d'IBM.

Une fois le certificat et la paire de clés générés, utilisez le certificat pour le trafic SSL entrant de tous les partenaires. Si vous disposez de plusieurs récepteurs ou consoles, copiez le fichier de clés résultant sur chaque instance. Si le certificat est généré à l'aide de la console d'administration de WebSphere Application Server, la clé et le certificat peuvent être importés dans un autre fichier de clés d'un serveur autre grâce à cette console. Si le certificat est auto-signé, fournissez-le aux partenaires. Pour obtenir ce certificat, utilisez l'utilitaire iKeyman afin d'extraire le certificat public dans un fichier.

Génération d'un certificat d'auto-signature : Si vous avez l'intention d'utiliser des certificats de serveur auto-signés, utilisez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman qui se trouve dans /<*WAS_Installation_dir*>/bin. Si vous utilisez iKeyman pour la première fois, supprimez le certificat "factice" (dummy) se trouvant dans le fichier de clés.
2. Ouvrez le fichier de clés du récepteur ou de la console à l'aide de l'utilitaire iKeyman, puis utilisez ce dernier pour générer un certificat d'auto-signature et une paire de clés pour le fichier de clés du récepteur ou de la console.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.

   Sauvegardez le fichier de clés dans un fichier JKS, PKCS12 ou JCEKS.
4. Distribuez le certificat à vos partenaires. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos partenaires doivent vous appeler et vous demander le mot de passe correspondant au fichier compressé.
5. A l'aide de la console d'administration de WebSphere Application Server, définissez le nouveau certificat dans la configuration SSL et dans les paramètres du récepteur et de la console. Vous pouvez également le faire en sélectionnant l'alias du nouveau certificat dans le fichier de clés figurant dans la configuration de chaque noeud ou serveur.

Obtention d'un certificat généré par une autorité de certification (CA) : Si vous envisagez d'utiliser un certificat signé par une autorité de certification, suivez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman qui se trouve dans le répertoire /<*WAS_Installation_dir*>/bin.
2. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le récepteur.
3. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.
4. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le fichier de clés.
5. Distribuez le certificat de CA à tous les partenaires, le cas échéant.
6. A l'aide de la console d'administration de WebSphere Application Server, définissez le nouveau certificat dans la configuration SSL et dans les paramètres du récepteur et de la console. Vous pouvez également le faire en sélectionnant l'alias du nouveau certificat dans le fichier de clés figurant dans la configuration de chaque noeud ou serveur.

   Remarque : Vous pouvez également utiliser la console d'administration de WebSphere Application Server pour effectuer les étapes précédentes.

Etape 2 : Authentification des clients : Si vous souhaitez authentifier les partenaires qui envoient des documents, procédez comme suit.

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

1. Procurez-vous le certificat de votre partenaire.
2. Si le certificat est auto-signé, installez le certificat dans le fichier de clés à l'aide de l'utilitaire iKeyman ou de la console d'administration de WebSphere Application Server.

3. Si le certificat est généré à l'aide de la console d'administration, ajoutez les certificats de CA associés au fichier de clés certifiées associé à l'aide de l'utilitaire iKeyman ou de la console d'administration de WebSphere Application Server.

Remarque : Lorsque vous ajoutez plusieurs partenaires à la communauté de votre concentrateur, vous pouvez utiliser iKeyman ou la console d'administration de WebSphere Application Server pour ajouter leurs certificats au fichier de clés certifiées. Si un partenaire quitte la communauté, vous pouvez utiliser iKeyman ou la console d'administration de WebSphere Application Server pour supprimer les certificats du partenaire du fichier de clés certifiées.

Configuration de l'authentification du client : Une fois le ou les certificats installés, configurez WebSphere Application Server afin d'utiliser l'authentification client en exécutant le script utilitaire bcgClientAuth.jacl.

1. Passez dans le répertoire : /<*ProductDir*>/bin
2. Pour activer l'authentification client, appelez le script comme suit :

```
./bcgwsadmin.sh -f /<ProductDir>/scripts/bcgClientAuth.jacl
   -conntype NONE set
```

Remarque : Pour désactiver l'authentification client, appelez le script comme suit :

```
./bcgwsadmin.sh -f /<ProductDir>/receiver/scripts/
bcgClientAuth.jacl-conntype NONE clear
```

Vous devez redémarrer le serveur bcgreceiver pour que ces modifications prennent effet. Vous pouvez également activer l'authentification du client à l'aide de la console d'administration de WebSphere Application Server. La valeur ″Pris en charge″ signifie que le serveur demande le certificat client, mais si ce dernier est indisponible, l'établissement de liaison SSL peut encore être établi. La valeur ″Obligatoire″ signifie que le certificat client doit être envoyé. Sinon, l'établissement de liaison SSL échoue.

Validation du certificat du client : Une fonction supplémentaire peut être utilisée avec l'authentification client SSL. Elle est activée via la Console de communauté. Pour HTTPS, WebSphere Partner Gateway vérifie les certificats par rapport aux ID entreprise contenus dans les documents entrants. Pour pouvoir utiliser cette fonction, créez le profil du partenaire, importez le certificat client et marquez-le comme SSL.

1. Importez le certificat client.
   a. Cliquez sur **Administrateur du compte > Profils > Partenaire** et recherchez le profil du partenaire.
   b. Cliquez sur **Certificats**.
   c. Cliquez sur **Charger un certificat**.
   d. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
   e. Sélectionnez **Client SSL** comme type de certificat.
   f. Tapez une description du certificat (obligatoire).
   g. Faites passer l'état sur **Activé**.
   h. Si vous souhaitez sélectionner un autre mode de fonctionnement que **Production** (valeur par défaut), sélectionnez-le dans la liste.
   i. Cliquez sur **Terminer**.

2. Mettez à jour la destination du client.
   a. Cliquez sur **Administrateur du compte > Profils > Partenaire** et recherchez le profil du partenaire.
   b. Cliquez sur **Destinations**.
   c. Sélectionnez la destination HTTPS précédemment créée. Si vous n'avez pas encore créé la destination HTTPS, consultez la section «Configuration d'une destination HTTPS», à la page 45.
   d. Cliquez sur l'icône **Edition** pour modifier la destination.
   e. Sélectionnez **Oui** pour **Valider le certificat client SSL**.
   f. Cliquez sur **Sauvegarder**.

Configuration de fichiers de clés et de fichiers de clés certifiées distincts pour le récepteur et pour la console : Par défaut, WebSphere Partner Gateway version 6.1 utilise des fichier de clés et fichier de clés certifiées communs pour le récepteur et pour la console. Toutefois, vous pouvez configurer des fichier de clés et fichiers de clés certifiées distincts pour le récepteur et pour la console au cours de l'installation en mode distribué.

Pour configurer les fichier de clés et fichiers de clés certifiées, créez et définissez des fichier de clés et fichiers de clés certifiées distincts pour le récepteur et pour la console. Créez également des configurations SSL distinctes. Les configurations SSL peuvent être définies au niveau du cluster ou au niveau du serveur. La définition des configurations SSL au niveau du cluster est plus facile puisque une fois définie, la configuration s'applique à tous les serveurs de ce cluster, ce qui vous évite d'avoir à configurer chaque serveur séparément.

Définition de la configuration SSL au niveau du cluster : Définir la configuration SSL avec de nouveaux fichier de clés et fichier de clés certifiées au niveau du cluster implique qu'aucune configuration SSL n'ait été définie au niveau du serveur. Mais si c'est le cas, la configuration SSL au niveau du cluster ne sera pas utilisée, c'est celle définie au niveau du serveur qui le sera.

Suivez la procédure ci-dessous pour définir la configuration SSL pour bcgconsoleCluster :

1. Créez un fichier de clés pour le cluster de la console. Ce fichier de clés doit être créé avec la portée du cluster bcgconsole en suivant le chemin de navigation **Sécurité > Gestion des certificats SSL et clés > Fichiers de clés et certificats**.
2. Créez un fichier de clés certifiées pour le cluster de la console. Ce fichier de clés certifiées doit être créé avec la portée du cluster bcgconsole en suivant le chemin de navigation **Sécurité > Gestion des certificats SSL et clés > Fichiers de clés et certificats**.
3. Créez une configuration SSL pour le cluster de la console avec la portée de ce cluster de console en suivant le chemin de navigation **Sécurité > Gestion des certificats SSL et clés > Configurations SSL**. Définissez les fichier de clés et fichier de clés certifiées créés aux étapes précédentes. Mettez à jour les alias de certificat figurant dans la liste du même nom en cliquant sur **Obtenir des alias de certificat** et sélectionnez l'alias obligatoire à employer pour l'authentification sur le serveur. Définissez le gestionnaire d'accréditation sur **IbmPKIX**.
4. Définissez cette configuration SSL dans bcgconsoleCluster en la substituant à la configuration SSL héritée. Mettez à jour les alias de certificat en cliquant sur **Mettre à jour les alias de certificat** et définissez l'alias à employer pour l'authentification sur le serveur.

5. Redémarrez bcgconsoleCluster.

Suivez la procédure ci-dessous pour définir la configuration SSL pour bcgreceiverCluster :

1. Créez un fichier de clés pour le cluster du récepteur. Ce fichier de clés doit être créé avec la portée du cluster bcgreceiver en suivant le chemin de navigation **Sécurité > Gestion des certificats SSL et clés > Fichiers de clés et certificats**.
2. Créez un fichier de clés certifiées pour le cluster du récepteur. Ce fichier de clés certifiées doit être créé avec la portée du cluster bcgconsole en suivant le chemin de navigation **Sécurité > Gestion des certificats SSL et clés > Fichiers de clés et certificats**.
3. Créez une configuration SSL pour le cluster du récepteur avec la portée de ce cluster de récepteur en suivant le chemin de navigation **Sécurité > Gestion des certificats SSL et clés > Configurations SSL** et définissez les fichier de clés et fichier de clés certifiées créés aux étapes précédentes. Obtenez les alias de certificat figurant en cliquant sur **Obtenir des alias de certificat** et sélectionnez l'alias obligatoire à employer pour l'authentification sur le serveur. Définissez le gestionnaire d'accréditation sur **IbmPKIX**.
4. Définissez cette configuration SSL dans bcgreceiverCluster en la substituant à la configuration SSL héritée. Mettez à jour les alias de certificat en cliquant sur **Mettre à jour les alias de certificat** et définissez l'alias à employer pour l'authentification sur le serveur.
5. Redémarrez bcgreceiverCluster.

Pour plus d'informations sur le travail avec les fichiers de clés, fichiers de clés certifiées, les configurations SSL et les configurations de noeud final, reportez-vous à la section *Sécurisation des applications et de leur environnement de la documentation WebSphere Application Server.*

Remarque :

Définition de NodeDefaultTrustStore dans NodeDefaultSSLSetting en mode distribué :
Cette définition doit être effectuée pour le mode distribué simple. Mais elle peut s'appliquer également au mode distribué complet si un fichier de clés et un fichier de clés certifiées communs sont utilisés pour le récepteur et la console. Si un noeud fédéré au sein d'une cellule, les certificats de signataire issus du noeud seront ajoutés à CellDefaultTrustStore. Par défaut, NodeDefaultSSLSetting se réfère à CellDefaultTrustStore comme fichier de clés certifiées. Pour le récepteur et la console de WebSphere Partner Gateway, l'utilisation de certificats de signataire en provenance d'autres noeuds n'est peut-être pas souhaitable. Pour utiliser un fichier de clés certifiées dédié pour les noeuds sur lesquels WebSphere Partner Gateway est installé, NodeDefaultTrustStore peut être défini dans NodeDefaultSSLSettings comme le fichier de clés certifiées.

Pour cette modification, procédez comme suit :

1. Dans la console d'administration de WebSphere Application Server, suivez le chemin de navigation **Sécurité > Gestion des certificats SSL et clés > Gérer les configurations de sécurité de noeud final > <nom_du_noeud> > Configurations SSL > NodeDefaultSSLSettings**.
2. Dans la zone Nom du fichier de clés certifiées, sélectionnez **NodeDefaultTrustStore**.

Remarque : Assurez-vous que NodeDefaultTrustStore est configuré pour le fichier de clés certifiées que vous souhaitez utiliser, exemple : bcgSecurityTrust.jks.

3. Cliquez sur **Appliquer**.
4. Sur la page suivante de la Console, cliquez sure **Sauvegarder** pour mettre à jour la configuration principale avec les modifications apportées.
5. Redémarrez les serveurs situés dans ce noeud.

Remarque : En mode distribué complet, les modifications ci-dessus doivent être réalisées sur l'ensemble des noeuds contenant des serveurs bcgreceiver et bcgconsole. En mode distribué simple, ces modifications doivent être réalisées sur l'ensemble des noeuds contenant des serveurs bcgserver.

Ajout de certificats de signataires dans trust.p12 si NodeDefaultTrustStore est défini pour le noeud contenant les serveurs WebSphere Partner Gateway : Pour le moment, NodeDefaultTrustStore se réfère à trust.p12. Si NodeDefaultTrustStore est défini comme le noeud contenant les serveurs WebSphere Partner Gateway, bcgSecurityTrust.jks n'est pas employé. Les certificats de signataire provenant de bcgSecurityTrust.jks doivent être ajoutés à trust.p12 selon les besoins.

Configuration de certificats SSL pour les communications sortantes

Une demande de connexion sortante est générée lorsque WebSphere Partner Gateway envoie un document à un partenaire. Si votre communauté n'utilise pas la couche SSL, vous n'avez pas besoin de certificat SSL pour les communications entrantes ou sortantes.

Etape 1 : Authentification du serveur : Si le protocole SSL est utilisé pour envoyer des documents sortants à vos partenaires, WebSphere Partner Gateway leur demande un certificat côté serveur. Le même certificat de CA peut être utilisé pour plusieurs partenaires. Le certificat doit être au format X.509 DER.

Remarque : Vous pouvez convertir le format avec l'utilitaire iKeyman. Procédez comme suit :

1. Démarrez iKeyman.
2. Créez un fichier 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 d'auto-signature du partenaire dans le profil Opérateur du concentrateur. Si le certificat a été signé par une CA et si le certificat de CA racine et tout autre certificat de la hiérarchie des certificats ne sont pas encore installés dans le profil Opérateur du concentrateur, procédez à leur installation.

1. Cliquez sur **Administrateur du compte > Profils > Certificats** pour afficher la liste des certificats.

   Assurez-vous d'être connecté à la console de communauté en tant qu'opérateur de concentrateur ou partenaire interne.
2. Cliquez sur **Charger PKCS12**.

Remarque : Le fichier PKCS12 envoyé ne doit contenir qu'une seule clé privée et le certificat associé. Vous pouvez également charger séparément le certificat et la clé privée de format PKCS#8.

3. Sélectionnez **Client SSL** comme type de certificat.
4. Tapez une description du certificat (obligatoire).
5. Faites passer l'état sur **Activé**.
6. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.
7. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
8. Entrez le mot de passe.
9. Si vous souhaitez sélectionner un autre mode de fonctionnement que **Production** (valeur par défaut), sélectionnez-le dans la liste.
10. Si vous avez deux certificats SSL, indiquez s'il s'agit du certificat principal ou secondaire en sélectionnant **Principal** ou **Secondaire** dans la liste **Utilisation du certificat**.
11. Cliquez sur **Charger**, puis sur **Sauvegarder**.

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

Etape 2 : Authentification des clients : Si une authentification SSL client est requise, le partenaire demande, en retour, un certificat au concentrateur. Utilisez la Console de communauté pour importer votre certificat dans WebSphere Partner Gateway. Vous pouvez générer le certificat à l'aide de iKeyman. Si le certificat est auto-signé, il doit être fourni au partenaire. S'il s'agit d'un certificat signé par une autorité de certification, il doit être envoyé aux partenaires, de sorte qu'ils puissent l'ajouter à leurs certificats authentifiés.

Vous pouvez attribuer plusieurs certificats. L'un est le certificat principal, utilisé par défaut. L'autre est un certificat secondaire qui est utilisé si le certificat principal expire.

Utilisation d'un certificat d'auto-signature : Si vous envisagez d'utiliser un certificat d'auto-signature, appliquez la procédure suivante.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer un certificat d'auto-signature et une paire de clés.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.
4. Distribuez le certificat à vos partenaires. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos partenaires doivent vous appeler et vous demander le mot de passe correspondant au fichier compressé.
5. Utilisez iKeyman pour exporter le certificat d'auto-signature et la paire de clés privées sous forme de fichier PKCS12.
6. Installez le certificat d'auto-signature et la clé via la Console de communauté.
   a. Cliquez sur **Administrateur du compte > Profils > Certificats** pour afficher la liste des certificats.

      Veillez à vous connecter à la Console de communauté en tant qu'opérateur du concentrateur.
   b. Cliquez sur **Charger PKCS12**.

Remarque : Le fichier PKCS12 envoyé ne doit contenir qu'une seule clé privée et le certificat associé. Vous pouvez également charger séparément le certificat et la clé privée de format PKCS#8.

c. Sélectionnez **Client SSL** comme type de certificat.

d. Tapez une description du certificat (obligatoire).

e. Faites passer l'état sur **Activé**.

f. Cliquez sur **Parcourir** et accédez au répertoire dans lequel vous avez enregistré le certificat.

g. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.

h. Entrez le mot de passe.

i. Si vous souhaitez sélectionner un autre mode de fonctionnement que **Production** (valeur par défaut), sélectionnez-le dans la liste.

j. Si vous avez deux certificats SSL, indiquez s'il s'agit du certificat principal ou secondaire en sélectionnant **Principal** ou **Secondaire** dans la liste **Utilisation du certificat**.

k. Cliquez sur **Charger**, 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 récepteur.
2. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.
3. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le fichier de clés.
4. Distribuez le certificat signé par l'autorité de certification à tous les partenaires.

Utilisation de certificats pour activer le chiffrement

Cette section apporte des informations sur les certificats de chiffrement.

Création et installation de certificats de chiffrement entrants

Ce certificat est utilisé par le concentrateur pour déchiffrer les fichiers codés, reçus de partenaires. Le concentrateur utilise votre clé privée pour déchiffrer les documents. Le chiffrement est utilisé pour empêcher toute autre personne que l'expéditeur et le destinataire prévu de visualiser les documents en transit.

Prenez note de la limitation importante formulée ci-dessous, concernant la réception de messages AS2 chiffrés envoyés par les partenaires. Si un partenaire envoie un message AS2 chiffré en utilisant le mauvais certificat, le déchiffrage échoue. Toutefois, aucune MDN n'est retournée au partenaire pour indiquer l'échec. Pour que votre partenaire puisse recevoir des MDN dans ce cas-là, créez une connexion au partenaire avec la définition de document suivante :

- Package : **AS** to Package: **None**
- Protocol: **Binary**to Protocol: **Binary**
- Document Type: **Binary**to Document Type: **Binary**

La connexion créée doit être une connexion d'AS à None ; en d'autres termes, il faut créer la connexion en activant les fonctions B2BAS sur un partenaire et B2B None sur l'autre. Assurez-vous que la passerelle source du côté AS est une passerelle SMTP (dans le cas d'AS1), HTTP (dans le cas d'AS2) ou FTP (dans le cas d'AS3), qui est configurée sur l'adresse MDN. Ce faisant, la MDN d'échec de déchiffrement sera renvoyée via cette connexion binaire AS to None.

Etape 1 : Obtention d'un certificat :

Génération d'un certificat d'auto-signature : Si vous envisagez d'utiliser un certificat d'auto-signature, appliquez la procédure suivante.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer un certificat d'auto-signature et une paire de clés.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.
4. Distribuez le certificat à vos partenaires. Ils doivent importer le fichier dans leur produit B2B pour l'utiliser comme certificat de chiffrement. Conseillez-leur de l'utiliser lorsqu'ils souhaitent envoyer des fichiers chiffrés au partenaire interne. Si votre certificat est signé par une autorité de certification, fournissez également le certificat de CA.
5. Utilisez iKeyman pour sauvegarder les certificats d'auto-signature et la paire de clés privées sous forme d'un fichier PKCS12.
6. Chemin de navigation : **Profil** > **{Opérateur de concentrateur/partenaire interne}** > **certificats** > **créer un certificat.**
7. Dans la liste déroulante **A quel partenaire ce certificat appartient-il ?**, sélectionnez le partenaire à associer au certificat nouvellement chargé.
8. Cliquez sur **Rechercher** pour trouver un partenaire particulier ou un sous-ensemble de partenaires.
9. Cliquez sur **Parcourir** en regard de **Emplacement du certificat** pour charger le certificat.
10. Cliquez sur **Suivant**.
11. Dans Fournir les caractéristiques du certificat, entrez les informations suivantes : **Certificat feuille**, **Certificat de CA racine** ou **Certificat de CA intermédiaire**.
12. Associez ce certificat à **Chiffrement**.
13. Dans **Usage du certificat**, sélectionnez **Principal** ou **Secondaire**.
14. Dans **Statut**, sélectionnez **Activé** ou **Désactivé** selon que vous souhaitez activer ou non le certificat après l'avoir chargé.
15. Sélectionnez le **Mode de fonctionnement**.
16. Cliquez sur **Terminer** pour sauvegarder les modifications et fermer l'assistant.

Utilisation d'un certificat signé par une autorité de certification (CA) : Si vous envisagez d'utiliser un certificat signé par une autorité de certification, suivez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le récepteur.
3. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.

4. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le fichier de clés.

Etape 2 : Distribution du certificat : Distribuez le certificat signé par l'autorité de certification à tous les partenaires.

Installation de certificats de chiffrement sortants

Ce certificat est utilisé lorsque le concentrateur envoie des documents chiffrés aux partenaires. WebSphere Partner Gateway chiffre les documents à l'aide des clés publiques des partenaires et ces derniers déchiffrent les documents avec leurs clés privées.

Le partenaire peut disposer de plusieurs certificats de chiffrement. L'un est le certificat principal, utilisé par défaut. L'autre est le certificat secondaire, utilisé si le certificat principal expire.

Etape 1 : Obtention du certificat du partenaire : Procurez-vous le certificat de chiffrement de votre partenaire. Le certificat doit être au format X.509 DER. Notez que WebSphere Partner Gateway n'accepte que les certificats X5.09.

Etape 2 : Installation du certificat du partenaire : Installez le certificat via la Console de communauté sous le profil du partenaire, en procédant de la manière suivante :

1. Chemin de navigation : **Profil** > **Partenaire externe** > **certificats** > **Charger un certificat**.
2. Sur la page **Sélectionner le partenaire, l'emplacement du fichier et le mot de passe** de l'assistant, entrez les valeurs suivantes :
   - **A quel partenaire ce certificat appartient-il ?** : Sélectionnez le partenaire à associer au certificat nouvellement chargé. Cliquez sur Rechercher pour trouver un partenaire particulier ou un sous-ensemble de partenaires. Si le partenaire est un opérateur de concentrateur ou un partenaire interne, entrez l'emplacement du certificat, l'emplacement de la clé privée et le mot de passe (OU) fournissez un mot de passe pour le fichier de clés certifiées ou le fichier de clés. Pour le partenaire externe, entrez l'emplacement du certificat (OU) indiquez l'emplacement du fichier de clés certifiées contenant la chaîne de certificats.
   - **Emplacement du certificat** : Cliquez sur Parcourir pour sélectionner l'emplacement du certificat public.
3. Cliquez sur **Suivant** pour accéder à la page **Caractéristiques du certificat** de l'assistant.
4. Sur la page **Caractéristiques du certificat** de l'assistant, entrez les caractéristiques suivants :
   - **Nom du certificat feuille** - comme son nom l'indique, c'est le nom du certificat feuille. Le nom de cette zone change en fonction de la nature du certificat (certificat feuille, certificat de CA racine ou certificat de CA intermédiaire).
   - **Description** - Description du certificat feuille.
   - **Type du certificat** - Associez ce certificat à Chiffrement.
   - **Utilisation du certificat** - Associez une utilisation au certificat. Les valeurs admisses sont Principal et Secondaire.
   - **Mode de fonctionnement** - Entrez le mode de fonctionnement.

- **Etat** - Sélectionnez Activé ou Désactivé selon que vous souhaitez activer ou désactiver un certificat après l'avoir chargé. Le bouton Suivant ne sera activé que si vous avez activé le certificat.
- **Gestion des jeux** - Vous pouvez associer un certificat à un jeu existant ou créer un nouveau jeu. Si le certificat est un certificat secondaire, il ne peut être associé qu'à un jeu existant. Vous pouvez associer le certificat à n'importe quel jeu, pour un partenaire interne de type Chiffrement ou pour un partenaire externe de type SSL (auth. client entrante) ou Signature (Vérification).

5. Cliquez sur **Suivant** pour accéder à la page Jeu de l'assistant. Si le certificat est un certificat principal, vous n'avez pas besoin de créer de jeux et d'associer le certificat à un jeu et à une connexion de participant. Si vous avez coché la case **Créer un jeu**, une page du même nom s'ouvre dans l'assistant. Dans le cas contraire, c'est la page **Ajouter à l'existant** qui s'ouvrira dans l'assistant. Si le fichier contient une clé privée du partenaire interne ou le certificat public du partenaire externe employé pour le SSL / la signature numérique, cliquez sur **Terminer**.
6. Dans la page **Créer un jeu** de l'assistant, entrez les caractéristiques du nouveau jeu. Si le certificat est un certificat principal, vous n'avez pas besoin de créer de jeux et d'y associer le certificat. Entrez les valeurs suivantes :
   - **Nom de jeu** - le nom du jeu.
   - **Description** - la description du jeu.
   - **Statut** - Sélectionnez activé ou désactivé. Si le statut est désactivé, le bouton **Suivant** ne sera pas activé.
   - **Utiliser les paramètres par défaut** - Cochez cette case si vous voulez que ce jeu soit le jeu par défaut.
7. Sur la page **Ajouter au jeu existant** de l'assistant, sélectionnez le jeu ou les jeux auxquels ajouter le certificat. Entrez les valeurs suivantes :
   - **Sélectionner dans la liste des jeux disponibles pour le type de certificat sélectionné** - Dans la liste, sélectionnez le jeu ou les jeux auxquels ajouter le certificat.
   - **Utiliser les paramètres par défaut** - Cochez cette case si vous voulez que ce jeu soit le jeu par défaut.
8. A partir de **Créer un jeu** ou **Ajouter à un jeu existant**, cliquez sur **Suivant** pour accéder à la page **Paramètres par défaut** de l'assistant. Le bouton **Suivant** ne sera activé que si le statut du jeu est activé.
9. Dans **Statut**, sélectionnez **Activé** ou **Désactivé** selon que vous souhaitez activer ou non le certificat après l'avoir chargé.

   Remarque : Si vous avez coché la case **Définir comme jeu par défaut** à la page précédente (Créer un jeu ou Ajouter à un jeu existant), vous devez associer le jeu à un mode de fonctionnement. Ceci affiche les différents cas d'utilisation des certificats en fonction des modes de fonctionnement. Le chiffrement sera désactivé pour les partenaires internes. Les options Client SSL et Signature numérique sont désactivées pour les partenaires externes.
10. Cliquez sur **Suivant** pour accéder à la page Configuration de l'assistant. Dans le cas où vous cliquez sur **Terminer** et que des certificats de CA racine ou intermédiaire sont manquants, vous serez invité à les charger. Si vous cliquez ″Oui″ à la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur **Annuler** si vous voulez effectuer le chargement plus tard.

11. Sur la page Configuration de l'assistant, entrez les valeurs suivantes :

    Remarque : La page Configuration affiche une liste de cas d'utilisation du certificat en fonction des modes de fonctionnement. Le nom du jeu actuel est prérempli mais vous pouvez le remettre à zéro.

    - **Partenaire source** - Cette zone est préremplie avec la valeur pour le partenaire interne.
    - **Partenaire cible** - Cette liste déroulante est préremplie avec la liste de l'ensemble des partenaires externes. Vous pouvez également sélectionner ″Tous″ pour inclure tous les partenaires externes.
    - **Package source**- Dans la liste, sélectionnez les objets Définitions de flux de documents du package pour le partenaire interne.
    - **Package de destination** - Dans la liste, sélectionnez les objets Définitions de flux de document du package du partenaire externe.

12. Cliquez sur **Ajouter plus de connexions** si vous souhaitez associer le jeu à d'autres connexions de participant.
13. Cliquez sur **Ajouter un certificat secondaire** pour ajouter un certificat secondaire au jeu actuel.
14. Cliquez sur **Terminer** pour charger le certificat. Si des certificats de CA racine ou intermédiaire sont manquants, vous serez invité à les charger. Si vous cliquez ″Oui″ à la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur **Annuler** dans la fenêtre d'invite si vous voulez procéder au chargement ultérieurement.

Répétez cette étape si le partenaire dispose d'un second certificat de chiffrement.

Etape 3 : Installation des certificats émis par une autorité de certification : Si le certificat a été signé par une autorité de certification (CA) et si le certificat de CA racine et tout autre certificat de la chaîne de certificats ne sont pas encore installés dans le profil Opérateur du concentrateur, procédez à leur installation de la manière suivante :

Remarque : Il est inutile d'effectuer cette étape si le certificat de CA est déjà installé.

1. Chemin de navigation : **Profil** > **{Opérateur de concentrateur/partenaire interne}** > **certificats** > **créer un certificat.**
2. Dans la liste déroulante **A quel partenaire ce certificat appartient-il ?**, sélectionnez le partenaire à associer au certificat nouvellement chargé.
3. Cliquez sur **Rechercher** pour trouver un partenaire particulier ou un sous-ensemble de partenaires.
4. Cliquez sur **Parcourir** en regard de **Emplacement du fichier de clés sécurisées (ou) du fichier de clés**.
5. Pour le certificat et le fichier de clés sécurisées, entrez un **Mot de passe**.
6. dans le cas de Fichier de clés sécurisées, entrez le **Type du fichier de clés**, puis cliquez sur **Suivant**.
7. Sur la page de l'assistant intitulée **Sélectionner un certificat d'entité finale à charger**, sélectionnez un certificat à charger.

   Remarque : Lorsque vous chargez des certificats au moyen d'un fichier de clés sécurisées comportant plus d'un certificat, tous les certificats sont renseignés sur la page **Sélectionner la liste des certificats de CA racine et intermédiaire à charger**. Vous avez aussi la possibilité de charger plusieurs certificats.

8. Cliquez sur **Terminer**.

Etape 4 : Activation du chiffrement : Activez le chiffrement au niveau package (niveau le plus élevé), partenaire ou connexion (niveau le plus bas). Votre définition peut remplacer les autres définitions au niveau connexion. Le résumé de la connexion vous indique si un attribut requis est manquant.

Par exemple, pour modifier les attributs d'une connexion de partenaire, cliquez sur **Administrateur du compte > Connexions**, puis sélectionnez les partenaires. Cliquez sur **Attributs**, puis éditez l'attribut (par exemple, **AS chiffré**).

Lorsque le message `Aucun certificat de chiffrement valide n'a été trouvé` est affiché, c'est qu'aucun des certificats (principal et secondaire) n'est valide. Les certificats peuvent avoir expirés ou avoir été révoqués. Si les certificats ont expiré ou ont été révoqués, l'événement correspondant (`Certificat révoqué ou expiré`) peut également être affiché dans l'afficheur d'événements. Notez que ces deux événements peuvent être séparés par d'autres.

Pour lancer l'Afficheur d'événements, procédez de la manière suivante :

1. Cliquez sur **Afficheurs > Afficheur d'événements**.
2. Sélectionnez les critères de recherche appropriés.
3. Cliquez sur **Rechercher**.

Pour obtenir davantage d'informations sur l'utilisation de l'Afficheur d'événements, voir le *Guide de l'administrateur de WebSphere Partner Gateway*.

Utilisation de certificats pour activer la signature numérique

Création d'un certificat de signature de communication sortante

Le Gestionnaire de documents utilise ce certificat lorsqu'il envoie des documents signés aux partenaires. Les mêmes certificat et clé sont utilisés pour tous les ports et protocoles.

Vous pouvez avoir plusieurs certificats de signature numérique. L'un est le certificat principal, utilisé par défaut. L'autre est le certificat secondaire, utilisé si le certificat principal expire.

Génération d'un certificat d'auto-signature : Si vous envisagez d'utiliser un certificat d'auto-signature, appliquez la procédure suivante.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer un certificat d'auto-signature et une paire de clés.
3. Utilisez iKeyman pour extraire dans un fichier le certificat qui contiendra votre clé publique.
4. Distribuez le certificat à vos partenaires. La méthode de distribution préférée consiste à envoyer le certificat par courrier électronique dans un fichier compressé protégé par mot de passe. Vos partenaires doivent vous appeler et vous demander le mot de passe correspondant au fichier compressé.
5. Utilisez iKeyman pour exporter le certificat d'auto-signature et la paire de clés privées sous forme de fichier PKCS12.

Installation de certificats d'auto-signature sortants :

1. Chemin de navigation : **Profil** > **Opérateur de concentrateur/partenaire interne** > **certificats** > **Charger un certificat**.

2. Sur la page **Sélectionner le partenaire, l'emplacement du fichier et le mot de passe** de l'assistant, entrez les valeurs suivantes :
   - **A quel partenaire ce certificat appartient-il ?** : Sélectionnez le partenaire à associer au certificat nouvellement chargé. Cliquez sur Rechercher pour trouver un partenaire particulier ou un sous-ensemble de partenaires. Si le partenaire est un opérateur de concentrateur ou un partenaire interne, entrez l'emplacement du certificat, l'emplacement de la clé privée et le mot de passe (OU) fournissez un mot de passe pour le fichier de clés certifiées ou le fichier de clés. Pour le partenaire externe, entrez l'emplacement du certificat (OU) indiquez l'emplacement du fichier de clés certifiées contenant la chaîne de certificats.
   - **Clé privée :** Cliquez sur **Parcourir** pour sélectionner la clé privée du certificat.
   - **Mot de passs :** Si le certificat possède un mot de passe, entrez ici sa valeur.
   - **Emplacement du fichier de clés certifiées (ou) du fichier de clés :** Cliquez sur **Parcourir** pour sélectionner l'emplacement du fichier de clés certifiées. Le fichier de clés est un ensemble de clés privées avec des certificats racine dignes de confiance et des certificats de CA.
   - **Mot de passe :** Entrez le mot de passe pour l'emplacement du fichier de clés.
   - **Type :** sélectionnez le type de fichier de clés sécurisées (ou) de fichier de clés. Les valeurs disponibles dans la liste déroulante sont : JKS, JCEKS, and PKCS12.
3. Cliquez sur **Suivant** pour accéder à la page **Caractéristiques du certificat** de l'assistant. La page **Sélectionner des certificats de CA et d'entité finale** de l'assistant s'ouvrira lorsque vous chargez des certificats via un fichier de clés ayant plusieurs certificats. La liste des certificats disponibles dans le fichier de clés certifiées s'affiche.
4. Sur la page de l'assistant intitulée **Sélectionner un certificat d'entité finale et un certificat de CA**, entrez les valeurs suivantes :
   - **Le fichier de clés contient plusieurs certificats d'entité finale. Sélectionner le certificat à charger ?** - La liste déroulante contient une liste de tous les certificats d'entité finale. Sélectionnez le certificat à charger.
   - **Mot de passe** - Si le fichier de clés comporte un mot de passe, cochez la case et entrez le mot de passe dans la zone de texte.
   - **Sélectionner la liste des certificats de CA racines et intermédiaires à charger** - Dans la liste déroulante, sélectionnez les certificats de CA racines et intermédiaires à charger.
5. Cliquez sur **Suivant** pour accéder à la page **Caractéristiques du certificat** de l'assistant.
6. Sur la page **Caractéristiques du certificat** de l'assistant, entrez les caractéristiques suivants :
   - **Nom du certificat feuille** - comme son nom l'indique, c'est le nom du certificat feuille. Le nom de cette zone change en fonction de la nature du certificat (certificat feuille, certificat de CA racine ou certificat de CA intermédiaire).
   - **Description** - Description du certificat feuille.
   - **Type du certificat** - Associez ce certificat à Chiffrement.
   - **Utilisation du certificat** - Associez une utilisation au certificat. Les valeurs admisses sont Principal et Secondaire.
   - **Mode de fonctionnement** - Entrez le mode de fonctionnement.

- **Etat** - Sélectionnez Activé ou Désactivé selon que vous souhaitez activer ou désactiver un certificat après l'avoir chargé. Le bouton Suivant ne sera activé que si vous avez activé le certificat.
- **Gestion des jeux** - Vous pouvez associer un certificat à un jeu existant ou créer un nouveau jeu. Si le certificat est un certificat secondaire, il ne peut être associé qu'à un jeu existant. Vous pouvez associer le certificat à n'importe quel jeu, pour un partenaire interne de type Chiffrement ou pour un partenaire externe de type SSL (auth. client entrante) ou Signature (Vérification).

Remarque : Pour l'opérateur de concentrateur, il n'y aura pas de gestion des jeux. Les certificats seront associés au jeu créé par défaut.

7. Cliquez sur **Suivant** pour accéder à la page Jeu de l'assistant. Si le certificat est un certificat principal, vous n'avez pas besoin de créer de jeux et d'associer le certificat à un jeu et à une connexion de participant. Si vous avez coché la case **Créer un jeu**, une page du même nom s'ouvre dans l'assistant. Dans le cas contraire, c'est la page **Ajouter à l'existant** qui s'ouvrira dans l'assistant. Si le fichier contient une clé privée du partenaire interne ou le certificat public du partenaire externe employé pour le SSL / la signature numérique, cliquez sur **Terminer**.
8. Dans la page **Créer un jeu** de l'assistant, entrez les caractéristiques du nouveau jeu. Si le certificat est un certificat principal, vous n'avez pas besoin de créer de jeux et d'y associer le certificat. Entrez les valeurs suivantes :
   - **Nom de jeu** - le nom du jeu.
   - **Description** - la description du jeu.
   - **Statut** - Sélectionnez activé ou désactivé. Si le statut est désactivé, le bouton **Suivant** ne sera pas activé.
   - **Utiliser les paramètres par défaut** - Cochez cette case si vous voulez que ce jeu soit le jeu par défaut.
9. Sur la page **Ajouter au jeu existant** de l'assistant, sélectionnez le jeu ou les jeux auxquels ajouter le certificat. Entrez les valeurs suivantes :
   - **Sélectionner dans la liste des jeux disponibles pour le type de certificat sélectionné** - Dans la liste, sélectionnez le jeu ou les jeux auxquels ajouter le certificat.
   - **Utiliser les paramètres par défaut** - Cochez cette case si vous voulez que ce jeu soit le jeu par défaut.
10. A partir de **Créer un jeu** ou **Ajouter à un jeu existant**, cliquez sur **Suivant** pour accéder à la page **Paramètres par défaut** de l'assistant. Le bouton **Suivant** ne sera activé que si le statut du jeu est activé.
11. Dans **Statut**, sélectionnez **Activé** ou **Désactivé** selon que vous souhaitez activer ou non le certificat après l'avoir chargé.

Remarque : Si vous avez coché la case **Définir comme jeu par défaut** à la page précédente (Créer un jeu ou Ajouter à un jeu existant), vous devez associer le jeu à un mode de fonctionnement. Ceci affiche les différents cas d'utilisation des certificats en fonction des modes de fonctionnement. Le chiffrement sera désactivé pour les partenaires internes. Les options Client SSL et Signature numérique sont désactivées pour les partenaires externes.

12. Cliquez sur **Suivant** pour accéder à la page Configuration de l'assistant. Dans le cas où vous cliquez sur **Terminer** et que des certificats de CA racine ou intermédiaire sont manquants, vous serez invité à les charger. Si vous cliquez

″Oui″ à la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur **Annuler** si vous voulez effectuer le chargement plus tard.

13. Sur la page Configuration de l'assistant, entrez les valeurs suivantes :

    Remarque : La page Configuration affiche une liste de cas d'utilisation du certificat en fonction des modes de fonctionnement. Le nom du jeu actuel est prérempli mais vous pouvez le remettre à zéro.

    - **Partenaire source** - Cette zone est préremplie avec la valeur pour le partenaire interne.
    - **Partenaire cible** - Cette liste déroulante est préremplie avec la liste de l'ensemble des partenaires externes. Vous pouvez également sélectionner ″Tous″ pour inclure tous les partenaires externes.
    - **Package source**- Dans la liste, sélectionnez les objets Définitions de flux de documents du package pour le partenaire interne.
    - **Package de destination** - Dans la liste, sélectionnez les objets Définitions de flux de document du package du partenaire externe.

14. Cliquez sur **Ajouter plus de connexions** si vous souhaitez associer le jeu à d'autres connexions de participant.
15. Cliquez sur **Ajouter un certificat secondaire** pour ajouter un certificat secondaire au jeu actuel.
16. Cliquez sur **Terminer** pour charger le certificat. Si des certificats de CA racine ou intermédiaire sont manquants, vous serez invité à les charger. Si vous cliquez ″Oui″ à la fenêtre d'invite, la première page de l'assistant s'ouvre. Cliquez sur **Annuler** dans la fenêtre d'invite si vous voulez procéder au chargement ultérieurement.

Si vous envoyez les certificats principaux et secondaires, pour l'authentification SSL du client et la signature numérique, et que vous envoyez les certificats principaux dans deux entrées séparées, assurez-vous que les certificats secondaires correspondant sont également envoyés comme des entrées séparées.

Obtention d'un certificat signé par une autorité de certification (CA) : Si vous envisagez d'utiliser un certificat signé par une autorité de certification, suivez la procédure ci-dessous.

1. Démarrez l'utilitaire iKeyman.
2. Utilisez iKeyman pour générer une demande de certificat et une paire de clés pour le récepteur.
3. Envoyez une demande de signature de certificat (CSR, Certificate Signing Request) à une autorité de certification.
4. Lorsque vous recevez le certificat signé de l'autorité de certification, utilisez iKeyman pour le placer dans le fichier de clés.
5. Distribuez le certificat signé par l'autorité de certification à tous les partenaires.

Installation d'un certificat de signature de communication entrante

Le Gestionnaire de documents utilise le certificat signé du partenaire pour vérifier la signature de l'expéditeur lorsque vous recevez des documents. Les partenaires vous envoient leurs certificats de signature auto-signés au format X.509 DER. De votre côté, vous installez les certificats des partenaires via la Console de communauté sous leurs profils respectifs.

Pour installer le certificat, utilisez la procédure ci-dessous.

1. Recevez le certificat de signature X.509 du partenaire au format DER.

2. Chemin de navigation : **Profil** > **Partenaire externe** > **certificats** > **Charger un certificat**.
3. Cliquez sur **Rechercher** pour trouver un partenaire particulier ou un sous-ensemble de partenaires.
4. Cliquez sur **Parcourir** en regard de **Emplacement du certificat** pour charger le certificat.
5. Cliquez sur **Suivant** pour accéder à la page **Caractéristiques du certificat** de l'assistant.
6. Associez ce certificat à **Signature numérique**.
7. Dans **Statut**, sélectionnez **Activé** ou **Désactivé** selon que vous souhaitez activer ou non le certificat après l'avoir chargé.
8. Sélectionnez le **Mode de fonctionnement**. Si vous êtes opérateur du concentrateur, le choix du **Mode de fonctionnement** ne s'applique pas à vous.
9. Cliquez sur **Terminer** pour sauvegarder les modifications et fermer l'assistant.
10. Si le certificat a été signé par une autorité de certification et si le certificat de CA racine et tout autre certificat de la hiérarchie des certificats ne sont pas encore installés dans le profil Opérateur du concentrateur, procédez à leur installation. Ceci ne s'applique qu'à Fichier de clés sécurisées/Fichier de clés.
    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 un 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 **Charger**, puis sur **Sauvegarder**.

    Remarque : Il est inutile d'effectuer l'étape précédente si le certificat de CA est déjà installé.
11. Activez la signature au niveau package (niveau le plus élevé), partenaire ou connexion (niveau le plus bas). Votre définition peut remplacer les autres définitions au niveau connexion. Le résumé de la connexion vous indique si un attribut requis est manquant.

    Par exemple, pour modifier les attributs d'une connexion de partenaire, cliquez sur **Administrateur du compte > Connexions**, puis sélectionnez les partenaires. Cliquez sur **Attributs**, puis éditez l'attribut (par exemple **AS signé**).

Création de groupes de console

Utilisez la fonction Groupe pour créer un groupe pour un type spécifique d'utilisateur, disposant de privilèges de console spécifiques. Par exemple : vous souhaitez créer un groupe Testeurs pour les utilisateurs affectés au test de la connectivité lors du cycle de test. Après l'avoir créé, vous pouvez attribuer à ce groupe des droits d'accès basés sur les fonctions de la console auxquelles ses utilisateurs doivent avoir accès pendant le cycle de test.

Le système créé automatiquement le groupe Administrateur et le groupe par défaut avec les paramètres de droit d'accès par défaut. Tous les utilisateurs des groupes administrateur du concentrateur ou du groupe administrateur du partenaire peuvent modifier ces paramètres.

Avertissement : Le groupe Administrateur et le groupe par défaut sont générés par le système et ne peuvent être édités ou supprimés. Le groupe Administrateur du concentrateur a un groupe supplémentaire, Admin du concentrateur.

Pour créer des groupes :

1. Cliquez sur **Administrateur du compte** > **Profils** > **Groupes**. Le système affiche l'écran Liste des groupes.
2. Cliquez sur **Créer** dans l'angle supérieur droit de l'écran. Le système affiche l'écran Caractéristiques du groupe.
3. Saisissez le **Nom** et la**Description** du nouveau groupe.
4. Cliquez sur **Sauvegarder**. Pour ajouter des groupes supplémentaires, répétez ces étapes.

Création d'utilisateurs

Utilisez cette fonction pour créer des profils utilisateur. Le système utilise les profils de partenaires pour contrôler l'accès à la console, la distribution d'alerte et la visibilité des utilisateurs.

Le profil d'un utilisateur comprend son nom et ses informations de contact (adresse électronique et numéros de téléphone), son état de connexion (Activé ou Désactivé), ainsi que son état d'alerte (Activé ou Désactivé) et sa visibilité (Local ou Global). Le nom d'utilisateur est unique.

- Si son état de connexion est Activé, l'utilisateur peut se connecter à la Console de communauté. S'il est Désactivé, l'utilisateur ne peut pas se connecter à la Console de communauté.
- Si son état d'alerte est Activé, l'utilisateur peut recevoir des notifications d'alerte. S'il est Désactivé, l'utilisateur ne peut pas recevoir de notification d'alerte.
- Si sa visibilité est Locale, l'utilisateur ne peut être vu que par votre organisation. Si elle est Globale, l'utilisateur peut être vu par toute la communauté de concentrateur.

Vous pouvez également générer automatiquement un mot de passe pour un utilisateur.

Création d'un utilisateur

Utilisez cette fonction pour ajouter un nouvel utilisateur. Après avoir défini vos utilisateurs et vos groupes, vous pouvez ajouter des utilisateurs aux groupes.

1. Cliquez sur **Administrateur du compte** > **Profils** > **Utilisateurs**. Le système affiche l'écran Liste des utilisateurs.
2. Cliquez sur **Créer** dans l'angle supérieur droit de l'écran. Le système affiche l'écran Caractéristiques de l'utilisateur.
3. Saisissez le **Nom d'utilisateur** (nom de connexion de l'utilisateur).
4. Sélectionnez l'**Etat**, selon si vous voulez Activer ou Désactiver l'accès à la console pour cet utilisateur.
5. Saisissez le nom de l'utilisateur (**Prénom** et **Nom**.)

6. Saisissez l'**Adresse électronique** que le système utilisera pour envoyer les notifications d'alerte à l'utilisateur.
7. Saisissez le **Numéro de téléphone** et le **Numéro de télécopie** de l'utilisateur.
8. Sélectionnez les paramètres régionaux de **Langue**, de **Format** et de **Fuseau horaire**.
9. Sélectionnez l'**Etat de l'alerte**, selon si vous voulez Activer ou Désactiver la notification d'alerte pour cet utilisateur. Lorsqu'elle est activée, l'utilisateur reçoit toutes les alertes auxquelles il a été abonné. Lorsqu'elle est désactivée, l'utilisateur ne reçoit pas d'alerte.

   Remarque : La valeur de Abonnés est renseignée par le système.
10. Sélectionnez la **Visibilité de l'abonné** pour que l'utilisateur ne soit visible que pour votre organisation (Local) ou pour qu'il soit visible pour toute la communauté de concentrateur (Global).
11. Cliquez sur **Mot de passe généré automatiquement** pour générer un mot de passe automatiquement. Si vous souhaitez choisir un mot de passe pour cet utilisateur, saisissez-le dans les zones de texte Mot de passe et Entrer de nouveau le mot de passe.
12. Cliquez sur **Sauvegarder**. Pour ajouter des utilisateurs supplémentaires, répétez ces étapes.

Configuration de l'utilisateur FTP

Pour activer l'utilisateur actuel comme utilisateur FTP, procédez comme suit :

1. Cliquez sur **Administrateur du compte** > **Profils** > **Utilisateurs**. Le système affiche l'écran Liste des utilisateurs.
2. Sélectionnez l'utilisateur requis, puis cliquez sur l'icône **Editer**.
3. Cliquez sur **Configuration FTP**.
4. Entrez le **Répertoire de base**, qui est le chemin relatif issu de la valeur spécifiée pour bcg.ftp.config.rootdirectory. Cette zone doit obligatoirement être renseignée.
5. Activez ou désactivez les **Droits en écriture** sur le répertoire de base.
6. Activez ou désactivez les droits en **Création/suppression du répertoire**.
7. Sélectionnez le **Nombre de connexion max.**, qui est le nombre maximal admis pour les connexions simultanées. Si vous sélectionnez Limite personnalisée, entrez cette valeur personnalisée dans la zone de texte.
8. Sélectionnez le **Nombre max. de connexions depuis la même IP**, qui est le nombre maximal de connexions autorisées depuis une même adresse IP. Si vous sélectionnez Limite personnalisée, entrez cette valeur personnalisée dans la zone de texte.
9. Sélectionnez le **Temps d'inactivité maximal**, qui est le temps d'inactivité maximal (en secondes) au bout duquel la connexion utilisateur est abandonnée. Si vous sélectionnez Limite personnalisée, entrez cette valeur personnalisée dans la zone de texte.
10. Sélectionnez le **Chargement max.**, qui est le débit maximal du chargement en octets/sec. Si vous sélectionnez Limite personnalisée, entrez cette valeur personnalisée dans la zone de texte.
11. Sélectionnez le **Téléchargement max.**, qui est le débit maximal du téléchargement en octets/sec. Si vous sélectionnez Limite personnalisée, entrez cette valeur personnalisée dans la zone de texte.
12. Cliquez sur **Sauvegarder**.

Ajout d’utilisateurs aux groupes

1. Cliquez sur **Administrateur du compte** > **Profils** > **Utilisateurs**. Le système affiche l’écran Liste des utilisateurs.
2. Cliquez sur l’icône Afficher les caractéristiques pour visualiser les caractéristiques d’appartenance au groupe de l’utilisateur cible.
3. Cliquez sur l’icône Editer pour éditer les appartenances au groupe de l’utilisateur.
4. Sélectionnez un groupe et cliquez sur **Ajouter au groupe** ou sur **Retirer du groupe** pour ajouter ou retirer un utilisateur du groupe.
5. Cliquez sur l’icône Quitter l’édition une fois l’édition terminée.

Création des informations de contact

Utilisez la fonction Contacts pour créer les informations de contact pour le personnel clé. Ces informations de contact serviront à identifier les personnes qui doivent recevoir une notification lorsque des événements ont lieu et que le système génère des notifications d'alerte.

En fonction de la taille de votre organisation, vous avertirez probablement différents contacts lorsque différents types d'événements auront lieu. Par exemple, lorsque la validation d'un document échoue, le personnel de la sécurité doit en être avisé afin de pouvoir évaluer l'incident. Lorsque les transmissions du partenaire interne dépassent les limites normales, votre administrateur réseau doit être prévenu afin de s'assurer que le système gère efficacement cette augmentation des transmissions.

Après avoir créé vos contacts, retournez dans la fonction Alerte pour relier les contacts appropriés à chaque alerte que vous avez créée.

Pour créer des contacts :

1. Cliquez sur **Administrateur du compte** > **Profils** > **Contacts**. Le système affiche la liste des contacts en cours.
2. Cliquez sur **Créer** dans l'angle supérieur droit de l'écran. Le système affiche l'écran Caractéristiques du contact.
3. Saisissez le **Prénom** et le **Nom** du contact.
4. Saisissez l'**Adresse** du contact.
5. Sélectionnez le **Type de contact** dans la liste déroulante (par exemple, Opportunité B2B ou Opportunité commerciale).
6. Saisissez l'**Adresse électronique** du contact.
7. Saisissez le **Numéro de téléphone** et le **Numéro de télécopie** du contact.
8. Sélectionnez les paramètres régionaux de **Langue**, de **Format** et de **Fuseau horaire**.
9. Sélectionnez l'**Etat de l'alerte**, selon si vous voulez Activer ou Désactiver la notification d'alerte pour ce contact. Lorsqu'elle est activée, l'utilisateur reçoit toutes les alertes auxquelles il a été abonné. Lorsqu'elle est désactivée, le contact ne reçoit pas d'alerte.

   Remarque : La valeur de Abonnés est renseignée par le système.
10. Sélectionnez la **Visibilité de l'abonné** du contact. Si vous sélectionnez Local, le contact ne peut être vu que par votre organisation. Si vous sélectionnez Global, le contact est visible par l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux abonner le contact aux alertes.
11. Cliquez sur **Sauvegarder**. Vous pouvez ajouter un contact à une alerte de différentes manières :

    Pour ajouter un contact à une alerte existante, voir «Ajout d'un contact à une alerte existante», à la page 40.

    Pour créer une alerte basée sur le volume et y ajouter des contacts, voir «Création d'une alerte basée sur le volume», à la page 35.

    Pour créer une alerte basée sur l'événement et y ajouter des contacts, voir «Création d'une alerte basée sur l'événement», à la page 37.

Création d'alertes et ajout de contacts

Pour résoudre rapidement les problèmes, il faut transmettre les informations sur les incidents du système à la bonne personne et au bon moment.

Les alertes de WebSphere Partner Gateway servent à avertir le personnel clé au sujet de fluctuations inhabituelles dans le volume de transmissions que vous recevez, ou lorsque des erreurs de traitement de documents de gestion ont lieu.

Une aide dans le module Afficheur, Afficheur d'événements, vous aide à mieux identifier, diagnostiquer et réparer les erreurs de traitement.

Une alerte consiste en un message envoyé par courrier électronique aux contacts abonnés ou à une liste de distribution du personnel clé. Les alertes sont basée sur l'occurrence d'un événement système (alerte basée sur l'événement) ou sur le volume du flux de documents prévu (alerte basée sur le volume).

- Utilisez une alerte basée sur le volume pour recevoir une notification lors d'une augmentation ou d'une baisse du volume de transmissions.

  Par exemple, si vous êtes un partenaire externe, vous pouvez créer une alerte basée sur le volume qui vous avertit si vous ne recevez aucune transmission du partenaire interne au cours d'un jour ouvrable (sélectionnez Aucun volume pour le Volume, Quotidien pour la fréquence et Lun à Ven pou l'option Jours de la semaine). Cette alerte peut mettre en évidence des difficultés de transmission réseau au niveau du partenaire interne.

  Si vous êtes un partenaire externe, vous pouvez également créer une alerte basée sur le volume pour vous avertir lorsque le nombre de transmissions provenant du partenaire interne dépasse le taux normal. Par exemple, si vous recevez habituellement environ 1000 transmissions par jour, vous pouvez définir le Volume prévu sur 1000 et l'Ecart de pourcentage sur 25%. L'alerte vous avertira lorsque vous recevrez plus de 1250 transmissions par jour (ainsi que lorsque vous recevrez moins de 750 transmissions par jour). Cette alerte peut identifier une demande accrue de la part du partenaire interne, qui peut vous amener, à long terme, à augmenter le nombre de serveurs dans votre environnement.

  Remarquez que les alertes basées sur le volume contrôlent celui-ci en fonction du type de document que vous avez sélectionné au moment où vous avez créé cette alerte. WebSphere Partner Gateway n'examine que les documents contenant le type de document sélectionné dans votre alerte et il ne génère d'alerte que lorsque tous les critères de l'alerte sont remplis.
- Utilisez une alerte basée sur l'événement pour recevoir une notification lorsque des erreurs ont lieu dans le traitement des documents. Par exemple, vous pouvez vouloir créer une alerte pour vous prévenir lorsque le traitement de votre document échoue en raison d'erreurs de validation ou parce que des document ont été reçus en double. Vous pouvez également créer des alertes vous informant lorsqu'un certificat est sur le point d'expirer.

  Vous utiliserez les codes événement prédéfinis par WebSphere Partner Gateway pour créer les alertes basées sur l'événement. Il existe cinq types d'événement : Débogage, Informations, Avertissement, Erreur, Critique. Chaque type d'événement englobe de nombreux événements. Vous pouvez afficher et sélectionner les événement prédéfinis dans l'écran Alerte : Evénements. Par exemple : 240601 Echec de la reprise AS ou 108001 Il ne s'agit pas d'un certificat.

Remarque : Le partenaire externe peut uniquement créer une alerte basée sur le volume concernant le volume de documents envoyés au partenaire interne. Pour pouvoir définir une alerte basée sur le volume de documents qu'il reçoit du partenaire interne, le partenaire externe doit demander à l'administrateur du concentrateur de lui configurer une alerte basée sur le volume, et de le définir comme propriétaire de cette alerte.

Conseil :

- Utilisez une alerte basée sur le volume pour recevoir une notification lorsque le volume de transmission prévu pour le
- partenaire externe ou le partenaire interne descend en dessous des limites d'exploitation. Cette alerte peut mettre en évidence des difficultés de transmission réseau au niveau du partenaire interne ou du partenaire externe.
- Utilisez une alerte basée sur l'événement pour recevoir une notification des erreurs dans le traitement des documents. Par exemple, vous pouvez créer une alerte basée sur l'événement qui vous prévient si le traitement de votre document échoue en raison d'erreurs de validation.

Création d'une alerte basée sur le volume

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche l'écran Recherche d'alerte.
2. Cliquez sur **Créer** dans l'angle supérieur droit de l'écran. Le système affiche l'onglet ce définition des alertes.
3. Sélectionnez **Alerte de volume** comme **Type d'alerte** (il s'agit du paramètre par défaut). Le système affiche les zones de texte appropriées pour une alerte de volume.
4. Saisissez un **Nom d'alerte** pour l'alerte.
5. Sélectionnez un **Partenaire** disposant des droits nécessaires pour créer une alerte basée sur le volume (partenaire interne et administrateur du concentrateur uniquement).
6. Sélectionnez le **Package**, le **Protocole** et le **Type de document** dans les listes déroulantes.

   Le Package, le Protocole et le Type de document sélectionnés doivent correspondre au Package, au Protocole et au Type de document du partenaire externe source.
7. Sélectionnez une des trois options de volume (Prévu, Intervalle ou Aucun volume) puis allez à l'étape 8, à la page 36 :
   - **Prévu** - Sélectionnez Prévu si vous souhaitez qu'une alerte soit générée lorsque le volume du type de document s'écarte d'une quantité précise. Suivez les étapes suivantes pour créer une alerte sur un volume de type de document prévu :
     a. Dans la zone de texte Volume, saisissez le nombre de types de document que vous prévoyez de recevoir durant le laps de temps sélectionné à l'étape 8. Saisissez uniquement un nombre positif : l'alerte ne fonctionnera pas si vous saisissez un nombre négatif.

b. Dans la zone de texte Ecart de pourcentage, saisissez un nombre définissant la limite dans laquelle le volume du flux de documents peut varier sans que l'alerte ne soit activée. Par exemple :
   - Si la zone de texte Volume a pour valeur 20 et que celle d'Ecart de pourcentage a pour valeur 10, un volume de flux de documents inférieur à 18 ou supérieur à 22 déclenchera une alerte.
   - Si la zone de texte Volume a pour valeur 20 et que celle d'Ecart de pourcentage a pour valeur 0, tout volume de flux de documents qui n'est pas égal à 20 déclenchera une alerte.

- **Intervalle**. Sélectionnez Intervalle pour qu'une alerte soit déclenchée si le volume du flux de documents sort d'une intervalle minimale-maximale. Suivez les étapes suivantes pour créer une alerte basée sur une intervalle de valeurs :
  a. Dans la zone de texte Min, saisissez le nombre minimal de types de documents que vous prévoyez de recevoir durant le laps de temps sélectionné à l'étape 8. L'alerte ne sera déclenchée que si le volume du flux de documents descend en dessous de ce nombre.
  b. Dans la zone de texte Max, saisissez le nombre maximal de types de document que vous prévoyez de recevoir durant le laps de temps sélectionné à l'étape 8.

  Remarque : Les zones de texte Min et Max doivent être toutes les deux complétées lors de la création d'une alerte basée sur l'intervalle du volume.
- **Aucun volume**. Sélectionnez Aucun volume pour qu'une alerte soit déclenchée si aucun type de document ne se présente dans le laps de temps défini à l'étape 8.

8. Sélectionnez Quotidien ou Intervalle pour le laps de temps (Fréquence) qui servira au système pour contrôler le volume du flux de documents et générer une alerte le cas échéant.
   - **Quotidien**. Sélectionnez Quotidien pour contrôler le volume du flux de documents sur un ou plusieurs jours ouvrables de la semaine ou du mois. Par exemple, sélectionnez Quotidien si vous voulez contrôler le volume du flux de documents sur un ou plusieurs jours spécifiques de la semaine (par exemple le lundi ou le lundi et le jeudi) ou du mois (par exemple le 1er et le 15 du mois).
   - **Intervalle**. Sélectionnez Intervalle pour contrôler le volume du flux de documents entre deux jours de la semaine ou du mois. par exemple, sélectionnez Intervalle pour contrôler le volume du flux de documents sur tous les jours entre le lundi et le vendredi ou sur tous les jours entre le 5 et le 20 du mois.
9. Sélectionnez l'Heure de début et de fin (journée de 24 heures) du contrôle, par le système, du volume du flux de documents pour les jours sélectionnés dans l'étape suivante. Notez que lorsqu'une fréquence d'Intervalle est sélectionnée, le volume du flux de documents est contrôlé à partir de l'Heure de début du premier jour de l'intervalle jusqu'à l'Heure de fin du dernier jour de l'intervalle.
10. Sélectionnez les jours appropriés de la semaine ou du mois pendant lesquels le contrôle de l'alerte aura lieu. Si vous avez choisi la fréquence Quotidien, sélectionnez les jours ouvrables de la semaine ou les jours du mois pendant lesquels le contrôle de l'alerte aura lieu. Si vous avez choisi la fréquence Intervalle, sélectionnez deux jours de la semaine ou du mois entre lesquels le contrôle de l'alerte aura lieu.

11. Sélectionnez l'**Etat de l'alerte** sur Activé ou Désactivé pour cette alerte.
12. Cliquez sur **Sauvegarder**.
13. Cliquez sur l'onglet **Notification**.
14. Cliquez sur l'icône Editer.
15. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement).
16. Si le contact à ajouter se trouve dans la zone de texte Contacts, sélectionnez-le et cliquez sur **Abonner**. Allez à l'étape 21.

    Si le contact à ajouter ne se trouve pas dans la zone de texte Contacts, cliquez sur **Ajouter une nouvelle entrée aux contacts**. Le système affiche la fenêtre instantanée Création d'un contrat.

    Notez que l'option Ajouter une nouvelle entrée aux contacts est uniquement présentée au Propriétaire de l'alerte pour créer des contacts qui lui sont associés. Cette fonction ne permet pas au Propriétaire de l'alerte d'ajouter des contacts pour les partenaires de l'alerte.
17. Saisissez le nom, l'adresse électronique et les numéros de téléphone et de télécopie du contact.
18. Choisissez l'Etat de l'alerte du contact.
    - Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.
    - Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.
19. Choisissez le niveau de visibilité du contact.
    - Sélectionnez **Local** pour que ce contact soit vu uniquement par votre organisation.
    - Sélectionnez **Global** pour que ce contact soit visible par l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux abonner le contact aux alertes.
20. Cliquez sur **Sauvegarder** pour sauvegarder le contact ; cliquez sur **Sauvegarder & Abonner** pour ajouter le contact à la liste des contacts pour cette alerte.
21. Cliquez sur **Sauvegarder**.

Remarque : Les modifications effectuées sur les alertes basées sur le volume après la période de contrôle originale prennent effet à la période de contrôle suivante. Par exemple : une alerte effectue un contrôle entre 13h et 15h tous les mercredis et jeudis. Un mercredi à 16h, l'alerte est modifiée de façon à effectuer son contrôle entre 17h et 19h. L'alerte n'effectuera pas de contrôle le jour même : la modification prendra effet le jeudi suivant.

Création d'une alerte basée sur l'événement

Remarque : Le serveur e-mail d'alerte doit être configuré. Reportez-vous au *Guide d'administration* pour la configuration du serveur e-mail d'alerte

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche l'écran Recherche d'alerte.
2. Cliquez sur **Créer** dans l'angle supérieur droit de l'écran. Le système affiche l'onglet ce définition des alertes.
3. Sélectionnez **Alerte d'événement** comme **Type d'alerte**. Le système affiche les zones de texte appropriées pour une alerte basée sur l'événement.

4. Saisissez un **Nom d'alerte** pour l'alerte. Il sera votre identifiant pour cette alerte.
5. Sélectionnez un **Partenaire** qui déclenchera l'alerte (cette option n'est disponible que pour le partenaire interne et l'administrateur du concentrateur).

   Sélectionnez l'option Tout partenaire pour associer l'alerte à tous les partenaires du système. Lorsque vous effectuez une recherche d'alerte et que vous sélectionnez Tout partenaire comme partenaire de l'alerte, le système affiche toutes les alertes qui ne sont pas associées à un partenaire spécifique.
6. Sélectionnez le **Package**, le **Protocole** et le **Type de document** dans les listes déroulantes.
7. Sélectionnez le type d'événement : Débogage, Informations, Avertissement, Erreur, Critique ou Tout. Ce filtre restreint le nombre d'événements affichés dans la liste Nom de l'événement.
8. Sélectionnez l'événement qui activera l'alerte, par exemple : BCG240601 Echec de la reprise AS ou 108001 Il ne s'agit pas d'un certificat. Pour créer une alerte qui vous informe lorsqu'un certificat est sur le point d'expirer, sélectionnez une des propositions suivantes :
   - BCG108005 Le certificat expire dans 60 jours
   - BCG108006 Le certificat expire dans 30 jours
   - BCG108007 Le certificat expire dans 15 jours
   - BCG108008 Le certificat expire dans 7 jours
   - BCG108009 Le certificat expire dans 2 jours
9. Sélectionnez l'état de cette alerte : Activé ou Désactivé.
10. Cliquez sur **Sauvegarder**.
11. Cliquez sur l'onglet **Notification**.
12. Cliquez sur l'icône Editer.
13. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement).
14. Si le contact à ajouter se trouve dans la zone de texte Contacts, sélectionnez-le et cliquez sur **Abonner**. Allez à l'étape 19.

    Si le contact à ajouter ne se trouve pas dans la zone de texte Contacts, cliquez sur **Ajouter une nouvelle entrée aux contacts**. Le système affiche la fenêtre instantanée Création d'un contrat.

    Notez que l'option Ajouter une nouvelle entrée aux contacts est uniquement présentée au Propriétaire de l'alerte pour créer des contacts qui lui sont associés. Cette fonction ne permet pas au Propriétaire de l'alerte d'ajouter des contacts pour les partenaires de l'alerte.
15. Saisissez le nom, l'adresse électronique et les numéros de téléphone et de télécopie du contact. Seule l'adresse électronique est utilisée pour l'envoi des alertes. Les autres entrées n'ont qu'un but informatif.
16. Choisissez l'Etat de l'alerte du contact.
    - Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.
    - Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.
17. Choisissez le niveau de visibilité du contact.
    - Sélectionnez **Local** pour que ce contact soit vu uniquement par votre organisation.

- Sélectionnez **Global** pour que ce contact soit visible par l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux abonner le contact aux alertes.

18. Cliquez sur **Sauvegarder** pour sauvegarder le contact. Cliquez sur **Sauvegarder et abonner** pour sauvegarder le contact et l'ajouter à la liste des contacts pour cette alerte.
19. Sélectionnez le Mode de distribution :
    - **Envoi d'alertes immédiat**. Lorsque vous sélectionnez cette option, le système envoie des notifications d'alerte au contact au moment ou l'alerte se déclenche. Utilisez cette option pour les alertes critiques.
    - **Alertes de lot par**. Lorsque vous sélectionnez cette option, vous pouvez préciser à quel moment vous souhaitez que le contact reçoive la notification d'alerte. Utilisez cette option pour les alertes qui ne sont pas critiques.

      Les deux options de cette section, Nombre et Heure, ne s'excluent pas mutuellement.

      Si vous sélectionnez l'option Nombre, vous devez toujours sélectionner l'option Heure.

      – Si nombre d'alertes (Nombre) est atteint pendant le délai que vous avez sélectionné (Heure), le système génère une notification d'alerte.

      – Si une alerte a lieu mais que le nombre d'alertes (Nombre) n'est pas atteint pendant le délai que vous avez sélectionné (Heure), le système générera une notification d'alerte à la fin du délai.

      L'option Heure peut être utilisée sans l'option Nombre, mais cette dernière doit toujours être associée à un délai (Heure).

      – **Nombre**. Vous devez aussi utiliser l'option Heure lorsque vous sélectionnez cette option. Saisissez un nombre (n). C'est le nombre d'alertes qui doivent avoir lieu pendant le délai sélectionné (Heure) pour que le système envoie une notification d'alerte au contact de l'alerte.

        Voici un exemple de la manière dont ces deux options fonctionnent ensemble :

        Dans notre exemple, les options Alertes de lot par se voient affecter la valeur de 10 pour le Nombre (10 alertes) et de 2 pour l'Heure (délai de 2 heures). Le système conserve toutes les notifications pour cette alerte jusqu'à ce que 10 alertes aient lieu dans un délai de 2 heures ou bien jusqu'à ce que la fin du délai soit atteint.

        Lorsque le nombre de 10 alertes est atteint dans un délai de 2 heures, le système envoie toutes les notifications d'alerte au contact.

        Si une alerte a lieu mais que le nombre de 10 alertes n'est pas atteint pendant le délai (2 heures), le système enverra une notification d'alerte au contact à la fin du délai.

      – **Heure**. Sélectionnez le nombre d'heures (n). Le système conserve la notification d'alerte pendant n heures. Toutes les n heures, le système envoie toutes les notifications conservées au contact.

        Par exemple, si vous tapez 2, le système conserve toutes les notifications pour cette alerte qui ont lieu dans chaque intervalle de deux heures. Lorsque l'intervalle de 2 heures est expirée, le système envoie toutes les notifications d'alerte au contact.
20. Cliquez sur **Sauvegarder**.

Ajout d'un contact à une alerte existante

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche l'écran Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et saisissez le Nom de l'alerte.
3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.
4. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques des alertes.
5. Cliquez sur l'icône Editer pour éditer les caractéristiques d'une alerte.
6. Cliquez sur l'onglet **Notification**.
7. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement).
8. Si le contact à ajouter se trouve dans la zone de texte Contacts, sélectionnez-le et cliquez sur **Abonner**. Allez à l'étape 13.

   Si le contact à ajouter ne se trouve pas dans la zone de texte Contacts, cliquez sur **Ajouter une nouvelle entrée aux contacts**. Le système affiche la fenêtre instantanée Création d'un contrat.

   Notez que l'option Ajouter une nouvelle entrée aux contacts est uniquement présentée au Propriétaire de l'alerte pour créer des contacts qui lui sont associés. Cette fonction ne permet pas au Propriétaire de l'alerte d'ajouter des contacts pour les partenaires de l'alerte.
9. Saisissez le nom, l'adresse électronique et les numéros de téléphone et de télécopie du contact.
10. Choisissez l'Etat de l'alerte du contact.
    - Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.
    - Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.
11. Choisissez le niveau de visibilité du contact.
    - Sélectionnez **Local** pour que ce contact soit vu uniquement par votre organisation.
    - Sélectionnez **Global** pour que ce contact soit visible par l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux abonner le contact aux alertes.
12. Cliquez sur **Sauvegarder** pour sauvegarder le contact. Cliquez sur **Sauvegarder et abonner** pour sauvegarder le contact et l'ajouter à la liste des contacts pour cette alerte.
13. Cliquez sur **Sauvegarder**.

Création d'une adresse

Utilisez cette fonction pour créer les adresses dans votre profil de partenaire. Le système est configuré pour prendre en charge plusieurs types d'adresses pour des emplacements de Société, de Facturation et de Technique.

Pour créer une adresse :

1. Cliquez sur **Administrateur du compte** > **Profils** > **Adresses**. Le système affiche l'écran Adresses.

2. Cliquez sur **Création d'une adresse** dans l'angle supérieur droit de l'écran. Le système affiche l'écran Adresses.
3. Sélectionnez le Type d'adresse dans la liste déroulante (Facturation, Société ou Technique).
4. Saisissez l'adresse dans les zones de texte appropriées.
5. Cliquez sur **Sauvegarder**.

Chapitre 3. Création de destinations

Les destinations définissent des points d'entrée dans le système. Ce chapitre indique les étapes à suivre pour créer des destinations et contient les rubriques suivantes :

Présentation

WebSphere Partner Gateway fait appel à des destinations pour acheminer les documents jusqu'à leur destination. Le destinataire peut être un partenaire externe ou le partenaire interne. Le protocole de transport sortant détermine les informations utilisées pendant la configuration des destinations.

Les transports suivants sont pris en charge (par défaut) pour les destinations des partenaires :

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

  Remarque : Vous pouvez définir une destination SMTP pour des partenaires externes uniquement (pas pour le partenaire interne).
- Répertoire de fichiers
- Scripts FTP

Vous pouvez également indiquer un type de transport défini par l'utilisateur, que vous chargez lors de la création de la destination.

Configuration d'une destination HTTP

La configuration d'une destination HTTP permet d'envoyer des documents depuis le concentrateur aux adresses IP des partenaires. Lorsque vous configurez une destination HTTP, vous pouvez également demander que les documents soient envoyés via un serveur proxy configuré.

Pour commencer à créer une destination HTTP, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page **Liste des destinations**, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire. Il s'agit du nom qui apparaîtra dans la liste des destinations.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. A titre facultatif, vous pouvez sélectionner un serveur proxy à utiliser. La **liste de proxy directs** répertorie tous les serveurs proxy que vous avez créés, y compris le serveur proxy par défaut. La valeur par défaut pour cette zone **Utiliser le serveur proxy par défaut**. Si vous souhaitez que le partenaire sélectionné emploie un autre serveur proxy, sélectionnez celui-ci dans la liste. Si vous ne souhaitez pas utiliser cette option pour le partenaire sélectionné, sélectionnez **Ne pas utiliser de proxy direct**.
2. Sélectionnez **HTTP/1.1** dans la liste **Transport**.
3. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est le suivant : http://*<nom_serveur>*:*<port_facultatif>*/*<chemin_accès>*

   Exemple :

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

   Lorsque vous configurez une destination utilisée par un service Web, précisez l'adresse URL privée indiquée par le fournisseur du service Web. Il s'agit du point où WebSphere Partner Gateway appelle le Service Web lorsqu'il se comporte comme un proxy pour le fournisseur de Service Web.
4. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur HTTP le nécessite.
5. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
8. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
9. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous souhaitez que la destination soit mise hors ligne (automatiquement) lorsqu'un

incident de livraison est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

Lorsque vous sélectionnez l'option **Mise en file d'attente automatique**, tous les documents restent dans la file d'attente jusqu'à ce que la destination soit mise en ligne manuellement.

10. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
11. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination HTTPS

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

Pour créer des destinations HTTPS, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page Liste des destinations, exécutez les étapes suivantes :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. Sélectionnez **HTTPS/1.0** ou **HTTPS/1.1** dans la liste **Transport**.La configuration de la destination HTTP/S ne comprend pas la configuration du proxy direct.
2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est le suivant : https://<*nom_serveur*>:<*port_facultatif*>/<*chemin_accès*>

   Par exemple :

   `https://autre_serveur.ibm.com:57443/bcgreceiver/Receiver`
3. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur HTTP sécurisé le nécessite.
4. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
8. Dans la zone **Validation du certificat SSL du client**, sélectionnez **Oui** pour que le certificat numérique du partenaire expéditeur soit validé en fonction du numéro business associé au document. La valeur par défaut est **Non**.
9. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous souhaitez que la destination soit mise hors ligne (automatiquement) lorsqu'un incident de livraison est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option **Mise en file d'attente automatique**, tous les documents restent dans la file d'attente jusqu'à ce que la destination soit mise en ligne manuellement.
10. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
11. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination FTP

Pour créer une destination FTP, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page Caractéristiques des destinations, procédez comme suit :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. Sélectionnez **FTP** dans la liste **Transport**.
2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est le suivant : ftp://<*nom_serveur_ftp*>:<*n°_port*>

   Par exemple :

   `ftp://serveur_ftp_1.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, si l'accès au serveur FTP le nécessite.
4. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous souhaitez que la destination soit mise hors ligne (automatiquement) lorsqu'un incident de livraison est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option **Mise en file d'attente automatique**, tous les documents restent dans la file d'attente jusqu'à ce que la destination soit mise en ligne manuellement.
9. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
10. Dans la zone **Utiliser un nom de fichier unique**, laissez la case cochée si nécessaire. Sinon, décochez-la. Si vous sélectionnez **Utiliser un nom de fichier unique**, le nom d'origine du fichier sera stocké dans la base de données.
11. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination SMTP

Pour créer une destination SMTP, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page Liste des destinations, exécutez les étapes suivantes :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. Sélectionnez **SMTP** dans la liste **Transport**.

2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est le suivant: mailto:<*utilisateur@nom_serveur*>

   Par exemple :

   `mailto:admin@autre_serveur.ibm.com`
3. Entrez éventuellement un nom d'utilisateur et un mot de passe, si l'accès au serveur SMTP le nécessite.
4. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous souhaitez que la destination soit mise hors ligne (automatiquement) lorsqu'un incident de livraison est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option **Mise en file d'attente automatique**, tous les documents restent dans la file d'attente jusqu'à ce que la destination soit 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. La valeur par défaut est **Non**.
10. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination JMS

Pour créer des destinations JMS, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page Liste des destinations, exécutez les étapes suivantes :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. Sélectionnez **JMS** dans la liste **Transport**.
2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

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

   `file:///<chemin_liaisons_JNDI_MQ_défini_utilisateur>`

   Par 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. Cette zone est obligatoire.
3. Indiquez éventuellement un nom d'utilisateur et un mot de passe JMS, s'ils sont requis pour accéder à la file d'attente JMS.
4. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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**, entrez le nombre de documents pouvant être traités simultanément. La valeur par défaut est 3.
7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous souhaitez que la destination soit mise hors ligne (automatiquement) lorsqu'un incident de livraison est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option **Mise en file d'attente automatique**, tous les documents restent dans la file d'attente jusqu'à ce que la destination soit 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. La valeur par défaut est **Non**.
10. Dans la zone **Nom de la fabrique JMS**, saisissez le nom de la classe Java utilisée par le fournisseur JMS pour se connecter à la file d'attente JMS. Cette zone est obligatoire.
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 est obligatoire.
12. Dans la zone **Type de message JMS**, entrez le type de message. Cette zone est facultative.
13. Dans la zone **Packages de l'URL fournisseur**, entrez le nom des classes (ou du fichier JAR) utilisé par Java pour comprendre l'URL de contexte JMS. Cette zone est facultative. Si vous ne définissez pas de valeur, le chemin au fichier de liaisons est utilisé.
14. Dans la zone **Nom de file d'attente JMS**, entrez le nom de la file d'attente vers laquelle les documents doivent être envoyés. Cette zone est obligatoire.

15. Dans la zone **Nom de la fabrique du JNDI du JMS**, entrez le nom de la fabrique utilisé pour la connexion au service annuaire. Cette zone est obligatoire.
16. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination fichier-répertoire

Pour créer des destinations fichier-répertoire, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page Liste des destinations, exécutez les étapes suivantes :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. Sélectionnez **Répertoire de fichiers** dans la liste **Transport**.
2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Pour les systèmes UNIX et Windows dans lesquels le répertoire de fichiers et WebSphere Business Integration Connect sont situés sur la même unité, le format est le suivant : file:///<chemin_accès_répertoire_cible>

   Par exemple :

   ```
   file:///répertoire_fichier_local
   ```

   où *répertoire_fichier_local* 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 le suivant : file:///<lettre_unité>:/<chemin_accès>
3. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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 devant être traités simultanément. La valeur par défaut est 3.
6. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
7. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous souhaitez que la destination soit mise hors ligne (automatiquement) lorsqu'un

incident de livraison est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

Lorsque vous sélectionnez l'option **Mise en file d'attente automatique**, tous les documents restent dans la file d'attente jusqu'à ce que la destination soit mise en ligne manuellement.

8. Dans la zone **Utiliser un nom de fichier unique**, laissez la case cochée si nécessaire. Sinon, décochez-la. Si vous sélectionnez **Utiliser un nom de fichier unique**, le nom d'origine du fichier sera stocké dans la base de données.
9. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination FTPS

Pour créer des destinations FTPS, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page Liste des destinations, exécutez les étapes suivantes :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. Sélectionnez **FTPS** dans la liste **Transport**.
2. Dans la zone **Adresse**, entrez l'URI correspondant à l'emplacement de livraison du document. Cette zone est obligatoire.

   Le format est le suivant : ftp://<*nom_serveur_ftp*>:<*n°_port*>

   Par exemple :

   `ftp://serveur_ftp_1.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, si l'accès au serveur FTP sécurisé le nécessite.
4. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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 devant être traités simultanément. La valeur par défaut est 3.

7. Dans la zone **Validation de l'IP du client**, sélectionnez **Oui** si vous souhaitez que l'adresse IP de l'expéditeur soit validée avant que le document ne soit traité. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.
8. Dans la zone **Mise en file d'attente automatique**, sélectionnez **Oui** si vous souhaitez que la destination soit mise hors ligne (automatiquement) lorsqu'un incident de livraison est sur le point de se produire du fait que le nombre de relances est épuisé. Dans le cas contraire, sélectionnez **Non**. La valeur par défaut est **Non**.

   Lorsque vous sélectionnez l'option **Mise en file d'attente automatique**, tous les documents restent dans la file d'attente jusqu'à ce que la destination soit mise en ligne manuellement.
9. Dans la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.
10. Dans la zone **Utiliser un nom de fichier unique**, laissez la case cochée si nécessaire. Sinon, décochez-la. Si vous sélectionnez **Utiliser un nom de fichier unique**, le nom d'origine du fichier sera stocké dans la base de données.
11. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination de script FTP

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

Création du script FTP

Pour utiliser une destination de script FTP, vous devez créer un fichier incluant toutes les commandes FTP requises et pouvant être acceptées par votre serveur FTP.

1. Créez un script pour les destinations de façon à indiquer les actions que vous souhaitez effectuer. Le script suivant est un exemple permettant de se connecter au serveur FTP indiqué (à l'aide du nom et du mot de passe spécifiés), d'accéder au répertoire indiqué sur le serveur FTP et d'envoyer tous les fichiers vers le répertoire spécifié sur le serveur.

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

   Lorsque la destination est mise en service, les paramètres fictifs (par exemple %BCGSERVERIP%) sont remplacés par les valeurs saisies lors de la création d'une instance spécifique d'une destination de script FTP, comme indiqué dans le tableau suivant :

Tableau 3. Mappage des paramètres de script et des informations des zones de destination de script FTP

Paramètre de script	Informations des zones de la destination de script FTP
%BCGSERVERIP%	IP serveur
%BCGUSERID%	ID utilisateur
%BCGPASSWORD%	Mot de passe

Tableau 3. Mappage des paramètres de script et des informations des zones de destination de script FTP (suite)

Paramètre de script	Informations des zones de la destination de script FTP
%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, binary ou passive) vers le serveur FTP.

- cd

  Cette commande permet de passer au répertoire indiqué.

- delete

  Cette commande supprime un fichier du serveur FTP.

- mkdir

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

- mput

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

- open

  Cette commande comprend 3 paramètres ; l'adresse IP du serveur FTP, le nom d'utilisateur, et le mot de passe. Ces paramètres mappent respectivement vers les variables %BCGSERVERIP% %BCGUSERID% et %BCGPASSWORD%. La ligne de votre script de cible FTP doit prendre la forme suivante :`open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%`.

- quit, bye

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

- quote

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

- rmdir

  Cette commande permet de supprimer un répertoire du serveur FTP.

- site

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

Destinations de script FTP

Si vous pensez utiliser des destinations de script FTP, effectuez les tâches suivantes :

Pour créer des destinations de script FTP, appliquez la procédure suivante.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.

Caractéristiques des destinations

Depuis la page Liste des destinations, exécutez les étapes suivantes :

1. Entrez un nom pour identifier la destination. Cette zone est obligatoire.
2. Indiquez éventuellement l'état de la destination. L'état par défaut est **Activé**. Une destination activée est prête à envoyer des documents. Une destination désactivée ne peut pas envoyer de documents.
3. Indiquez éventuellement si la destination est en ligne ou hors ligne. La valeur par défaut est **En ligne**.
4. Entrez éventuellement une description de la destination.

Configuration de la destination

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

1. Sélectionnez **Scripts FTP** dans la liste **Transport**.
2. Entrez l'adresse IP du serveur FTP auquel vous envoyez 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 le **Mode FTPS**. Sinon, cliquez sur **Non**.
5. Chargez le fichier script en procédant comme suit :
   a. Cliquez sur **Charger un fichier script**.
   b. Entrez le nom du fichier contenant le script de traitement des documents ou cliquez sur **Parcourir** pour accéder au fichier.
   c. Cliquez sur **Charger un fichier** pour charger le fichier script dans la zone de saisie **Fichier script actuellement chargé**.
   d. Si le fichier script est celui que vous souhaitez utiliser, cliquez sur **Sauvegarder**.
   e. Cliquez sur **Fermer la fenêtre**.
6. Dans la zone **Nombre de relances**, indiquez le nombre de tentatives que la destination doit effectuer pour envoyer un document avant que l'opération n'échoue. 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 la zone **Délai de connexion**, indiquez le nombre de secondes durant lesquelles une connexion peut rester ouverte en l'absence de trafic. La valeur par défaut est 120 secondes.

9. Dans la zone **Verrouiller l'utilisateur**, indiquez si la destination demandera un verrouillage pour qu'aucune autre instance d'une destination de script FTP ne puisse accéder simultanément au même répertoire du serveur FTP.

Attributs définis par l'utilisateur

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

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

Prenons un exemple de script FTP :

```
Open %BCGSERVERIP% %BCGUSERID% %BCGPASSWORD%
          cd %BCGOPTION1%
          mput *
          quit
```

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

Planification

Depuis la section Planification de la page, exécutez les étapes suivantes :

1. Indiquez si vous souhaitez procéder à une planification en fonction d'un intervalle ou du calendrier.
   - Si vous avez sélectionné **Planification en fonction de l'intervalle**, sélectionnez le nombre de secondes qui doivent s'écouler avant que la destination ne soit interrogée (ou acceptez la valeur par défaut).
   - Si vous sélectionnez **Planification en fonction du calendrier**, choisissez le type de planification (**Planification quotidienne**, **Planification hebdomadaire**, ou **Planification personnalisée**).
     - Si vous avez sélectionné **Planification quotidienne**, choisissez l'heure de la journée à laquelle la destination doit être interrogée.
     - Si vous sélectionnez **Planification hebdomadaire**, choisissez un ou plusieurs jours de la semaine, en plus de l'heure.
     - Si vous sélectionnez **Planification personnalisée**, choisissez l'heure de la journée puis **Intervalle** ou **Sélection des jours** pour indiquer la semaine et le mois. Dans **Intervalle**, indiquez une date de début et de fin. Vous pouvez, par exemple, cliquer sur **Lun** et **Ven** si vous souhaitez que le serveur soit interrogé à une certaine heure uniquement les jours ouvrés. L'option **Sélection des jours** permet de choisir certains jours de la semaine ou du mois.
2. Si vous voulez configurer l'étape Traitement préalable ou Traitement ultérieur de la destination, voir «Configuration de gestionnaires», à la page 56. Sinon, cliquez sur **Sauvegarder**.

Configuration de gestionnaires

Vous pouvez modifier deux points de traitement pour une destination - Traitement préalable et Traitement ultérieur.

Aucun gestionnaire n'est fourni par défaut pour l'étape Traitement préalable ou Traitement ultérieur, par conséquent, aucun gestionnaire n'est répertorié par défaut dans la **Liste disponibles**. Si vous avez chargé un gestionnaire, vous pouvez le sélectionner et le déplacer vers la **Liste configurés**.

Pour appliquer un gestionnaire écrit par l'utilisateur pour ces paramètres de configuration, vous devez d'abord charger le gestionnaire. Pour obtenir les instructions permettant de charger un gestionnaire, reportez-vous au *Guide de configuration du concentrateur*. Ensuite, procédez comme suit :

1. Sélectionnez **Traitement préalable** ou **Traitement ultérieur** dans la liste **Gestionnaires des paramètres de configuration**.
2. Sélectionnez un gestionnaire dans la **Liste des éléments disponibles** et cliquez sur **Ajouter**.
3. Si vous souhaitez modifier les attributs du gestionnaire, sélectionnez-le dans la **Liste des éléments configurés** et cliquez sur **Configurer**. La liste des attributs pouvant être modifiés s'affiche. Effectuez les modifications nécessaires et cliquez sur **Définir les valeurs**.
4. Cliquez sur **Sauvegarder**.

Vous pouvez modifier davantage la **Liste des éléments configurés** de la façon suivante :

- Supprimez un gestionnaire en le sélectionnant dans la **Liste des éléments configurés** et cliquez sur **Retrait**. Le gestionnaire est déplacé vers la **Liste des éléments disponibles**.
- Modifiez l'ordre dans lequel les gestionnaires sont traités en le sélectionnant et en cliquant sur **Déplacer vers le haut** ou **Déplacer vers le bas**.

Spécification d'une destination par défaut

Après avoir créer des destinations pour le partenaire interne ou le partenaire externe, sélectionnez l'une des destinations comme destination par défaut.

1. Cliquez sur **Administrateur du compte > Profils > Destinations**.
2. Cliquez sur **Créer**.
3. Cliquez sur **Afficher les destinations par défaut**.

   La liste des destinations définies pour le partenaire s'affiche.
4. Dans la liste **Production**, sélectionnez la destination par défaut de ce partenaire. Vous pouvez également définir des destinations par défaut pour d'autres types de destinations, **Test** par exemple.
5. Cliquez sur **Sauvegarder**.

Chapitre 4. Gestion des connexions de la communauté et des utilisateurs : Administrateur du compte

Les fonctions du module de l'Administrateur du compte contrôlent par qui et comment WebSphere Partner Gateway est utilisé.

Par exemple, vous pouvez contrôler l'accès à la Console de communauté et à chacune de ses fonctions. Vous pouvez choisir les personnes qui reçoivent les alertes lorsque des événements importants surviennent. Voici des exemples d'événements : Connexion du Partenaire introuvable, Erreur de validation RosettaNet et Echec de la sortie du document.

Vous utiliserez aussi ce module pour gérer votre profil de partenaire, les certificats, les destinations, les utilisateurs, les groupes, les contacts, les adresses, les alertes et les fonctions B2B. (Les fonctions B2B définissent les types de processus métier que votre système peut envoyer et recevoir). Si vous avez participé au processus de configuration, vous êtes déjà familiarisé avec ces fonctions.

Tableau 4. Fonctions de l'Administrateur du compte

Quelle fonction voulez-vous utiliser ?
«Gestion des destinations»
«Gestion des certificats», à la page 59
«Gestion de groupes», à la page 59
«Gestion des utilisateurs», à la page 61
«Gestion des contacts», à la page 63
«Gestion des alertes», à la page 64
«Gestion des adresses», à la page 66

Gestion des destinations

Utilisez la fonction Destinations pour afficher les informations sur les destinations utilisées pour acheminer les documents vers leur destination. Vous pouvez afficher l'URI cible, le protocole de transport et l'état de la destination à partir de cette fonction.

Avertissement : Certaines valeurs de la destination dépendent du protocole de transport sélectionné. Les restrictions sont notées dans les procédures et le tableau des valeurs.

Affichage d'une liste de destinations

Cliquez sur **Administrateur de compte** > **Profils** > **Destinations** pour afficher une liste des destinations du système.

Affichage ou édition des caractéristiques de la destination

Important : Si vous désactivez une destination, vous désactivez également la connexion du partenaire associé à la destination. La destination ne fonctionnera pas. Si vous la mettez la destination hors ligne, les documents se mettront en file d'attente jusqu'à ce qu'elle soit remise en ligne.

1. Cliquez sur **Administrateur du compte** > **Profils** >**Destinations**. Le système affiche l'écran Liste des destinations.
2. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques des destinations.
3. Cliquez sur l'icône Editer pour éditer les caractéristiques d'une destination.
4. Editez les informations si nécessaire. Le tableau suivant décrit les valeurs des destinations.

Tableau 5. Valeurs sur l'écran des destinations

Valeur	Description
Nom de la destination	Nom de la destination. Remarque : Nom de la destination est une zone à format libre définie par l'utilisateur. Les utilisateurs sont invités à utiliser des noms différents pour les différentes destinations, afin d'éviter une confusion potentielle.
Transport	Protocole utilisé pour acheminer les documents.
URI cible	Identificateur URI de la destination.
En ligne ou Hors ligne	Si elle est hors ligne, les documents sont mis en file d'attente jusqu'à ce que la destination soit en ligne.
Etat	Activé ou Désactivé. Le traitement des documents acheminés par une destination désactivée échoue.
Valeur par défaut	Identifie la destination par défaut.

5. Cliquez sur **Sauvegarder**.

Affichage, sélection ou édition de vos destinations par défaut

1. Cliquez sur **Administrateur du compte** > **Profils** >**Destinations**. Le système affiche l'écran Liste des destinations.
2. Cliquez sur **Afficher les destinations par défaut** dans l'angle supérieur droit de l'écran. Le système affiche l'écran Liste des destinations par défaut.
3. Utilisez les listes déroulantes pour sélectionner ou modifier une ou plusieurs destinations par défaut.
4. Cliquez sur **Sauvegarder**.

Affichage de la destination Emplacement d'utilisation

Pour afficher les caractéristiques concernant l'emplacement d'utilisation d'une destination, procédez comme suit :

1. Cliquez sur **Administrateur du compte** > **Profils** > **Destinations**
2. Dans la liste des destinations, cliquez sur l'icône **Emplacement d'utilisation** en regard de la destination souhaitée. La liste de tous les emplacements où la destination sélectionnée est utilisée s'affiche.

   Remarque : Cet écran comporte des informations de pagination car le nombre de canaux utilisant cette destination peut être élevé. Chaque page comportera 10 connexions maximum.

Suppression de la destination

La fonction de suppression des destinations est disponible pour toutes les destinations à l'exception de la destination par défaut. Pour supprimer une destination, procédez comme suit :

1. Cliquez sur **Administrateur du compte** > > **Profils** >**Destinations**.

2. Dans la liste des destinations, cliquez sur l'icône **Supprimer** en regard de la destination à supprimer.

   Remarque : Cette icône n'est pas disponible pour la destination par défaut. C'est pourquoi l'opération de suppression est uniquement autorisée si la destination sélectionnée n'est pas utilisée au niveau des connexions. Pour toute information concernant l'utilisation des destinations, voir «Affichage de la destination Emplacement d'utilisation», à la page 58.

3. Cliquez sur **OK** dans la fenêtre d'avertissement pour confirmer la suppression.

Gestion des certificats

Cette section indique les étapes à suivre pour afficher, éditer et supprimer les certificats numériques à l'aide de la Console de communauté.

Affichage et édition des caractéristiques du certificat numérique

1. Cliquez sur **Administrateur du compte** > **Profils** > **Certificats**. Le système affiche la liste des certificats numériques existants.
2. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques des certificats. Le système affiche l'écran Caractéristiques du certificat.
3. Cliquez sur l'icône Editer pour éditer le certificat.
4. Editez si nécessaire.
5. Cliquez sur **Sauvegarder**.

Désactivation d'un certificat numérique

1. Cliquez sur **Administrateur du compte** > **Profils** > **Certificats**. Le système affiche l'écran Liste des certificats.
2. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques des certificats. Le système affiche l'écran Caractéristiques du certificat.
3. Cliquez sur l'icône Editer pour éditer le certificat.
4. Cliquez sur **Désactivé**.
5. Cliquez sur **Sauvegarder**.

Gestion de groupes

Vous pouvez afficher, éditer et supprimer des groupes à l'aide de la Console de communauté. Cette fonction est uniquement disponible pour les utilisateurs des partenaires internes/externes du groupe administrateur.

Affichage des appartenances au groupe et attribution des utilisateurs aux groupes

1. Cliquez sur **Administrateur du compte** > **Profils** > **Groupes**. Le système affiche l'écran Liste des groupes.

Tableau 6. Valeurs sur l'écran Liste des groupes

Valeur	Description
Nom	Nom du groupe.
Description	Description du groupe.
Type de groupe	Type, par exemple Système.

2. Cliquez sur l'icône Afficher les membres pour visualiser la liste des membres d'un groupe. Si cette icône n'apparaît pas, cela signifie qu'il n'y a aucun membre dans ce groupe. Cliquez sur Appartenances dans le sous-menu.
3. Cliquez sur l'icône Editer pour éditer les utilisateurs appartenant à un groupe.
4. Cliquez sur **Ajouter au groupe** pour affecter des utilisateurs au groupe.
5. Cliquez sur l'icône Quitter l'édition pour enregistrer et quitter.

Affichage, édition ou attribution des droits d'accès du groupe

Les droits d'accès du groupe pour les utilisateurs et les groupes ne peuvent pas être définis par un utilisateur du groupe administrateur. Les droits d'accès des autres groupes peuvent toujours être inférieurs ou égaux à ceux de l'administrateur. Par exemple, si l'administrateur a un droit d'accès en lecture seule pour Adresse, le droit d'accès des autres groupes peut être ″pas d'accès″ ou ″lecture seule″.

1. Cliquez sur **Administrateur du compte** > **Profils** > **Groupes**. Le système affiche l'écran Liste des groupes.
2. Cliquez sur l'icône Afficher les autorisations pour visualiser les droits d'accès d'un groupe. Le système affiche la liste des droits d'accès du groupe sélectionné.
3. Sélectionnez **Pas d'accès**, **Lecture seule,** ou **Lecture/Ecriture** pour chaque fonction.
4. Cliquez sur **Sauvegarder**.

Affichage ou édition des caractéristiques du groupe

1. Cliquez sur **Administrateur du compte** > **Profils** > **Groupes**. Le système affiche l'écran Liste des groupes.
2. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques du groupe (Nom et Description). Le système affiche l'écran Caractéristiques du groupe.
3. Cliquez sur l'icône Editer pour éditer les caractéristiques du groupe (il n'est pas possible d'éditer les groupes générés par le système).
4. Editez si nécessaire.
5. Cliquez sur **Sauvegarder**.

Restrictions : Le groupe Administrateur et le groupe par défaut sont générés par le système et ne peuvent être édités ou supprimés. L'Administrateur du concentrateur dispose d'un groupe supplémentaire, Administrateur du concentrateur.

Suppression d'un groupe

1. Cliquez sur **Administrateur du compte** > **Profils** > **Groupes**. Le système affiche l'écran Liste des groupes.
2. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques du groupe. Le système affiche l'écran Caractéristiques du groupe.
3. Cliquez sur l'icône Editer pour éditer les caractéristiques du groupe<
4. Cliquez sur **Supprimer**. Confirmez la suppression.

Avertissement : Le groupe Administrateur et le Groupe par défaut sont générés par le système et ne peuvent pas être édités ou supprimés.

Gestion des utilisateurs

Utilisez cette fonction pour afficher et éditer des profils de partenaires. Cette fonction est uniquement disponible pour les utilisateurs des partenaires internes / externes du groupe administrateur.

Remarque : Vous pouvez utiliser cette fonction pour attribuer ou créer automatiquement un nouveau mot de passe pour un utilisateur.

1. Cliquez sur **Administrateur du compte** > **Profils** > **Utilisateurs**. Le système affiche l'écran Liste des utilisateurs.

   Le tableau suivant décrit les valeurs sur l'écran Liste des utilisateurs.

Tableau 7. Valeurs sur l'écran Liste des utilisateurs

Valeur	Description
Nom d'utilisateur	Nom de connexion de la console.
Nom complet	Nom complet de l'utilisateur.
Courrier électronique	Adresse électronique utilisée pour les notifications d'alerte.
Abonnés	Si cette option est cochée, une ou plusieurs alertes sont attribuées à l'utilisateur. Si l'utilisateur est supprimé du système, tous les abonnements aux alertes dont il était titulaire lui sont supprimés.
Etat de la connexion	L'état Activé permet à l'utilisateur de se connecter à la console.

2. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques d'un utilisateur.
3. Cliquez sur l'icône Editer pour éditer les caractéristiques d'un utilisateur.
4. Editez les informations si nécessaire. Le tableau suivant décrit les valeurs sur l'écran Caractéristiques de l'utilisateur.

Tableau 8. Caractéristiques de l'utilisateur

Valeur	Description
Nom d'utilisateur	Nom de connexion de l'utilisateur de la console
Activé	Activer ou Désactiver l'accès à la console
Prénom	Prénom de l'utilisateur.
Nom de famille	Nom de famille de l'utilisateur.
Courrier électronique	Adresse électronique utilisée pour les notifications d'alerte.
Téléphone	Numéro de téléphone de l'utilisateur.
Numéro de télécopie	Numéro de télécopie de l'utilisateur.
Environnement local de la langue	Sélectionnez la zone géographique de l'utilisateur. L'environnement local de la langue par défaut sera celui défini par l'administrateur de concentrateur.
Environnement local du format	Sélectionnez le pays de l'utilisateur. L'environnement local de la langue par défaut sera celui défini par l'administrateur de concentrateur.
Fuseau horaire	Sélectionnez le fuseau horaire de l'utilisateur. Le fuseau horaire par défaut sera celui défini par l'administrateur de concentrateur.
Etat de l'alerte	Lorsqu'elle est activée, l'utilisateur reçoit toutes les alertes auxquelles il a été abonné. Sélectionnez Désactiver pour que cet utilisateur ne reçoive plus toutes les alertes.
Abonnés	Cette valeur est définie par le système.
Visibilité	Sélectionnez Local pour que l'utilisateur soit visible uniquement dans votre organisation. Sélectionnez Global pour que l'utilisateur soit visible par votre organisation et par le gestionnaire.

Remarque : Après l'installation et le lancement, l'environnement local et le fuseau horaire par défaut sont respectivement l'anglais (Etats-Unis) et le temps UTC. Le système utilise le temps UTC pour ses calculs de fuseaux horaires, le temps UTC par défaut ne peut pas être changé au niveau du système. Les utilisateurs peuvent cependant tous modifier le fuseau horaire affiché dans la Console de communauté.

Lorsque l'utilisateur *Administrateur de concentrateur* se connectera au système pour la première fois, l'environnement local et le fuseau horaire du système (Anglais, UTC) seront récupérés. Etant donné que l'utilisateur Administrateur de concentrateur est le superutilisateur responsable de la configuration du système, l'environnement local et le fuseau horaire de la Console qu'il choisira deviendront les nouvelles valeurs par défaut pour tous les utilisateurs de la Console de communauté. Les utilisateurs individuels ont aussi la possibilité de modifier leur environnement local et leur fuseau horaire si nécessaire.

5. Cliquez sur **Sauvegarder**.

Suppression des utilisateurs

Vous devez disposer des droits d'accès appropriés pour utiliser la fonction de suppression des utilisateurs. Il est possible de supprimer tous les utilisateurs à l'exception de HUBADMIN.

Utilisez la fonction suivante pour supprimer un utilisateur :

1. Cliquez sur **Administrateur du compte** > **Profils** > **Utilisateurs**.

2. Cliquez sur l'icône **Supprimer** en regard de l'utilisateur que vous voulez supprimer.
3. Dans la fenêtre d'avertissement, cliquez sur **OK** pour confirmer la suppression. Si vous cliquez sur **Annuler** vous annulerez la suppression.

Gestion des contacts

Utilisez la fonction Contacts pour afficher et éditer les informations de contact pour le personnel clé.

En fonction de la taille de votre organisation, vous avertirez probablement différents contacts lorsque différents types d'événements auront lieu. Par exemple, lorsque la validation d'un document échoue, le personnel de la sécurité doit en être avisé afin de pouvoir évaluer l'incident. Lorsque les transmissions du partenaire interne dépassent les limites normales, votre administrateur réseau doit être prévenu afin de s'assurer que le système gère efficacement cette augmentation des transmissions.

Affichage ou édition des caractéristiques du contact

1. Cliquez sur **Administrateur du compte** > **Profils** > **Contacts**. Le système affiche la liste des contacts en cours.

   Le tableau suivant identifie les valeurs apparaissant sur l'écran Contacts.

Tableau 9. Valeurs sur l'écran Liste des contacts

Valeur	Description
Nom complet	Nom complet du contact.
Type de contact	Décrit le rôle du contact, par exemple : Opportunité B2B ou Opportunité commerciale.
Courrier électronique	Adresse électronique utilisée pour les notifications d'alerte.
Visibilité	• Local. Le contact est visible uniquement par votre organisation. • Global. Le contact est visible par l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux abonner le contact aux alertes.
Abonnés	Si cette option est cochée, une ou plusieurs alertes sont attribuées à ce contact. Si le contact est supprimé du système, tous les abonnements aux alertes faits pour lui sont supprimés.
Etat de l'alerte	Lorsque l'Etat d'alerte est activé, ce contact reçoit toutes les alertes auxquelles il est abonné.

2. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques du contact. Le système affiche l'écran Caractéristiques du contact.
3. Cliquez sur l'icône Editer pour éditer les caractéristiques du contact.
4. Editez les informations si nécessaire. Le tableau suivant décrit les valeurs du contact.

Tableau 10. Caractéristiques du contact

Valeur	Description
Prénom	Prénom du contact.
Nom de famille	Nom de famille du contact.
Adresse	Adresse du contact, comprenant la rue, la ville et le code postal.
Type de contact	Décrit le rôle du contact, par exemple : Opportunité B2B ou Opportunité commerciale.
Adresse électronique	Adresse électronique du contact pour les notifications d'alerte.
Téléphone	Numéro de téléphone du contact.
Numéro de télécopie	Numéro de télécopie du contact.
Etat de l'alerte	Lorsqu'elle est activée, ce contact reçoit toutes les alertes auxquelles il a été abonné. Sélectionnez Désactiver pour que ce contact ne reçoive plus toutes les alertes.
Abonnés	Cette valeur est définie par le système.
Visibilité	• Local. Le contact est visible uniquement par votre organisation. • Global. Le contact est visible par l'administrateur du concentrateur et le partenaire interne. Ces derniers peuvent tous les deux abonner le contact aux alertes.

5. Cliquez sur **Sauvegarder**.

Retrait d'un contact

1. Cliquez sur **Administrateur du compte** > **Profils** > **Contacts**. Le système affiche la liste des contacts en cours.
2. Cliquez sur l'icône Supprimer pour supprimer le contact approprié.

Gestion des alertes

Les alertes de WebSphere Partner Gateway servent à avertir le personnel clé au sujet de fluctuations inhabituelles dans le volume de transmissions que vous recevez, ou lorsque des erreurs de traitement de documents de gestion ont lieu.

Une aide dans le module Afficheur, Afficheur d'événements, vous aide à mieux identifier et réparer les erreurs de traitement.

Affichage ou édition des caractéristiques de l'alerte et des contacts

Le partenaire interne peut afficher toutes les alertes, quel que soit le propriétaire de l'alerte (le créateur de l'alerte).

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche l'écran Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte. Vous pouvez aussi cliquer sur **Rechercher** sans sélectionner de critère de recherche (le système affiche toutes les alertes).
3. Cliquez sur **Rechercher**. Le système affiche l'écran Résultats de la recherche d'alerte.
4. Cliquez sur l'icône Afficher les caractéristiques pour visualiser les caractéristiques d'une alerte.
5. Cliquez sur l'icône Editer pour éditer les caractéristiques d'une alerte.
6. Editez les informations si nécessaire.

7. Cliquez sur l'onglet **Notification**.
8. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement). Le partenaire interne peut afficher toutes les alertes, quel que soit le propriétaire de l'alerte.
9. Si vous le souhaitez, éditez les contacts pour cette alerte.
10. Cliquez sur **Sauvegarder**.

Recherche d'alertes

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche l'écran Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte. Vous pouvez aussi cliquer sur **Rechercher** sans sélectionner de critère de recherche (le système affiche toutes les alertes).

Tableau 11. Critères de recherche d'alerte pour les partenaires

Valeur	Description
Type d'alerte	Alerte de volume, d'événement ou tous les types d'alerte.
Nom de l'alerte	Nom de l'alerte.
Etat de l'alerte	Alertes activées, désactivées ou toutes les alertes.
Contacts abonnés	Contacts désignés pour recevoir des alertes. Vous pouvez sélectionner Pour les abonnés, Aucun abonné ou Tous.
Résultats par page	Contrôle le mode d'affichage des résultats de la recherche.

Tableau 12. Critères de recherche d'alerte pour le partenaire interne et l'administrateur du concentrateur

Valeur	Description
Propriétaire de l'alerte	Créateur de l'alerte.
Partenaire de l'alerte	Partenaire auquel l'alerte s'applique.
Type d'alerte	Alerte de volume, d'événement ou tous les types d'alerte.
Nom de l'alerte	Nom de l'alerte.
Etat de l'alerte	Alertes activées, désactivées ou toutes les alertes.
Contacts abonnés	Contacts désignés pour recevoir des alertes. Vous pouvez sélectionner Pour les abonnés, Aucun abonné ou Tous.
Résultats par page	Contrôle le mode d'affichage des résultats de la recherche.

3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.

Désactivation ou activation d'une alerte

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche l'écran Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte.
3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.
4. Localisez l'alerte et cliquez sur **Désactivé** ou **Activé** sous Etat. Seuls l'administrateur du concentrateur et le propriétaire de l'alerte (créateur de l'alerte) ont le droit d'éditer l'^état de l'alerte.

Suppression d'une alerte

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche l'écran Recherche d'alerte.
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte.
3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.
4. Localisez l'alerte et cliquez sur l'icône Supprimer pour la supprimer. Seuls l'administrateur du concentrateur et le propriétaire de l'alerte (créateur de l'alerte) peuvent supprimer une alerte.

Notification d'événement

WebSphere Partner Gateway vous permet de configurer une alerte d'événement de sorte que le partenaire source et le partenaire sont notifiés lorsque l'événement se produit. Deux options sont disponibles pour la notification d'alerte. Ces options sont les suivantes :

- Notifier toutes les parties concernées
- Notifier les contacts abonnés uniquement

Lorsque l'option Notifier toutes les parties concernées est sélectionnée, l'alerte notifie automatiquement les contacts du partenaire source et les contacts du partenaire cible de l'événement, ainsi que les contacts du propriétaire de l'alerte. L'utilisateur n'a pas besoin de spécifier (et n'y est pas autorisé) ″Contacts abonnés″ lorsque ce mode est sélectionné. Lorsque le mode Alerter uniquement les contacts abonnés est sélectionné, l'alerte ne notifie que les contacts abonnés.

Après avoir déterminé quelles sont les parties à notifier, vous pouvez choisir :

- Envoi d'alertes immédiat
- Regroupement des alertes (par nombre ou intervalle de temps)

Remarque : Le serveur des messages d'alerte doit être configuré pour utiliser cette fonctionnalité supplémentaire. Reportez-vous au*Guide de l'administrateur système* pour obtenir des instructions de configuration de ce serveur.

Gestion des adresses

Utilisez cette fonction pour gérer les adresses dans votre profil de partenaire.

Edition d'une adresse

1. Cliquez sur **Administrateur du compte** > **Profils** > **Adresses**. Le système affiche l'écran Adresses.
2. Localisez l'adresse à éditer, puis cliquez sur l'icône Editer.
3. Effectuez les modifications requises. Le tableau suivant décrit les valeurs de l'adresse.

Tableau 13. Valeurs de l'adresse

Valeur	Description
Type d'adresse	Société, Facturation et Technique.
Adresse	Adresse comprenant la rue, la ville et le code postal.

4. Cliquez sur **Sauvegarder**.

Suppression d’une adresse

1. Cliquez sur **Administrateur du compte** > **Profils** > **Adresses**. Le système affiche l’écran Adresses.
2. Localisez l’adresse à supprimer, puis cliquez sur l’icône Supprimer.
3. Assurez-vous que vous souhaitez effectivement supprimer l’adresse.

Chapitre 5. Affichage des événements et des documents : Afficheurs

Les afficheurs donnent une vue de l'état de santé général du système. Ils constituent aussi des outils d'identification des incidents pour la résolution des événements.

Le module Afficheurs comprend les fonctions suivantes :

- «Afficheur d'événements»
- «Afficheur AS», à la page 72
- «Afficheur ebMS», à la page 75
- «Afficheur RosettaNet», à la page 77
- «Afficheur de documents», à la page 79
- «File d'attente de destination», à la page 84

Les afficheurs RosettaNet et AS incluent des critères de recherche supplémentaires pour l'administrateur du concentrateur. Pour plus d'informations, voir le *Guide de l'administrateur*.

Remarque : Le terme partenaires est utilisé dans les fenêtres des afficheurs pour désigner un membre de la communauté du concentrateur, notamment le partenaire interne.

Afficheur d'événements

L'Afficheur d'événements vous permet de rechercher des événements par heure, date, type d'événement, nom d'événement et emplacement de l'événement. L'administrateur du concentrateur peut aussi faire une recherche par partenaire, IP source et ID événement.

Les données générées par l'Afficheur d'événements identifient, parmi d'autre éléments, le Nom de l'événement, l'Horodatage et l'IP source. Elles permettent également d'afficher les caractéristiques des événements et des documents afin de diagnostiquer l'incident. Vous pouvez également afficher le document de base, qui identifie la zone, la valeur et la cause de l'erreur.

Un événement permet de savoir que quelque chose d'inhabituel s'est produit dans le système. Il peut indiquer qu'une fonction ou qu'une opération du système a abouti (par exemple, vous avez réussi à ajouter un partenaire au système, ou à créer une connexion de partenaire entre le partenaire interne et le partenaire externe). Il peut également identifier un incident (par exemple, le système n'a pas pu traiter un document ou il a détecté une erreur non critique dans un document). La plupart des documents sont renvoyés plusieurs fois : si un document échoue et génère une alerte, vous devez donc examiner le problème et faire les corrections nécessaires pour éviter ce genre d'échecs à l'avenir.

WebSphere Partner Gateway inclut des événements prédéfinis. Utilisez la fonction Alerte du produit, dans le module Administrateur du compte, pour créer une alerte basée sur l'événement. Ce processus identifie les événements qui vous

concernent. Utilisez ensuite la fonction Contacts, également située dans le module Administrateur du compte, pour identifier les membres du personnel qui seront avertis si ces événements ont lieu.

L'Afficheur d'événements affiche les événements sur la base de critères de recherche spécifiques. Vous pouvez localiser un événement spécifique et en rechercher la cause. L'Afficheur d'événements vous permet de rechercher des événements par heure, date, type d'événement (débogage, informations, avertissement, erreur et critique), nom d'événement (par exemple, 210031) et emplacement d'événement.

Les données disponibles via l'Afficheur d'événements incluent le nom de l'événement, l'horodatage, l'utilisateur et les informations sur le partenaire. Ces données aident à identifier le document ou le processus qui a créé l'événement. Si l'événement est associé à un document, vous pouvez également afficher le document de base identifiant la zone, la valeur et la cause de l'erreur.

Types d'événements

WebSphere Partner Gateway comprend les types d'événements suivants.

Tableau 14. Types d'événements

Type d'événement	Description
Débogage	Les événements Débogage servent à la prise en charge et aux opérations de système de bas niveau. Leur visibilité et leur utilisation dépendent du niveau d'autorisation de l'utilisateur. Les utilisateurs n'ont pas tous accès aux événements Débogage.
Information	Les événements informationnels sont générés lorsqu'une opération de système a abouti. Ils servent aussi à indiquer l'état des documents en cours de traitement. Ces événements ne demandent aucune intervention de la part de l'utilisateur.
Avertissement	Les événements Avertissement sont dus à des anomalies non critiques, dans le traitement de documents ou dans les fonctions du système, qui n'empêchent pas la poursuite de l'opération.
Erreur	Les événements Erreur sont dus à des anomalies dans le traitement du document, qui provoquent l'arrêt du processus.
Critique	Les événements critiques sont générés lorsque les services sont interrompus en raison d'une défaillance du système. Ils demandent une intervention de la part du personnel administratif.

Exécution des tâches de l'Afficheur d'événements

Tableau 15. Tâches de l'Afficheur d'événements

Que souhaitez-vous faire ?	Voir
Rechercher des événements	page 70
Afficher les caractéristiques de l'événement	page 71

Recherche d'événements

1. Cliquez sur **Afficheurs** > **Afficheur d'événements**.

   Les événements sont classés par gravité, de gauche à droite, dans l'écran Recherche de l'afficheur d'événement. Informations, à gauche, représente le type d'événement le moins grave ; Critique, à droite, représente le type le plus grave. (Les événements Débogage ne peuvent pas être affichés par tous les utilisateurs.) Pour tout événement sélectionné, l'Afficheur d'événements affiche

cet événement ainsi que tous les événements plus graves. Par exemple, si le type d'événement Avertissement est sélectionné dans les critères de recherche, les événement Avertissement, Erreur et Critique sont affichés. Si les événements Information sont sélectionnés, tous les types d'événements sont affichés.

2. Sélectionnez les critères de recherche dans les listes déroulantes.

Tableau 16. Critères de recherche d'événements

Valeur	Description
Date et heure de début	Date et heure de l'apparition du premier événement. La valeur par défaut est 10 minutes avant.
Date et heure de fin	Date et heure de l'apparition du dernier événement.
Partenaires	Sélectionnez tous les partenaires ou un partenaire spécifique (partenaire interne uniquement).
Type d'événement	Type d'événement : Débogage, Info, Avertissement, Erreur ou Critique.
Nom de l'événement	Recherche des noms d'événements disponibles en fonction du type d'événement sélectionné.
Emplacement de l'événement	Emplacement où l'événement a été généré : tous, inconnu, source (de), cible (à).
Trier par	Valeur utilisée pour trier les résultats.
Ordre croissant ou Ordre décroissant	Trie par ordre croissant ou décroissant.
Résultats par page	Nombre d'enregistrements affichés par page.
Régénérer	Le paramètre par défaut est Hors fonction. Lorsque la valeur Régénérer est En fonction, l'Afficheur d'événements exécute d'abord une nouvelle requête, puis il reste en mode de régénération.
Fréquence de régénération	Contrôle la fréquence de régénération des résultats de la recherche (partenaire interne uniquement).

3. Cliquez sur **Rechercher**. Le système affiche la liste des événements.

Conseil : La liste des événements peut être filtrée à nouveau en fonction du type d'événement sélectionné en haut de l'écran Afficheur d'événements. La régénération d'écran suivante prend en compte le nouveau type d'événement sélectionné.

Affichage des caractéristiques de l'événement

1. Cliquez sur **Afficheurs** > **Afficheur d'événements**.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche la liste des événements.
4. Cliquez sur l'icône Afficher les caractéristiques en regard de l'événement à afficher. Le système affiche les caractéristiques de l'événement et les documents associés.
5. Cliquez sur l'icône Afficher les caractéristiques en regard du document à afficher, le cas échéant.
6. Cliquez sur l'icône Afficher le document de base pour le cas échéant, visualiser le document de base.
7. Cliquez sur l'icône Afficher les erreurs de validation pour visualiser les erreurs de validation.

Lorsque le message d'erreur ″Aucun certificat de chiffrement valide n'a été trouvé″ s'affiche, les certificats principal et secondaire ne sont valides, ni l'un ni l'autre. Les certificats peuvent avoir expirés ou avoir été révoqués. Dans ces deux cas, l'événement correspondant (Aucun certificat de chiffrement valide n'a été trouvé) apparaît dans l'afficheur d'événements.

Conseil : Si un événement Document en double est affiché dans les caractéristiques de l'Afficheur d'événements, affichez le document original envoyé en cliquant sur l'icône Afficher le document d'origine dans les Caractéristiques du document.

Afficheur AS

L'Afficheur AS sert à rechercher et à afficher les informations de transport pour les documents utilisant le protocole de communication AS1, AS2 ou AS3. Vous pouvez afficher les ID message, l'état et l'identificateur URI de la destination de la MDN (Message Disposition Notification) et les caractéristiques du document (le document et l'encapsuleur).

L'Afficheur AS permet également d'afficher les caractéristiques des transactions B2B mises en forme et du processus B2B utilisant le protocole de communication AS1, AS2 ou AS3 (Applicability Statement 1 ou 2). Vous pouvez afficher les mouvements du processus B2B et des documents de gestion associés, les signaux d'accusé de réception, l'état du processus, les en-têtes HTTP et les contenus des documents transmis.

Comme son prédécesseur AS1, qui définit une norme pour les transmissions de données utilisant SMTP, AS2 définit une norme pour les transmissions de données utilisant HTTP.

AS2 identifie le mode de connexion, de livraison, de validation et de réponse aux données ; il ne s'occupe pas du contenu du document mais de son transport. AS2 crée un encapsuleur autour d'un document afin qu'il puisse être transporté par Internet via HTTP ou HTTPS. L'ensemble du document et de l'encapsuleur est nommé message. AS2 assure la sécurité et le chiffrement des paquets HTTP. AS2 offre une base de chiffrement avec distribution garantie. Le protocole AS3 fournit un nouveau standard de transmission sécurisée de documents via FTP ou FTPS.

Un composant important d'AS2 est le mécanisme de réception, nommé MDN (Message Disposition Notification). Il garantit à l'expéditeur du document que le destinataire a reçu le document. L'expéditeur spécifie comment la MDN doit être renvoyée (de manière synchrone ou asynchrone, signée ou non signée).

Vous pouvez utiliser l'Afficheur AS pour afficher l'ID message, les Horodatages, le Type de document, le Type de destination, l'Etat synchrone ainsi que les caractéristiques du document. Les informations supplémentaires sur le traitement du document apparaissent lors de l'affichage des caractéristiques du document.

Exécution des tâches de l’Afficheur AS

Tableau 17. Tâches de l’Afficheur AS1/AS2

Que souhaitez-vous faire ?	Voir
Recherche de messages AS	page «Recherche de messages»
Affichage des documents de base	page «Affichage des caractéristiques du message», à la page 74

Recherche de messages

1. Cliquez sur **Afficheurs** > **Afficheur AS**. Le système affiche l’écran Afficheur AS.

2. Sélectionnez les critères de recherche dans les listes déroulantes.

Tableau 18. Critères de recherche de l'Afficheur AS

Valeur	Description
Date et heure de début	Date et heure du lancement du processus.
Date et heure de fin	Date et heure de l'achèvement du processus.
Partenaire source	Identifie le partenaire émetteur (partenaire interne uniquement).
Partenaire cible	Identifie le partenaire récepteur.
Recherche	Indique si le document à rechercher est le type de document source ou cible.
ID entreprise de la source AS	Numéro d'identification d'entreprise du partenaire source. Par exemple, Duns.
ID entreprise de la source de charge	Numéro d'identification de la source de charge.
Mode de fonctionnement	Production, Test, Partenaire externe de simulateur RN ou Partenaire externe de simulateur RN. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.
Package	Décrit le format du document, l'empaquetage, le chiffrement et l'identification du type de contenu.
Protocole	Format de document disponible pour les partenaires. Par exemple, RosettaNet de XML.
Type de document	Processus métier spécifique.
ID message	ID attribué au document mis en forme AS1, AS2 ou AS3. Les critères de recherche peuvent inclure le caractère générique astérisque (*). Longueur maximale, 255 caractères.
ID document	Numéro d'identification unique attribué au document.
Synch / Async	Recherche les documents reçus en mode synchrone ou asynchrone. Le mode synchrone signifie que la connexion entre l'initiateur et le Gestionnaire de documents reste ouverte jusqu'à ce que la transaction soit terminée, notamment une requête et la notification MDN (Message Disposition Notification).
Etat MDN	Cette zone vous permet de sélectionner l'état de la notification MDN sur ce message.
Trier par	Trier les résultats par cette valeur.
Ordre décroissant ou Ordre croissant	Ordre croissant. Affiche en premier l'horodatage le plus ancien ou la fin de l'alphabet. Ordre décroissant. Affiche en premier l'horodatage le plus récent ou le début de l'alphabet.
Résultats par page	Sert à sélectionner le nombre de rapports affichés par page.

3. Cliquez sur **Rechercher**. Le système affiche la liste des messages.

Affichage des caractéristiques du message

1. Cliquez sur **Afficheurs** > **Afficheur AS**. Le système affiche l'écran Afficheur AS.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche la liste des messages.
4. Cliquez sur l'icône Afficher les caractéristiques en regard du message à afficher. Le système affiche les caractéristique du message et du document associé.

Tableau 19. Afficheur AS : Caractéristiques du package

Valeur	Description
ID message	ID attribué au document mis en forme AS1, AS2 ou AS3. Ce numéro identifie uniquement le package. Le document possède son propre numéro ID qui apparaît lors de l'affichage des caractéristique du document. Longueur maximale, 255 caractères.
Partenaire source	Partenaire qui initialise un processus métier.
Partenaire cible	Partenaire qui reçoit le processus métier.
Horodatage d'initiation	Date et heure de début du traitement du document.
Type de destination	Test ou production. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.
Identificateur URI de la MDN	Adresse de destination de la MDN. Cette adresse peut être définie comme un identificateur URI HTTP ou comme une adresse électronique.
Texte de disposition de la MDN	Ce texte indique l'état du message d'origine qui a été reçu (qu'il ait abouti ou échoué). Voici des exemples : • Automatic-action / MDN-sent-automatically; processed. • Automatic-action / MDN-sent-automatically;processed / Warning;duplicate-document. • Automatic-action / MDN-sent-automatically;processed / Error;description-failed. • Automatic-action / MDN-sent-automatically;failed:unsupported MIC-algorithms.

5. (Facultatif) Cliquez sur l'icône Afficher le document de base pour visualiser le document de base.

Afficheur ebMS

Le mécanisme ebMS (ebXML Message Service) offre une méthode standard pour l'échange de messages entre partenaires d'échanges ebXML. Il constitue un moyen fiable d'échanger des messages sans utiliser des solutions ou des technologies propriétaires. Un message ebXML message contient des structures correspondant à un en-tête de message (nécessaire pour l'acheminement et la livraison) et à une charge. Le mécanisme ebMS offre une méthode standard pour l'échange de messages entre partenaires d'échanges ebXML. Le message ebXML est un protocole de communication indépendant de l'enveloppe de message MIME / Multipart.

Exécution des tâches de l'afficheur ebMS

Tableau 20. Tâches de l'afficheur ebMS

Que souhaitez-vous faire ?	Voir
Rechercher des processus ebMS	«Recherche de processus ebMS», à la page 76
Afficher des processus ebMS	«Affichage des caractéristiques des processus ebMS», à la page 76
Afficher des documents de base	«Affichage des documents de base», à la page 77
Afficher l'état des documents	«Affichage de l'état des documents», à la page 77

Recherche de processus ebMS

1. Cliquez sur **Afficheurs** > **Afficheur ebMS**. Le système affiche l'écran de recherche de l'afficheur ebMS.
2. Sélectionnez les critères de recherche dans les listes déroulantes.

Valeur	Description
Date et heure de début	Date et heure du lancement du processus.
Date et heure de fin	Date et heure de l'achèvement du processus.
Partenaire source	Identifie le partenaire expéditeur.
Partenaire cible	Identifie le partenaire récepteur.
ID entreprise source	Numéro d'identification d'entreprise du partenaire expéditeur. Par exemple, DUNS.
Mode de fonctionnement	Production, test, partenaire externe de simulateur RN ou partenaire externe de simulateur RN. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.
Protocole	Protocoles disponibles pour les partenaires.
Type de document	Type de document à traiter.
ID de conversation	Numéro d'identification unique attribué au processus. Les critères de recherche peuvent inclure le caractère générique astérisque (*).
Trier par	Trie les résultat, par exemple, par Horodatage reçu.
Ordre décroissant ou Ordre croissant	Ordre croissant. Affiche en premier l'horodatage le plus ancien ou la fin de l'alphabet. Ordre décroissant. Affiche en premier l'horodatage le plus récent ou le début de l'alphabet.
Résultats par page	Affiche un nombre n de résultats par page.

3. Cliquez sur **Rechercher**. Le système affiche les processus ebMS correspondant à vos critères de recherche.

Affichage des caractéristiques des processus ebMS

1. Cliquez sur **Afficheurs > Afficheur ebMS**. Le système affiche l'écran de l'afficheur ebMS.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche les résultats de votre recherche.

Tableau 21. Valeurs des critères de recherche de l'afficheur ebMS

Valeur	Description
Partenaires	Partenaires impliqués dans le processus métier.
Horodatage source	Date et heure de début du traitement du premier document.
Type de document	Processus métier spécifique, par exemple : ebMS 2.0 : ALMService Production
Mode de fonctionnement	Mode de fonctionnement, par exemple : Production
ID de conversation	Numéro d'identification unique affecté à cet événement

Affichage des documents de base

Pour afficher le document de base :

1. Cliquez sur **Afficheurs > Afficheur ebMS**.
2. Sélectionnez les critères de recherche dans les listes déroulantes, voir «Recherche de processus ebMS», à la page 76
3. Cliquez sur **Rechercher**.
4. Cliquez sur l'icône ″**Cliquer pour voir le document de base**″ sous la section **Légende**.

- Pour identifier les incidents des documents dont le traitement a échoué, voir «Affichage des erreurs de validation des données», à la page 83.
- L'afficheur du document de base présente l'en-tête HTTP avec le document de base.

Affichage de l'état des documents

1. Cliquez sur **Afficheurs > Afficheur ebMS**.
2. Sélectionnez les critères de recherche dans les listes déroulantes, voir «Recherche de processus ebMS», à la page 76
3. Cliquez sur **Rechercher**.
4. Cliquez sur **Demander l'état**.
5. Cliquez sur **Afficher l'état**.

Afficheur RosettaNet

L'Afficheur RosettaNet sert à localiser un processus spécifique ayant généré un événement. Lorsque vous identifiez le processus cible, vous pouvez afficher ses caractéristiques et le document de base.

RosettaNet est un groupe de sociétés ayant créé une norme industrielle pour les transactions e-business. Les PIP (Partner Interface Processes) définissent les processus métier entre les membres de la communauté de concentrateur. Chaque PIP identifie un document spécifique et la manière dont il est traité entre le partenaire interne et les partenaires externes.

L'afficheur RosettaNet affiche les mouvements des documents qui composent un processus métier. Les valeurs pouvant apparaître sur l'Afficheur RosettaNet comprennent l'état du processus, les caractéristiques, les documents de base et les événements de processus associés.

L'Afficheur RosettaNet affiche les processus à partir de critères de recherche spécifiques.

Exécution des tâches de l'Afficheur RosettaNet

Tableau 22. Tâches de l'Afficheur RosettaNet

Que souhaitez-vous faire ?	Voir
Rechercher des processus RosettaNet	page 78
Afficher les caractéristiques du processus RosettaNet	page 78
Afficher des documents de base	page 79

Recherche de processus RosettaNet

1. Cliquez sur **Afficheurs** > **Afficheur RosettaNet**. Le système affiche l'écran Recherche de l'afficheur RosettaNet.
2. Sélectionnez les critères de recherche dans les listes déroulantes. POINT DE DEPART

Tableau 23. Critères de recherche RosettaNet

Valeur	Description
Date et heure de début	Date et heure du lancement du processus.
Date et heure de fin	Date et heure de l'achèvement du processus.
Partenaire source	Identifie le partenaire expéditeur.
Partenaire cible	Identifie le partenaire récepteur.
ID entreprise source	Numéro d'identification d'entreprise du partenaire expéditeur. Par exemple, DUNS.
Mode de fonctionnement	Production, test, partenaire externe de simulateur RN ou partenaire externe de simulateur RN. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.
Protocole	Protocoles disponibles pour les partenaires.
Type de document	Type de document à traiter.
ID Instance du processus	Numéro d'identification unique attribué au processus. Les critères de recherche peuvent inclure le caractère générique astérisque (*).
Trier par	Trie les résultat, par exemple, par Horodatage reçu.
Ordre décroissant ou Ordre croissant	Ordre croissant. Affiche en premier l'horodatage le plus ancien ou la fin de l'alphabet. Ordre décroissant. Affiche en premier l'horodatage le plus récent ou le début de l'alphabet.
Résultats par page	Affiche un nombre n de résultats par page.

3. Cliquez sur **Rechercher**. Le système affiche les processus RosettaNet qui correspondent à vos critères de recherche.
4. Cliquez sur l'icône Afficher les caractéristiques en regard du processus ebMS à afficher. Le système affiche les caractéristiques du processus sélectionné et les documents qui lui sont associés.
5. Cliquez sur l'icône Afficher les caractéristiques en regard du document à afficher. Le système affiche les caractéristiques du document et de l'événement associé.

Affichage des caractéristiques du processus RosettaNet

1. Cliquez sur **Afficheurs** > **Afficheur RosettaNet**. Le système affiche l'écran Recherche de l'afficheur RosettaNet.
2. Sélectionnez les critères de recherche dans les listes déroulantes.

3. Cliquez sur **Rechercher**. Le système affiche les résultats de votre recherche.

Tableau 24. Caractéristiques du traitement de documents

Valeur	Description
Partenaires	Partenaires impliqués dans le processus métier.
Horodatages	Date et heure de début du traitement du premier document.
Type de document	Processus métier spécifique, par exemple RosettaNet (1.1) : 3A7.
Type de destination	Par exemple, Production.
ID Instance du processus	Numéro unique attribué au processus par le membre de la communauté expéditeur.
ID document	ID document du propriétaire attribué par le partenaire expéditeur. Cette zone n'est pas sur un emplacement fixe et varie selon le type de document.
Partenaire source	Partenaire expéditeur.
Partenaire cible	Partenaire récepteur.

4. Cliquez sur l'icône Afficher les caractéristiques en regard du processus RosettaNet à afficher. Le système affiche les caractéristiques du processus sélectionné et les documents qui lui sont associés.
5. Cliquez sur l'icône Afficher les caractéristiques en regard du document à afficher. Le système affiche les caractéristiques du document et de l'événement associé.

Affichage des documents de base

1. Cliquez sur **Afficheurs** > **Afficheur RosettaNet**. Le système affiche l'écran Recherche de l'afficheur RosettaNet.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche la liste des processus.
4. Cliquez sur l'icône Afficher les caractéristiques en regard du processus à afficher. Le système affiche les caractéristiques du processus sélectionné et les documents qui lui sont associés.
5. Cliquez sur l'icône Afficher le document de base en regard du type de document pour afficher le document de base.

Restrictions : Les documents de base de plus de 100 Ko sont tronqués.

Conseil :

- Pour identifier les incidents des documents dont le traitement a échoué, voir «Affichage des erreurs de validation des données», à la page 83.
- L'afficheur du document de base présente l'en-tête HTTP avec le document de base.

Afficheur de documents

L'Afficheur de documents sert à localiser et à afficher un document spécifique que vous souhaitez rechercher. Vous pouvez rechercher des documents à partir de la date, de l'heure, du type de processus (de début ou de fin), de la connexion du partenaire, du type de destination, de l'état du document, du protocole, du type de document et de la version du processus.

Certains protocoles, comme le protocole XML (Extensible Markup Language) utilisant les formats XML, peuvent extraire des informations de documents et les enregistrer pour que vous puissiez les rechercher avec l'Afficheur de documents. Les attributs de zones de recherche définies par l'utilisateur dans les définitions de format XML servent à cela. Dans le cas d'un document routé à l'aide d'un format XML incluant des zones de recherche, les informations relatives au document obtenu avec les zones de recherche peuvent faire l'objet d'une recherche. Prenons comme exemple un document XML personnalisé qui est en fait un ordre d'achat. Avec votre connaissance de la structure de document, vous pouvez définir un format XML avec une zone de recherche qui extrait le numéro de l'ordre d'achat. Lorsque des documents sont routés avec ce format XML, vous pouvez les rechercher à l'aide du numéro d'ordre d'achat en le saisissant dans la zone de recherche définie par l'utilisateur appropriée dans l'écran de recherche de l'Afficheur de documents.

Le routage de documents EDI (Electronic Data Interchange) qui extrait des informations du document peut également être défini. Un mappage DIS est alors codé pour renseigner les valeur des zones de recherche définies par l'utilisateur.

Vous pouvez également écrire un exit utilisateur qui extrait les information d'un document afin de pouvoir faire l'objet d'une recherche. Utilisez la méthode d'exit utilisateur BusinessDocumentInterface.setAttribute() pour renseigner les valeur des zones de recherche définies par l'utilisateur.

Les résultats de la recherche affichent tous les documents correspondant à vos critères de recherche et identifient les horodatages, le processus, la connexion du partenaire et les types de destination. Localisez le document cible et utilisez les fonctions de l'afficheur pour afficher le document de base. Vous pouvez également utiliser l'afficheur de documents pour renvoyer des documents ayant échoué ou abouti.

Recherche des documents

1. Cliquez sur **Afficheurs** > **Afficheur de documents**. Le système affiche l'écran Recherche de l'afficheur de documents.

2. Sélectionnez les critères de recherche dans les listes déroulantes.

Tableau 25. Critères de recherche de l'Afficheur de documents

Valeur	Description
Date et heure de début	Date et heure du lancement du processus.
Date et heure de fin	Date et heure de l'achèvement du processus.
Partenaire source	Identifie le partenaire expéditeur.
Partenaire cible	Identifie le partenaire récepteur. .
Recherche	Recherche sur le type de document d'origine ou le type de document de destination.
Mode de fonctionnement	Production, test, partenaire externe de simulateur RN ou partenaire externe de simulateur RN. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.
Etat du document	Etat actuel du document dans le système. Vous pouvez choisir En cours, Succès ou Echec. La valeur par défaut est Tout.
Package	Décrit le format du document, l'empaquetage, le chiffrement et l'identification du type de contenu.
Protocole	Type de protocole de processus disponible pour les partenaires.
Type de document	Processus métier spécifique.
ID document	Créé par le partenaire source. Les critères de recherche peuvent inclure le caractère générique astérisque (*).
ID référence	Numéro d'ID créé par le système pour suivre l'état de document.
Adresse IP source	Adresse IP du partenaire source.
Filtre	Recherche de documents reçus en mode synchrone. Cela signifie que la connexion entre l'expéditeur et le Gestionnaire de documents reste ouverte jusqu'à ce que la transaction soit terminée, y compris la requête et l'accusé de réception ou la requête et la réponse.
Trier par	Valeur utilisée pour trier les résultats.
Résultats par page	Nombre d'enregistrements affichés par page.
Ordre décroissant	Trie les résultats par ordre croissant ou décroissant.
Zones de recherche définies par l'utilisateur	Effectuez la recherche en fonction des critères définis par l'utilisateur.

Remarque : Les événements Avertissement sont affichés par défaut. Pour voir tous les événements, sélectionnez Débogage.

3. Cliquez sur **Rechercher**. Le système affiche la liste des messages correspondant à vos critères de recherche.

Tableau 26. Informations du document disponibles à l'aide de l'Afficheur de documents.

Valeur	Description
Partenaires	Partenaires source (expéditeur) et cible (destinataire) impliqués dans le processus métier.
Horodatages	Date et heure de début et de fin du traitement du document.
Type de document	Processus métier en cours de transaction.
Type de destination	Test ou production. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.

Tableau 26. Informations du document disponibles à l'aide de l'Afficheur de documents. (suite)

Valeur	Description
Synchrone	Indique que le document a été reçu en mode synchrone. Cela signifie que la connexion entre l'expéditeur et le Gestionnaire de documents reste ouverte jusqu'à ce que la transaction soit terminée, y compris la requête et l'accusé de réception ou la requête et la réponse.

Affichage des caractéristique du document, des événements et du document de base

1. Cliquez sur **Afficheurs** > **Afficheur de documents**. Le système affiche l'écran Recherche de l'afficheur de documents.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche la liste des documents.
   - Pour afficher les événements et les caractéristiques d'un document, cliquez sur l'icône d'ouverture de dossiers située en regard du document affiché sous l'en-tête Documents associés. Le système affiche les caractéristiques et les événements du processus du document sélectionné. Pour les documents EDI, s'il y a des transactions EDI enfant issues d'un désenveloppement ou d'un enveloppement, elles peuvent être affichées en sélectionnant le bouton d'option cible ou source **Enfants de document**. Pour plus d'informations sur l'affichage de documents EDI, reportez-vous au *Guide d'administration*.
   - Pour afficher le document de base avec l'en-tête HTTP, cliquez sur l'icône Afficher le document de base en regard du document. Le système affiche le contenu du document de base.

Les informations suivantes sur le traitement du document apparaissent lors de l'affichage des caractéristiques du document:

Tableau 27. Valeurs de traitement disponibles à l'aide de l'Afficheur de documents.

Valeur	Description
ID référence	Numéro d'identification unique attribué par le système au document.
ID document	Numéro d'identification unique attribué à un document par le partenaire source.
Horodatage du document	Date et heure de création du document par le partenaire.
Destination	Destination par laquelle le document est passé.
Type de document de la connexion	Actions exécutées sur un document par le système pour vérifier sa compatibilité avec les exigences commerciales entre les partenaires.
Source et cible	Partenaires source et cible impliqués dans le processus métier.
Horodatage d'entrée	Date et heure de réception par le système du document provenant du partenaire.
Horodatage de l'état de fin	Date et heure d'acheminement réussi par le système jusqu'au partenaire cible.
ID entreprise source et cible	Numéro d'identification d'entreprise des partenaires source et cible. Par exemple, DUNS.
Type de document source et cible	Processus métier spécifique établi entre les partenaires source et cible.

Restrictions : Les documents de base de plus de 100 Ko sont tronqués.

Conseil : Si le système affiche un événement Document en double, affichez le document original envoyé en cliquant sur la flèche bleue située en regard de l'événement Document en double, puis sur l'icône Afficher le document d'origine.

Conseil : Pour identifier les incidents des documents dont le traitement a échoué, voir «Affichage des erreurs de validation des données», à la page 83.

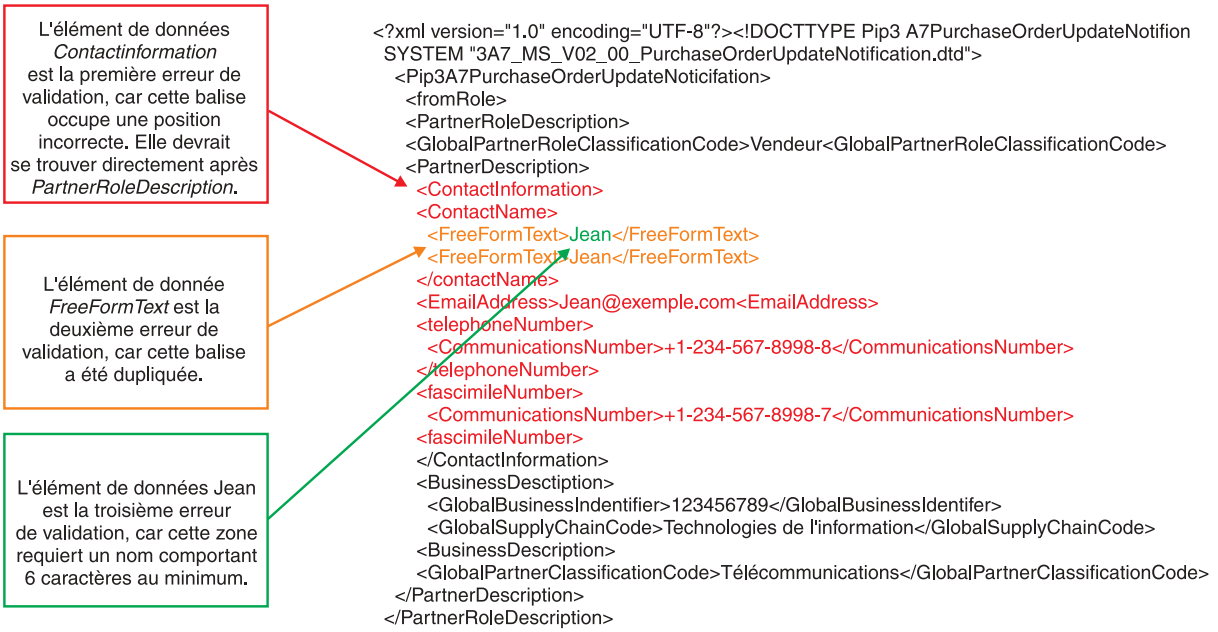
Affichage des erreurs de validation des données

Vous pouvez rechercher rapidement des documents dont le traitement a échoué en utilisant le texte à code couleur dans les zones XML contenant des erreurs de validation. Ces zones sont affichées en rouge. Si plus de trois erreurs de validation différentes apparaissent dans les zones XML imbriquées, les couleurs suivantes servent à distinguer les zones d'erreurs :

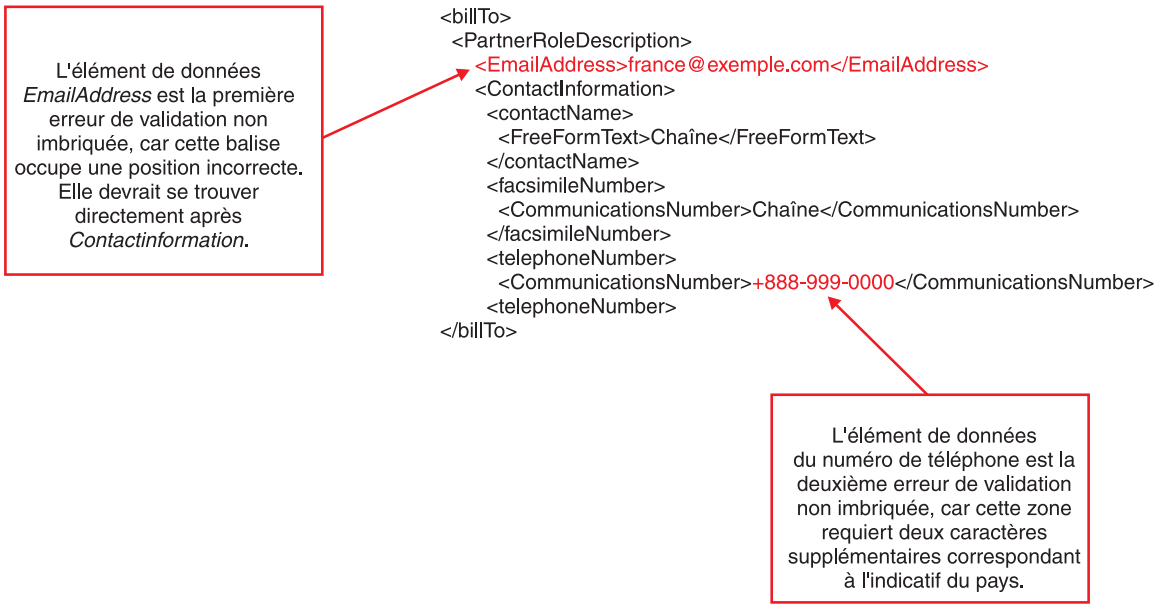
Tableau 28. Erreurs de validation de document à code couleur

Valeur	Description
Rouge	Première erreur de validation
Orange	Deuxième erreur de validation
Vert	Troisième erreur de validation

Voici un exemple d'erreurs de validation XML imbriquées :



Exemple d'erreurs de validation XML non-imbriquées :



Pour afficher les erreurs de validation dans un document de base, voir «Affichage des documents de base», à la page 79.

Restrictions : La console n'affiche que les cent premiers kilo-octets d'un document de base. Les erreurs de validation au delà des 100 Ko ne sont pas affichables.

Utilisation de la fonction Arrêt du processus

Cliquez sur **Arrêt du processus** pour interrompre un document en cours. Cette fonction n'est pas restreinte à l'utilisateur administrateur du concentrateur. Les droits du groupe doivent être configuré pour rendre cette fonction disponible.

Remarque : Le système peut mettre jusqu'à une heure pour interrompre le document. Pendant ce temps, l'Afficheur de documents continue d'afficher l'état du document comme étant en cours.

File d'attente de destination

La file d'attente de destination vous permet d'afficher les documents mis en file d'attente en vue de leur livraison depuis n'importe quelle destination du système. Elle permet également de visualiser toutes les destinations ayant des documents en file d'attente pour livraison, d'afficher et de supprimer des documents d'une file d'attente et d'activer ou de désactiver des destinations.

Elle permet de s'assurer que des documents évoluant dans le temps ne demeurent pas dans la file d'attente et que le nombre maximal de documents pouvant être placés en file d'attente n'est pas dépassé. Grâce à la file d'attende de destination, vous pouvez :

- Voir la liste de toutes les destinations contenant des documents mis en file d'attente pour livraison.
- Afficher un document resté en file d'attente de la destination pendant un laps de temps important (30 secondes ou plus). Ceci peut indiquer un problème avec le

document lui-même. Vous pouvez également afficher les caractéristiques pour identifier et résoudre les incidents du document de la file d'attente.

Remarque : Si vous mettez en oeuvre une destination de script FTP en planifiant un intervalle ou un agenda, les documents peuvent rester dans cette file d'attente pour une durée plus longue, jusqu'à ce que cet intervalle ou cet horodatage soient atteints. Il s'agit en général de l'opération prévue et les documents ne doivent pas être supprimés de la file d'attente.

- Afficher les caractéristiques de la destination pour garantir un fonctionnement correct. L'accumulation de documents au niveau de la destination peut indiquer une erreur de cette dernière ou du gestionnaire de livraison.
- Confirmer l'état d'une destination. Une destination hors ligne peut provoquer une accumulation de documents dans la file d'attente jusqu'à la mise en ligne de la destination. Le statut de la destination n'affecte pas la fonction de connexion et les documents continuent d'être traités et placés dans la file d'attente en attendant leur envoi.
- Limiter la taille de liste de la file d'attente de destination en vous servant des zones **Nom de partenaire** et **Destination**.

Affichage de la liste de destinations

Pour afficher la liste des documents résidant dans la destination, effectuez la procédure suivante :

1. Sélectionnez **Afficheurs** > **File d'attente de destination**. La Console affiche la fenêtre File d'attente de destination.

2. Entrez les paramètres indiqués dans le tableau 29.

Tableau 29. Fenêtre File d'attente de la destination

Critères	Description
Nom de partenaire	Vous pouvez remplir ce champs de la manière suivante : 1. Entrez le nom du partenaire. 2. Entrez une partie du nom du partenaire dans cette zone, puis cliquez sur **Afficher les partenaires**. Sélectionnez un partenaire dans la liste. 3. Indiquez le caractère générique * et cliquez sur **Afficher les partenaires**. Sélectionnez un partenaire dans la liste. Lorsque vous cliquez sur **Afficher les partenaires**, une zone Partenaire s'affiche. Elle affiche la totalité des partenaires, par ordre alphabétique.
Destination	Le premier élément de la liste, `Tout`, est sélectionné par défaut. Le reste de la liste correspond aux transports, par ordre alphabétique, de la destination. Vous ne pouvez sélectionner qu'une seule destination. La destination sélectionnée par défaut est `Tout`. **Remarque :** Cette liste est automatiquement alimentée par les destinations de partenaires sélectionnées et présentée par ordre alphabétique.
Mis en file d'attente au moins	Nombre minimal de minutes qu'un document a attendu dans la file d'attente de la destination. Par exemple, si une valeur de 6 minutes est sélectionnée, toutes les destinations contenant des documents qui ont attendu d'être livrés pendant 6 minutes ou plus seront affichées. La valeur par défaut est `0`.
Trier par	Les résultats de la recherche sont triés par partenaire (valeur par défaut) ou par nom de la destination.
Régénérer	Vous pouvez activer ou désactiver (valeur par défaut) la régénération.
Nombre minimal de documents	Nombre minimal de documents dans la file d'attente d'une destination. La valeur par défaut est 1.
Sens	Cliquez sur **Ordre croissant** pour afficher des documents en commençant par l'horodatage le plus ancien ou par la fin de l'alphabet, ou **Ordre décroissant** pour afficher des documents en commençant par l'horodatage le plus récent ou le début de l'alphabet.
Fréquence de régénération	Nombre de secondes pendant lesquelles la Console attend avant de mettre à jour les données affichées.

3. Cliquez sur **Rechercher**. Le système recherche tous les documents situés sur la destination qui correspondent à vos critères de recherche. Le **tableau 30** contient les informations renvoyées suite à la recherche.

Tableau 30. Résultats de la recherche de la file d'attente de destination

Critères	Description
Partenaire	Partenaires d'échanges associés à la destination
Destination	Nom de la destination
Mis en file d'attente	Nombre de documents dans la file d'attente de destination en attente de livraison. Lien vers les caractéristiques de la destination
Etat	Indique si la destination est en ligne ou hors ligne
Dernier envoi	Date et heure du dernier envoi d'un document à la destination

Remarque : Pour que la Console affiche une destination, celle-ci doit respecter tous les critères de recherche utilisant l'opérateur logique AND.

Affichage des documents mis en file d'attente

Pour afficher les documents placés en file d'attente pour un partenaire spécifique, procédez comme suit :

1. Cliquez sur **Afficheurs** > > **File d'attente de destination**.
2. Dans la fenêtre de recherche de la File d'attente de destination, cliquez sur **Rechercher les documents**.
3. Dans la fenêtre de recherche de la file d'attente de destination, entrez les critères de recherche (voir tableau 31, à la page 87).

Tableau 31. Fenêtre de recherche des documents de la file d'attente

Critères	Description
Nom de partenaire	Vous pouvez remplir ce champs de la manière suivante : 1. Entrez le nom du partenaire. 2. Entrez une partie du nom du partenaire dans cette zone, puis cliquez sur **Afficher les partenaires**. Sélectionnez le partenaire dans la liste. 3. Indiquez le caractère générique * et cliquez sur **Afficher les partenaires**. Sélectionnez un partenaire dans la liste. **Remarque :** Lorsque vous cliquez sur **Afficher les partenaires**, une zone Partenaire s'affiche. Elle affiche la totalité des partenaires, par ordre alphabétique.
Destination	Le premier élément de la liste, Tout, est sélectionné par défaut. Le reste de la liste correspond aux transports, par ordre alphabétique, de la destination. Vous ne pouvez sélectionner qu'une seule destination. La destination sélectionnée par défaut est Tout. **Remarque :** Cette liste est automatiquement alimentée par les destinations de partenaires sélectionnées et présentée par ordre alphabétique.
Trier par	Indiquez si la liste doit être triée par partenaire (valeur par défaut), par destination, par ID référence ou par horodatage des documents en file d'attente (heure du dernier envoi du document).
ID référence	Numéro d'identification unique attribué par le système au document.
Sens	Cliquez sur **Ordre croissant** pour afficher des documents en commençant par l'horodatage le plus ancien ou par la fin de l'alphabet, ou **Ordre décroissant** pour afficher des documents en commençant par l'horodatage le plus récent ou le début de l'alphabet.
ID document	Numéro d'identification unique attribué à un document par le partenaire source.
Résultats par page	Nombre de documents affichés par page.
Nombre maximal de documents admis	Nombre d'enregistrements à afficher.

4. Cliquez sur **Rechercher**. Les résultats de la recherche sur les files d'attente s'affichent.

Suppression de documents de la file d'attente de livraison

La procédure suivante décrit comment supprimer des documents de la file d'attente de livraison. Vous devez être connecté en tant qu'administrateur du concentrateur pour pouvoir supprimer les documents de la file d'attente.

1. Cliquez sur **Afficheurs** > **File d'attente de destination**.
2. Dans la fenêtre File d'attente de destination, cliquez sur **Rechercher**.

3. Renseignez les paramètres dans la fenêtre (voir tableau 30, à la page 86).
4. Cliquez sur l'icône Supprimer pour supprimer le document.

Affichage des caractéristiques de la destination

Pour afficher les informations relatives à une destination spécifique, y compris la liste des documents de la file d'attente, procédez comme suit :

1. Cliquez sur **Afficheurs** > **File d'attente de destination**.
2. Dans la fenêtre File d'attente de destination, entrez les critères de recherche (voir le tableau 29, à la page 86).
3. Cliquez sur **Rechercher**.
4. Dans la liste des destinations, cliquez sur le lien associé au nombre de documents dans la colonne **Mis en file d'attente**. Les caractéristiques de la destination et la liste des documents mis en file d'attente s'affichent.

Modification de l'état de la destination

Pour mettre une destination en ligne ou hors ligne, procédez comme suit :

1. Cliquez sur **Afficheurs** > **File d'attente de destination**.
2. Dans la fenêtre File d'attente de destination, entrez les critères de recherche (voir le tableau 29, à la page 86).
3. Cliquez sur **Rechercher**.
4. Dans la liste des destinations, cliquez sur le lien associé au nombre de documents dans la colonne **Mis en file d'attente**. Les caractéristiques de la destination et la liste des documents mis en file d'attente s'affichent.
5. Cliquez sur **Connecté** dans **Informations sur la destination** pour mettre une destination hors ligne, ou cliquez sur **Déconnecté** pour la mettre en ligne. (Vous devez être connecté en tant qu'administrateur du concentrateur pour pouvoir modifier l'état de la destination.)

Chapitre 6. Analyse du type de document : Outils

Utilisez l'outil Analyse de document pour obtenir une vue d'ensemble détaillée du nombre de documents présents dans le système, selon leur état (Reçu, En cours, Echec et Succès). Les critères de recherche incluent notamment la date, l'heure, le type de processus (destination ou origine), le type de destination, le protocole, le type de document ainsi que la version du processus. Utilisez les résultats de la recherche pour localiser et afficher les documents ayant échoué afin de rechercher la cause de ces échecs.

L'outil Rapport du volume de document permet de gérer, suivre et résoudre les incidents liés à votre flux de documents de gestion. Le rapport affiche le volume de documents traités par le système dans un intervalle donné. Vous pouvez afficher, imprimer et enregistrer ce rapport afin de l'envoyer aux autres membres du personnel. Vous pouvez également personnaliser ce rapport pour afficher les informations selon des critères de recherche spécifiques.

L'outil Test de la connexion du partenaire permet de tester la destination ou le serveur Web.

Tableau 32. Outils

Quelle fonction voulez-vous utiliser ?	**Voir**
Analyse de document	page 89
Rapport du volume de document	page 92
Test de la connexion du partenaire	page 94
Rapports EDI	page 96
Rapports FTP	page 100

Analyse de document

Utilisez l'outil Analyse de document pour obtenir une vue d'ensemble détaillée du nombre de documents présents dans le système, selon leur état, dans une période donnée.

Utilisez les critères de recherche pour localiser les documents ayant échoué et rechercher la cause de ces incidents.

L'écran Analyse de document contient une alarme. Si un processus échoue, la ligne contenant le processus en question clignote en rouge.

Etats des documents

Le tableau ci-dessous présente les différents états du document.

Tableau 33. Etats du document

Etat	Description
Reçu	Le document a été reçu par le système et attend d'être traité.
En cours	Le document se trouve dans l'une des étapes de traitement suivantes : • **Incomplet**. Le système attend d'autres documents. • **Validation des données**. Le système contrôle le contenu du document. • **Conversion**. Le système convertit le document dans un autre protocole. • **File d'attente**. Par exemple, le document est en attente de routage vers le partenaire externe ou le partenaire interne.
Echec	Le traitement du document a été interrompu en raison d'erreurs dans le système, d'une validation des données ou de la présence de copies.
Succès	Message final signalant la fin du traitement du document a été transmis par le système au partenaire cible.

Affichage de documents dans le système

1. Cliquez sur **Outils** > **Analyse de document**. Le système affiche l'écran Recherche de l'analyse du document.
2. Sélectionnez les critères de recherche dans les listes déroulantes.

Tableau 34. Critères de recherche du document

Valeur	Description
Date & heure de début	Date et heure auxquelles le processus a commencé.
Date & heure de fin	Date et heure auxquelles le processus s'est terminé.
Partenaire source	Partenaire à l'initiative du processus métier (partenaire interne uniquement).
Partenaire cible	Partenaire ayant reçu le processus métier (partenaire interne uniquement).
Recherche	Recherche sur le type de document d'origine ou le type de document de destination.
Type de destination	Par exemple, production ou test. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.
Package	Décrit le format, l'empaquetage, le chiffrement et l'identification du type de contenu du document.
Protocole	Protocole de documents disponible pour les partenaires.
type de document	Processus métier spécifique.
Trier par	Trier les résultats par nom de partenaire source ou par nom de partenaire cible.
Régénérer	Contrôle si les résultats de la recherche sont régénérés périodiquement (partenaire interne uniquement).
Fréquence de régénération	Contrôle la fréquence de régénération des résultats de la recherche (partenaire interne uniquement).

3. Cliquez sur **Rechercher**. Le système affiche le Récapitulatif de l'analyse du document.

Affichage des caractéristiques du processus et de l'événement

1. Cliquez sur **Outils** > **Analyse de document**. Le système affiche l'écran Recherche de l'analyse du document.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche le Récapitulatif de l'analyse du document.
4. Cliquez sur l'icône Afficher les caractéristiques en regard des partenaires source et cible que vous souhaitez afficher. Le système affiche la liste de tous les documents qui correspondent aux partenaires sélectionnés. Les documents sont organisés en colonne en fonction de l'état de traitement du document.
5. Sélectionnez le lien de quantité dans les colonnes Reçu, En cours, Echec ou Succès. Le système présente les caractéristiques du traitement du document dans le Rapport de l'analyse du document. Si vous avez sélectionné Echec, le rapport inclut également un Récapitulatif d'événement du document.

Traitement du fichier XML personnalisé

WebSphere Partner Gateway V6.0 et versions antérieures offraient une prise en charge du traitement XML (Extensible Markup Language) personnalisé à l'aide de formats XML. Toutefois, ces formats XML utilisés par WebSphere Partner Gateway V6.0 et versions antérieures ne permettent pas l'utilisation complète du langage d'expression XPath pour extraire les informations de traitement des documents. C'est pourquoi dans WebSphere Partner Gateway V6.1, le fonctionnement des formats XML a été repensé. Dans WebSphere Partner Gateway V6.1, les expressions XPath version 1.0 peuvent être utilisées dans les formats. La puissance de traitement ajoutée pour la prise en charge complète de XPath limite la taille des fichiers qui peuvent être utilisés avec les formats XML XPath complets. Pour permettre le traitement des fichiers volumineux, vous pouvez sélectionner une option lors de la définition d'une famille de documents. Dans une famille pour laquelle l'option de traitement des fichiers volumineux a été définie, la puissance de traitement XPath est limitée de la même manière que dans WebSphere Partner Gateway V6.0 et versions antérieures, mais les fichiers volumineux peuvent être traités. Lorsque l'option de traitement des fichiers volumineux est utilisée dans une famille de documents, ces limites sont placées sur les expressions utilisées dans les formats XML stockés dans la famille :

1. Seuls les chemins d'éléments simples qui commencent à la racine du document peuvent être utilisés.
2. Les chemins d'éléments ne doivent pas contenir de préfixes d'espace de nom, même s'ils apparaissent dans les documents.

La fenêtre Gestion des formats XML contient une liste déroulante appelée Options de fichiers volumineux. Cette liste comporte les choix suivants : *Aucune*, *Utiliser le processeur de fichiers volumineux* et *Utiliser le processeur de fichiers volumineux avec espace de nom*. L'utilisateur doit sélectionner une option de traitement des fichiers volumineux s'il génère des formats XML correspondant à des documents volumineux qui ne peuvent pas être traités à l'aide du processeur XPath. L'option de traitement avec espace de nom signifie que les chemins d'éléments comprennent les préfixes d'espace de nom lorsqu'ils apparaissent dans un document.

Remarque : Cette option n'est plus modifiable une fois la famille créée. En effet, il se peut que la famille de documents contienne déjà des formats XML

qui ne seraient plus valides en cas de changement de type de famille. Le traitement du fichier XML personnalisé n'est pas disponible pour les partenaires.

Rapport du volume de document

L'outil Rapport du volume de document permet de gérer, suivre et résoudre les incidents liés à votre flux de documents de gestion. Le rapport affiche le volume de documents traités par le système dans un intervalle donné. Vous pouvez afficher, imprimer et enregistrer ce rapport afin de l'envoyer aux autres membres du personnel.

Vous pouvez également personnaliser ce rapport pour afficher les informations selon des critères de recherche spécifiques.

Le Rapport du volume de document affiche le nombre de documents en cours de traitement selon leur état :

Tableau 35. Etats du document

Valeur	Description
Nombre de documents reçus	Nombre total de documents reçus par le système.
En cours	Les documents qui sont à l'état En cours sont testés et validés. Aucune erreur n'a été détectée, mais le processus n'est pas encore terminé.
Echec	Le traitement du document a été interrompu en raison d'une erreur.
Succès	Message final signalant la fin du traitement du document a été transmis par le système au partenaire cible.

Utilisez ce rapport pour effectuer les tâches suivantes :

- Déterminer si les processus métier clés sont terminés.
- Suivre l'évolution du volume de processus pour le contrôle des coûts.
- Gérer l'état du processus (succès ou échec).
- Si vous êtes le partenaire interne, aider les partenaires à suivre les performances du processus.

Création d'un Rapport du volume de document

1. Cliquez sur **Outils** > **Rapport du volume de document**. Le système affiche l'écran Rapport du volume de document.
2. Sélectionnez les critères de recherche dans les listes déroulantes.

Tableau 36. Critères de recherche du rapport du volume de document

Valeur	Description
Date & heure de début	Date et heure auxquelles le processus a commencé.
Date & heure de fin	Date et heure auxquelles le processus s'est terminé.
Partenaire source	Partenaire ayant initialisé le processus métier (partenaire interne uniquement).
Partenaire cible	Partenaire ayant reçu le processus métier (partenaire interne uniquement).
Recherche	Recherche sur le type de document d'origine ou le type de document de destination.
Type de destination	Production ou test. Le type de destination Test est disponible uniquement sur les systèmes qui prennent en charge ce type de destination.
Package	Décrit le format, l'empaquetage, le chiffrement et l'identification du type de contenu du document.
Protocole	Type de protocole de processus, par exemple, XML, EDI, fichier à plat.
type de document	Processus métier spécifique.
Trier par	Trier les résultats en fonction de ce critère (type de document source ou type de document cible).
Résultats par page	Nombre d'enregistrements affichés par page.

3. Cliquez sur **Rechercher**. Le système affiche le rapport.

Exportation du Rapport du volume de document

1. Cliquez sur **Outils** > **Rapport du volume de document**. Le système affiche l'écran Rapport du volume de document.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche le rapport.
4. Cliquez sur l'icône Exporter l'état pour exporter un rapport. Naviguez jusqu'à l'emplacement souhaité pour enregistrer le fichier.

Remarque : Les rapports sont enregistrés au format CSV (comma-separated value). Le nom du fichier doit porter le suffixe ".csv".

Impression des rapports

1. Cliquez sur **Outils** > **Rapport du volume de document**. Le système affiche l'écran Rapport du volume de document.
2. Sélectionnez les critères de recherche dans les listes déroulantes.
3. Cliquez sur **Rechercher**. Le système affiche le rapport.
4. Cliquez sur l'icône Imprimer pour imprimer le rapport.

Test de la connexion du partenaire

La fonction de test de la connexion du partenaire permet de tester la destination ou le serveur Web. Si vous êtes le partenaire interne, vous pouvez également sélectionner un partenaire spécifique. Le test consiste à envoyer une requête POST vide à une destination ou à une adresse URL. La requête revient à accéder à l'URL de Yahoo (www.yahoo.com) dans la zone d'adresse de votre navigateur. Rien n'est envoyé ; il s'agit d'une requête vide. La réponse renvoyée par le destination ou le serveur Web indique son état :

- Si une réponse est renvoyée, le serveur est actif.
- Si rien n'est renvoyé, le serveur est inactif.

Important : La fonctionnalité de test de la connexion du partenaire fonctionne avec le protocole HTTP sans nécessiter de paramètres de connexion.

Pour tester une connexion de partenaire :

1. Cliquez sur **Outils > Test de la connexion du partenaire**. Le système affiche l'écran Test de la connexion du partenaire.
2. Sélectionnez les critères de test dans les listes déroulantes.

Tableau 37. Valeurs du test de la connexion du partenaire

Valeur	Description
Partenaire	Partenaire à tester (partenaire interne uniquement).
Destination	Affiche les destinations disponibles en fonction du partenaire sélectionné précédemment.
URL	Zone complétée dynamiquement en fonction de la destination sélectionnée précédemment.
Commande	Post ou Get.

3. Cliquez sur **Test de l'URL**. Le système affiche les résultats du test. Pour plus d'informations sur le code d'état renvoyé, voir les sections suivantes.

Codes de résultat du serveur Web

Série 200 :

- 200 - OK - Transmission réussie. Il ne s'agit pas d'une erreur. Il indique le fichier que vous avez demandé.
- 201 - Créé - La demande a été satisfaite et la ressource créée. La nouvelle ressource peut être référencée par les adresses URL renvoyées dans la zone d'en-tête de l'URL de la réponse, en attribuant l'URL le plus spécifique à la ressource indiquée par une zone d'en-tête Emplacement.
- 202 - Accepté - La demande a été acceptée en vue du traitement, mais celui-ci n'est pas encore terminé.
- 203 - Information non définitive - Les informations META renvoyées dans l'en-tête Entity-Header ne correspondent pas au jeu définitif tel qu'il est disponible sur le serveur d'origine, mais sont regroupées à partir d'une copie locale ou tierce.
- 204 - Pas de contenu - Le serveur a satisfait la demande, mais il n'a pas de nouvelles informations à renvoyer.
- 206 - Contenu partiel - Le serveur affiche la plage d'octets demandée dans le fichier. Il s'agit d'une nouveauté dans HTTP 1.1

Série 300 :

- 301 - Déplacé définitivement - La ressource demandée a changé d'adresse URL et toutes les références ultérieures à cette ressource doivent se faire à l'aide de l'un des URL renvoyés.
- 302 - Déplacé temporairement - La ressource demandée réside temporairement sous une nouvelle adresse URL. Redirection vers un nouvel URL. La page originale a changé. Il ne s'agit pas d'une erreur. La plupart des navigateurs recherchent automatiquement la nouvelle page lorsqu'ils voient ce résultat.

Série 400 :

- 400 - Requête erronée - Le serveur n'a pas pu traiter la requête car sa syntaxe est incorrecte. Le client a effectué une requête erronée.
- 401 - Non autorisé - La requête requiert l'authentification de l'utilisateur. La réponse doit inclure une zone d'en-tête WWW-Authenticate contenant une demande d'authentification applicable à la source demandée. L'utilisateur a demandé un document mais n'a pas fourni un nom d'utilisateur ou un mot de passe correct.
- 402 - Paiement exigé - Ce code n'est actuellement pas pris en charge, mais est réservé à un usage ultérieur.
- 403 - Interdit - Le serveur a traité la requête mais refuse de l'exécuter pour une raison inconnue. L'accès à ce document est expressément refusé. Cette erreur peut se produire lorsque le serveur Web ne dispose pas des droits de lecture pour le fichier que vous demandez. Le serveur refuse de vous envoyer le fichier. Il est possible que les droits d'accès ont été désactivés explicitement.
- 404 - Page introuvable - Le serveur ne trouve pas le document correspondant à l'URL demandé. Ce fichier n'existe pas. Vous recevez ce message lorsque vous indiquez une adresse URL incorrecte. Ce message peut également être envoyé si le serveur a été configuré en vue de protéger le document en déclarant celui-ci inexistant aux personnes non autorisées. Les erreurs 404 surviennent lorsque les pages demandées n'existent pas. Elles peuvent avoir différentes explications : une adresse URL incorrecte, un signet qui pointe vers un fichier qui n'existe plus, des moteurs de recherche qui recherchent un fichier robots.txt (utilisé pour marquer les pages que vous ne voulez pas que les moteurs de recherche indexent), des noms de fichiers incorrects, des liens erronés à partir de votre site ou d'autres sites, etc.
- 405 - Méthode non autorisée - La méthode indiquée dans la ligne de la requête n'est pas autorisée pour la ressource identifiée par l'URL.
- 406 - Non acceptable - Le serveur a trouvé une ressource correspondant à l'URL de la requête, mais qui ne répond pas aux conditions identifiées par les en-têtes de requête Accept et Accept-Encoding.
- 407 - Authentification proxy exigée - Ce code est réservé à un usage ultérieur. Il est similaire au code 401 (Non autorisé) mais indique que le client doit s'authentifier auprès d'un proxy. HTTP 1.0 ne permet pas l'authentification de proxy.
- 408 - Délai de requête dépassé - Le client n'a pas émis de requête dans le délai d'attente du serveur.
- 409 - Conflit - La requête n'a pas pu aboutir en raison d'un conflit avec l'état en cours de la ressource.
- 410 - Supprimé - La ressource demandée n'est plus disponible sur le serveur et aucune adresse de réacheminement n'est indiquée.
- 411 - Autorisation refusée - Les données d'identification de requête fournies par le client ont été rejetées par le serveur ou sont insuffisantes pour autoriser l'accès à la ressource.

- 412 - Echec de précondition
- 413 - Entité requête trop grande
- 414 - URI requête trop long
- 415 - Type de support non pris en charge

Série 500 :

- 500 - Erreur interne du serveur - Le serveur HTTP a rencontré une condition inattendue qui l'a empêché de traiter la requête. Un incident s'est produit sur le serveur web, qui n'est pas en mesure de renvoyer une réponse appropriée. Le navigateur ne peut généralement rien faire pour corriger cette erreur ; l'administrateur du serveur devra probablement consulter le fichier journal du serveur pour tenter de résoudre l'incident. Il s'agit souvent d'un message d'erreur correspondant à un script CGI qui n'a pas été correctement codé.
- 501 - Méthode non implémentée - Le serveur ne prend pas en charge la fonctionnalité requise pour traiter la requête. Une méthode d'application (GET ou POST) n'est pas implémentée.
- 502 - Erreur de destination - Le serveur a reçu une réponse non valide en provenance de la destination ou du serveur amont contacté pour tenter d'exécuter la requête.
- 503 - Service indisponible - Le serveur ne peut pas traiter la requête en raison d'une surcharge temporaire ou d'une maintenance du serveur. Le serveur manque de ressources.
- 504 - Délai d'accès à la destination dépassé - Le serveur n'a pas reçu de réponse dans le délai imparti de la part de la destination ou du serveur amont auquel il a accédé pour tenter de traiter la requête.
- 505 - Version HTTP non prise en charge

Rapports d'EDI

Utilisez Rapports d'EDI pour rechercher les FA (accusés de réception fonctionnels) d'EDI (échange de données informatisé) en retard. Vous pourrez rechercher également les transactions d'EDI rejetées. Les sections suivantes détaillent la procédure à suivre pour utiliser Rapports d'EDI.

Recherche de FA d'EDI en retard

La page Recherche de FA d'EDI en retard propose des critères de recherche permettant d'effectuer des recherche de FA (accusés de réception fonctionnels) d'EDI (Echange de Données Informatisé) en retard.

Remarque : Tout enregistrement, renvoyé par les recherches de retards de FA d'EDI précédentes, qui a été supprimé des rapports résultants sera ignoré lors des recherches suivantes. Les enregistrements supprimés n'apparaîtront donc pas dans les rapports ultérieurs. Pour supprimer des enregistrements d'un rapport, cliquez sur **Ignorer les rapports sélectionnés** dans la page Rapport de retards de FA d'EDI. Seul l'utilisateur concentrateur peut supprimer des enregistrements d'un rapport.

Pour rechercher des enregistrements de FA d'EDI en retard, procédez comme suit :

1. Cliquez sur **Outils > Rapports d'EDI**. L'écran de recherche FA d'EDI en retard s'affiche.

2. Sélectionnez un ou plusieurs critères de recherche dans la liste déroulante :

Tableau 38. Critères de recherche de retard de FA d'EDI

Valeur	Description
Date & heure de début	Date et heure auxquelles la transaction a été lancée.
Date & heure de fin	Date et heure auxquelles la transaction s'est achevée.
Partenaire source	Partenaire à l'initiative de la transaction.
Partenaire cible	Partenaire ayant reçu la transaction.
Recherche sur	Recherche sur le type du document source ou le type du document cible.
Package	Décrit le format, l'empaquetage, le chiffrement et l'identification du type de contenu du document.
Protocole	Type de protocole de processus, par exemple, XML, EDI, fichier à plat. Les protocoles affichés varient selon la valeur choisie dans la zone Package.
Type de document	Type spécifique du document. Les types affichés varient en fonction de la valeur sélectionnée dans la zone Protocole.
ID référence	Indique un ID de transaction.
Trier par	Précise les critères de tri des résultats de la recherche. Les critères par défaut sont En retard de et Décroissant. Décroissant permet d'afficher en premier les plus gros retards de FA. Croissant permet d'afficher en premier les plus légers retards de FA.
Résultats par page	Précise le nombre de résultats de recherche de transaction à afficher sur chaque page.

3. Cliquez sur **Rechercher** pour afficher le rapport Recherche de retards de FA d'EDI.

Viewing EDI FA Overdue package reports

En fonction des critères de recherche sélectionnés sur la page Recherche des retards de FA d'EDI, les résultats s'afficheront sur la page Rapport des retards de FA d'EDI.

Les données suivantes, le cas échéant, s'affichent dans le rapport de FA EDI en retard.

Tableau 39. Rapport de retard de FA d'EDI

Valeur	Description
Date	Date à laquelle l'EDI a été envoyé par le partenaire source au partenaire cible.
Heure	Heure (GMT) à laquelle l'EDI a été envoyé par le partenaire source au partenaire cible.
ActivityID	ID virtuellement unique (ou VUID) de la transaction.
Partenaire d'échange source	Partenaire ayant envoyé la transaction.
Package source	Package source de la transaction.
Protocole source	Protocole source de la transaction.
Type de document source	Type du document source de la transaction.
Partenaire d'échange cible	Partenaire ayant reçu la transaction.
Package cible	Package cible de la transaction.
Protocole cible	Protocole cible de la transaction.
Type de document cible	Type du document cible de la transaction.
Numéro d'échange	Numéro d'échange de la transaction.
Numéro de groupe	Numéro de groupe de la transaction.
Numéro de transaction	Numéro identifiant la transaction.
Echéance du FA	Date d'échéance du FA de la transaction.
En retard de	Durée du retard du FA.
Ignorer les enregistrements sélectionnés	Lorsque vous sélectionnez cette option pour un enregistrement, celui-ci est supprimé du rapport. Lorsqu'un enregistrement est supprimé d'un rapport, il est ignoré par les recherches de retards FA EDI ultérieures, et il n'apparaît donc pas dans les rapports résultants. Seul l'utilisateur concentrateur peut supprimer des enregistrements d'un rapport.

Recherche de transactions d'EDI rejetées

La page Recherche de transactions d'EDI rejetées présente des critères de recherche permettant d'effectuer des recherches de transactions d'EDI (Echange de Données Informatisé) dont le FA (accusé de réception fonctionnel) contient un code d'erreur. Les enregistrements de transaction sans FA ne sont pas renvoyés par une recherche de transaction rejetée EDI.

Pour rechercher des enregistrements de retards d'EDI rejetés, procédez comme suit :

1. Cliquez sur **Outils > Rapports d'EDI > Rapports d'EDI rejetés**.

2. Sélectionnez un ou plusieurs critères de recherche dans la liste déroulante :

Tableau 40. Critères de recherche de transactions d'EDI rejetées

Valeur	Description
Date & heure de début	Date et heure auxquelles la transaction a été lancée.
Date & heure de fin	Date et heure auxquelles la transaction s'est achevée.
Partenaire source	Partenaire à l'initiative de la transaction.
Partenaire cible	Partenaire ayant reçu la transaction.
Recherche sur	Recherche sur le type du document source ou le type du document cible.
Package	Décrit le format, l'empaquetage, le chiffrement et l'identification du type de contenu du document.
Protocole	Type de protocole de processus, par exemple, XML, EDI, fichier à plat. Les protocoles affichés varient selon la valeur choisie dans la zone Package.
Type de document	Type spécifique du document. Les types affichés varient en fonction de la valeur sélectionnée dans la zone Protocole.
ID référence	Indique un ID de transaction.
Trier par	Précise les critères de tri des résultats de la recherche. Les critères par défaut sont En retard de et Décroissant. Décroissant permet d'afficher en premier les plus gros retards de FA. Croissant permet d'afficher en premier les plus légers retards de FA.
Résultats par page	Précise le nombre de résultats de recherche de transaction à afficher sur chaque page.

3. Cliquez sur **Rechercher** pour afficher le rapport Transactions d'EDI rejetées.

Affichage des rapports sur les transactions d'EDI rejetées

En fonction des critères de recherche sélectionnés sur la page Recherche des transactions d'EDI rejetées, les résultats s'afficheront sur la page Rapport des transactions d'EDI rejetées.

Les données suivantes, le cas échéant, s'affichent dans le rapport Transactions d'EDI rejetées.

Tableau 41. Rapport Transactions d'EDI rejetées

Valeur	Description
Date	Date à laquelle l'EDI a été reçu.
Heure	Heure (GMT) à laquelle la transaction d'EDI a été envoyée par le partenaire source au partenaire cible.
ActivityID	ID virtuellement unique (ou VUID) de la transaction.
Partenaire d'échange source	Partenaire ayant envoyé la transaction.
Package source	Package source de la transaction.
Protocole source	Protocole source de la transaction.
Type de document source	Type du document source de la transaction.
Partenaire d'échange cible	Partenaire ayant reçu la transaction.
Package cible	Package cible de la transaction.
Protocole cible	Protocole cible de la transaction.
Type de document cible	Type du document cible de la transaction.
Numéro d'échange	Numéro d'échange de la transaction.
Numéro de groupe	Numéro de groupe de la transaction.
Numéro de transaction	Numéro identifiant la transaction.
Code d'état	Code de l'état du FA.
Texte d'état	Texte de l'état du FA.

Rapports FTP

Rapports FTP permet de connaître les caractéristiques des Statistiques FTP et des Connexions FTP.

Statistiques FTP

La page Statistiques FTP affiche l'état du serveur FTP en lecture seule.

Remarque : Les statistiques ne s'affichent pas si le serveur FTP ou le serveur de gestion FTP n'est pas disponible.

Pour voir l'état du serveur FTP, procédez comme suit :

1. Cliquez sur **Outils > Rapports FTP**. La page Statistiques FTP s'affiche.

2. Les informations suivantes s'affichent sur l'état du serveur :

Tableau 42. Statistiques FTP

Valeur	Description
Heure de démarrage du serveur	Heure de démarrage du serveur FTP.
Nombre de répertoires créés	Nombre de répertoires créés par les utilisateurs à l'aide de mkdir.
Nombre de répertoires supprimés	Nombre de répertoires supprimés par les utilisateurs à l'aide de rmdir.
Nombre de fichiers chargés	Nombre de fichiers chargés par tous les utilisateurs.
Nombre de fichiers téléchargés	Nombre de fichiers téléchargés par tous les utilisateurs.
Nombre de fichiers supprimés	Nombre de fichiers supprimés par tous les utilisateurs à l'aide de la commande delete.
Octets chargés	Nombre total d'octets chargés.
Octets téléchargés	Nombre total d'octets téléchargés.
Ouvertures de session existantes	Affiche le nombre d'ouvertures de session existantes.
Nombre total d'ouvertures de session	Nombre total d'ouvertures de session depuis la dernière réinitialisation.
Nombre total d'échecs d'ouverture de session	Nombre total d'échecs à l'ouverture de session.
Connexions en cours	Connexions en cours depuis la dernière réinitialisation.
Nombre total de connexions	Nombre total de connexions depuis la dernière réinitialisation.

3. Cliquez sur **Recharger** pour actualiser les ouvertures de session en cours.
4. Cliquez sur **Réinitialiser** pour remettre à zéro les zones.

Connexions FTP

Prenez connaissance des Connexions FTP en suivant les étapes ci-dessous :

1. Cliquez sur **Outils > Rapports FTP > Connexions FTP.**
2. Les informations suivantes s'affichent sur les connexions dans le rapport :

Tableau 43. Connexions FTP

Valeur	Description
Nom de connexion	ID utilisateur d'ouverture de session pour cette connexion. Si cette zone est vide, cela signifie que l'utilisateur a établi une connexion, mais n'a pas ouvert de session.
Heure d'ouverture de session	Heure à laquelle l'utilisateur a ouvert une session. Si cette zone est vide, cela signifie que l'utilisateur a simplement établi une connexion.
Heure du dernier accès	Heure à laquelle l'utilisateur a accédé à cette connexion pour la dernière fois. Si cette zone est vide, cela signifie que l'utilisateur a simplement ouvert une session, mais n'a encore émis aucune commande.
Adresse du client	Adresse IP à partir de laquelle l'utilisateur a ouvert une session.

Glossaire

A

Actif : Etat dans lequel un participant a terminé de tester des règles de gestion, et dans lequel le partenaire interne a émis une demande de service afin de leur attribuer l'état Actif.

Action : (1) Actions exécutées sur un document par le système pour vérifier sa compatibilité avec les exigences commerciales entre les partenaires. (2) Série d'étapes de traitement, telle que la validation et la transformation de documents.

Action commerciale en réponse : Identifie le type de document de gestion envoyé en réponse à une action dans le même processus.

Activation : Connexion d'un partenaire au système.

Administrateur du compte : Le module Administrateur du compte vous permet d'afficher et de modifier les informations qui identifient votre entreprise sur le réseau. Cet écran permet également de gérer les droits d'accès à la console des autres personnes de l'entreprise.

Alerte : Les alertes fournissent une notification et une résolution rapides lorsque des limites de fonctionnement prédéfinies ont été atteintes. Une alerte est un message électronique texte envoyé à des personnes ou à une liste de diffusion de personnes clés situées en dehors ou sur le réseau. Les alertes peuvent reposer sur l'occurrence d'un événement système ou d'un volume de processus prévu.

Allègement des données : Processus qui consiste à tester et à réparer les erreurs présentes dans la structure et le format d'un document conformément aux normes du processus métier.

Approvisionnement : L'approvisionnement (ou intégration) consiste à effectuer une série d'étapes requises pour connecter une passerelle B2B d'utilisateur à l'infrastructure du système.

C

Caractère générique : Les critères des recherches avec caractères génériques comprennent l'astérisque (*).

Chorégraphie : Ordre des documents nécessaire pour exécuter un processus métier.

Classification : Identifie le rôle du partenaire dans un processus métier.

Code du signal commercial : Identifie le type de signal (document) envoyé en réponse à une action. Il peut s'agir d'un accusé de réception d'acceptation ou d'une exception générale.

Connexion partenaire : Une connexion partenaire définit la connexion établie entre deux environnements de membre de communauté spécifiques, à travers laquelle un processus unique est exécuté.

Console de communauté : La console de communauté est un outil Web qui permet de surveiller le flux des documents de gestion de votre entreprise à destination et en provenance du partenaire interne ou des partenaires externes.

Contact abonné : Un contact abonné est une personne qui a été désignée pour recevoir des alertes par courrier électronique.

Conversion : Lorsqu'un document est converti d'un protocole à un autre.

D

Définition de document : Fournit au système toutes les informations nécessaires pour recevoir, traiter et acheminer les documents entre les membres de la communauté. Les types de définition de document incluent notamment le package, le protocole, le type de document, l'activité et l'action.

Désenveloppement : Extraction d'un document d'une enveloppe EDI.

Destination : Point de réseau B2B qui permet d'accéder à un autre réseau. Les problèmes de compatibilité et de conversion des données peuvent être résolus par une destination, qui assure le transfert des données.

Document : Ensemble d'informations respectant les conventions d'une entreprise. Il peut s'agir de textes, d'images et de fichiers son.

DUNS : Le numéro D&B D-U-N-S est une séquence d'identification unique à neuf chiffres qui fournit des identifiants uniques d'entités de gestion en assurant un lien entre les familles d'entreprises. D&B associe les numéros D&B D-U-N-S des compagnies mères, des filiales, des sièges sociaux et des succursales de plus de 64 millions de membres de familles d'entreprises à travers le monde. Utilisé par les organismes mondiaux les plus prestigieux en matière de normes, il est reconnu, recommandé et souvent exigé par plus de 50 organisations, parmi lesquelles les industries, les associations d'affaires, les Nations-Unies, le

Gouvernement fédéral américain, le Gouvernement australien, ainsi que la Communauté européenne. Dans l'économie mondiale d'aujourd'hui, le numéro D&B D-U-N-S est devenu la norme du suivi des entreprises à l'échelle mondiale.

E

EDI : Echangé informatisé des informations dans un format structuré prédéfini. L'objectif du système EDI est de remplacer les formulaires d'entreprise prédéfinis, comme les bons de commande et les factures, par des formulaires électroniques définis de la même manière.

Enfant du partenaire interne : Un enfant de partenaire interne est un type spécifique de partenaire qui agit comme un partenaire dans la console mais comme un partenaire interne lors d'un routage.

Etat : (1) Les documents traités par le système ont quatre états : (2) reçu, en cours, échec ou succès.

Evénement : Message généré par le système associé au traitement des documents.

F

Fermé : Date et heure auxquelles le dernier document d'un processus est transféré ou qu'un processus est annulé.

Filtre : Supprimer des données dans une sous-transaction en fonction de paramètres prédéfinis.

FTP : File Transfer Protocol (FTP), protocole Internet standard qui permet d'échanger des fichiers entre des ordinateurs sur Internet.

G

Gestionnaire entrait : Extrait les documents du serveur NAS et les prépare pour la tâche correspondante effectuée par le moteur de processus métier.

Global : Contact pouvant se voir affecter des alertes par le partenaire et le partenaire interne.

Groupe : Ensemble d'utilisateurs disposant des droits d'accès à la console pour réaliser les opérations sélectionnées.

H

HTTP : Le protocole HTTP (Hypertext Transfer Protocol) est l'ensemble des règles (protocole) qui permettent d'échanger des fichiers (texte, images graphiques, son, vidéo et d'autres fichiers multimédia) sur le Web.

HTTPS : Le protocole HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) est un protocole Web qui chiffre et déchiffre les demandes de page de l'utilisateur ainsi que les pages renvoyées par le serveur Web.

I

ID de transaction : Numéro d'ID du processus métier.

ID d'instance d'action : Identifie les documents dont le contenu est de nature commerciale, comme un bon de commande ou un appel d'offres.

ID d'instance du processus : Numéro d'identification unique d'un processus métier spécifique.

ID d'instance du signal : Identifie les documents qui constituent des accusés de réception positifs ou négatifs en réponse aux actions.

ID en réponse : Numéro d'ID de l'Action métier en réponse.

J

Jeu de certificats : Jeu de certificats principaux et secondaires pouvant être associés à une connexion de participant.

M

Mode de fonctionnement : Identifie les documents qui sont transférés à une passerelle spécifique en cours de test ou de production.

N

Nombre de tentatives : Indique si la transaction constitue une première tentative ou une relance. La valeur 1 correspond à une première tentative. La valeur 2 ou plus correspond au nombre de relances.

O

Outils : Le module Outils vous permet d'identifier et de résoudre les incidents liés aux processus en affichant les documents défaillants, les zones de données et les événements associés.

P

Packages : Permet d'identifier les formats d'empaquetage du document qui peuvent être reçus par le serveur système. Par exemple, AS1 et AS2.

Partenaire externe : Membre de la communauté du concentrateur qui échange des transactions commerciales avec le partenaire interne.

PIP (Partner Interface Process) : Définit les processus métier entre les partenaires internes et les partenaires (dans WebSphere Partner Gateway, les partenaires sont des participants). Chaque processus PIP identifie un document de gestion spécifique et la manière dont il est traité.

Processus métier : Ensemble prédéfini de transactions qui représentent la méthode d'exécution des tâches nécessaires pour réaliser un objectif commercial.

Production : Passerelle de destination utilisée pour transférer des documents actifs.

Profil : Le module Profil vous permet d'afficher et de modifier les informations qui identifient votre entreprise sur le système.

Protocole de document : Ensemble de règles et d'instructions (protocole) qui déterminent la mise en forme et la transmission des informations sur un réseau informatique. Il peut s'agit par exemple du protocole RosettaNet, XML, du fichier à plat et du protocole EDI.

Protocole de transport : Ensemble des règles (protocole) utilisées pour envoyer des données sous la forme d'unités de message entre les ordinateurs sur Internet. Il peut s'agir des protocoles HTTP, HTTPS, SMTP et FTP.

Protocoles : Permettent d'identifier des types spécifiques de formats de document pour différents processus métier. Par exemple, RosettaNet et XML.

R

Rapports : Le module Rapports permet aux utilisateurs de créer des rapports détaillés sur le volume de documents traités ainsi que sur les événements générés par le système.

Remplacer : Remplacer les données dans une sous-transaction par d'autres données selon des paramètres prédéfinis.

RNIF : Le protocole RosettaNet Implementation Framework (RNIF) est une instruction qui permet de créer un conteneur d'enveloppe standard pour tous les processus PIP (Partner Interface Process).

RTF : Le format RTF (Rich Text Format) est un format de fichier qui permet d'échanger des fichiers texte entre plusieurs traitements de texte sur des systèmes d'exploitation différents. Par exemple, vous pouvez créer un fichier à l'aide de Microsoft Word sous Windows 98, l'enregistrer au format RTF (il portera l'extension .rtf) et l'envoyer à un utilisateur de WordPerfect 6.0 sous Windows 3.1.

S

Service : Identifie si le message est basé sur le protocole RosettaNet.

Servlet : Programme exécuté sur le serveur Web qui enregistre le document entrant sur le serveur NAS.

Signal : Document envoyé en réponse à une action.

Signature numérique : Une signature numérique est une signature électronique utilisée pour authentifier l'identité des partenaires, et qui garantit l'intégrité du contenu d'origine d'un document qui a été envoyé.

SMTP : Le protocole SMTP (Simple Mail Transfer Protocol) est utilisé pour échanger des messages électroniques.

SR : Demande de service

SSL : Le protocole SSL (Secure sockets layer) est une méthode sécurisée d'envoi des données qui utilise le protocole HTTP.

T

Test : Etat dans lequel un partenaire procède à l'allègement des données ou au test des règles de gestion pendant le processus d'approvisionnement.

Test des règles de gestion : Processus de test et de réparation des erreurs dans un document entre les partenaires.

Transaction : Série d'échange d'informations et de travaux associés traitée comme une unité dans le but de transférer des documents de gestion entre les partenaires.

Transformer : Remplacer le contenu d'un document par les données d'une table de références croisées.

U

URL : Une adresse URL (Uniform Resource Locator) est l'adresse d'un document ou d'un processus accessible sur Internet.

V

Validation : La validation est l'opération qui consiste à comparer la sous-transaction d'un processus aux exigences énoncées afin de déterminer sa validité ou son invalidité. La séquence de contenu et de transaction sont des paramètres classiques.

Version : Version d'un protocole de document.

Version du signal : Version du processus métier envoyé comme signal.

Visibilité : La visibilité définit si un contact peut être affecté à une alerte par un partenaire (local) ou par le partenaire interne (global).

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 caractéristiques, 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 Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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. Ce document 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.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

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.

COPYRIGHT

Le présent logiciel contient des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Websphere Partner Gateway contient du code désigné ICU4J dont la licence d'utilisation vous est accordée par IBM sous les conditions stipulées par les

Conditions Internationales d'Utilisation de Logiciels IBM, auxquelles s'appliquent les dispositions concernant les composants exclus. Toutefois, IBM est tenu de vous informer des remarques suivantes :

COPYRIGHT ET AUTORISATION

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.

LE LOGICIEL EST FOURNI ″EN L'ETAT″ SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. 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 relatives aux interfaces de programmation

Les informations relatives aux interfaces de programmation, lorsqu'elles sont disponibles, ont pour objet de vous aider à créer des applications à l'aide de ce programme.

Les interfaces de programmation générique permettent de concevoir des applications qui utilisent les services des outils de ce programme.

Toutefois, ces informations peuvent également contenir des données de diagnostic ainsi que les modifications et les optimisations effectuées. Ces informations sont mises à votre disposition pour vous permettre de résoudre les incidents liés à vos applications.

Avertissement : N'utilisez pas les informations relatives aux diagnostics, aux modifications et à l'optimisation comme une interface de programmation dans la mesure où elles sont susceptibles d'être modifiées.

Marques commerciales et marques de service

Les termes qui suivent sont des marques d'International Business Machines Corporation aux Etats-Unis et/ou dans certains autres pays :

IBM, le logo IBM, AIX, CICS, DB2, DB2 Universal Database, IBMLink, IMS, MQSeries, MVS, OS/390, WebSphere et 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 ainsi que tous les logos 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 and Advanced Editions, version 6.1.

Index

A

B

C

D

E

F

G

I

M

N

O

P

R

S

T

U

V

Z