

WebSphere® IBM WebSphere Partner Gateway Enterprise et Advanced
Editions
Version 6.2.1

Guide du partenaire

IBM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 113.

janvier 2011

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

© Copyright IBM France 2011. Tous droits réservés

© **Copyright IBM Corporation 2010, 2011.**

Table des matières

Avis aux lecteurs canadiens v

Chapitre 1. A propos de ce guide 1

| | |
|---|---|
| Public concerné | 1 |
| Conventions typographiques | 1 |
| Documents associés | 2 |
| Nouveautés de l'édition 6.2.1 | 3 |

Chapitre 2. Introduction 5

| | |
|---|---|
| Communauté du concentrateur | 5 |
| Administrateur du concentrateur | 5 |
| Partenaire interne. | 5 |
| Partenaires externes | 5 |
| Icônes de la console de communauté | 6 |
| Utilisation de la console de communauté | 8 |

Chapitre 3. Configuration de votre environnement WebSphere Partner Gateway 9

| | |
|---|----|
| Connexion à la console de communauté | 9 |
| Vérification du profil de votre partenaire | 10 |
| Affichage et édition de votre profil partenaire | 10 |
| Création d'une destination | 11 |
| Examen des fonctions B2B | 11 |
| Définitions de type de document | 12 |
| Révision et édition des fonctions B2B : | 13 |
| Création et installation de certificats | 14 |
| Dispositions du certificat | 15 |
| Types de certificat et formats pris en charges | 17 |
| Serveur SSL et authentification client | 18 |
| Configuration de certificats SSL entrants. | 18 |
| Installation de certificats de chiffrement sortants | 20 |
| Utilisation de certificats pour activer la signature numérique. | 25 |
| Création d'utilisateurs | 26 |
| Création d'utilisateurs | 26 |
| Configuration d'un utilisateur FTP et SFTP | 28 |
| Création des informations de contact | 28 |
| Création d'alertes et ajout de contacts. | 30 |
| Création d'une alerte dépendant du volume | 32 |
| Création d'une alerte de type événement | 34 |
| Ajout d'un contact à une alerte existante. | 36 |
| Création d'une adresse | 37 |

Chapitre 4. Création de destinations 39

| | |
|---|----|
| Présentation | 39 |
| Configuration d'une destination HTTP | 40 |
| Détails de destination | 40 |
| Configuration de la destination. | 40 |
| Configuration d'une destination HTTPS | 41 |
| Caractéristiques des destinations | 41 |
| Configuration de la destination. | 42 |
| Configuration d'une destination FTP | 42 |
| Détails de destination | 43 |

| | |
|--|----|
| Configuration de la destination. | 43 |
| Configuration d'une destination SMTP | 44 |
| Détails de destination | 44 |
| Configuration de la destination. | 44 |
| Configuration d'une destination JMS | 45 |
| Détails de destination | 45 |
| Configuration de la destination. | 45 |
| Configuration d'une destination fichier-répertoire. | 46 |
| Détails de destination | 47 |
| Configuration de la destination. | 47 |
| Configuration d'une destination FTPS | 48 |
| Détails de destination | 48 |
| Configuration de la destination. | 48 |
| Configuration d'une destination de script FTP | 49 |
| Création du script FTP | 49 |
| Commandes de script FTP | 50 |
| Destinations de script FTP | 51 |
| Détails de destination | 51 |
| Configuration de la destination. | 51 |
| Attributs définis par l'utilisateur | 52 |
| Planification | 52 |
| Configuration d'une destination SFTP | 53 |
| Création de destinations SFTP sur les systèmes sur lesquels la sécurité administrative WAS est activée | 53 |
| Caractéristiques de la destination | 54 |
| Configuration de destination | 54 |
| Configuration de gestionnaires | 55 |
| Spécification d'une destination par défaut | 55 |

Chapitre 5. Gestion des connexions de la communauté et des utilisateurs : Administrateur du compte 57

| | |
|---|----|
| Gestion des destinations | 57 |
| Affichage d'une liste de destinations | 57 |
| Affichage ou édition des caractéristiques de la destination | 58 |
| Affichage, sélection ou édition de vos destinations par défaut | 58 |
| Affichage de la destination Emplacement d'utilisation | 58 |
| Suppression de la destination | 59 |
| Gestion des certificats | 59 |
| Affichage et édition des caractéristiques du certificat numérique | 59 |
| Désactivation d'un certificat numérique | 59 |
| Gestion des contacts | 60 |
| Affichage ou édition des caractéristiques du contact | 60 |
| Suppression d'un contact | 62 |
| Gestion des alertes | 62 |
| Affichage ou édition des caractéristiques de l'alerte et des contacts | 62 |
| Recherche d'alertes | 63 |
| Désactivation ou activation d'une alerte | 63 |

| | |
|-------------------------------------|----|
| Retrait d'une alerte | 64 |
| Notification d'événement | 64 |
| Gestion des adresses | 64 |
| Edition d'une adresse | 64 |
| Suppression d'une adresse | 65 |

Chapitre 6. Affichage des événements et des documents : Afficheurs 67

| | |
|--|----|
| Afficheur d'événements | 67 |
| Types d'événement | 68 |
| Exécution des tâches de l'Afficheur d'événements | 68 |
| Recherche d'événements | 69 |
| Affichage des caractéristiques de l'événement . . | 70 |
| Événements d'erreur | 70 |
| Afficheur AS | 71 |
| Exécution des tâches de l'Afficheur AS | 71 |
| Recherche de messages | 72 |
| Affichage des détails relatifs à un message . . . | 73 |
| Afficheur ebMS | 74 |
| Exécution des tâches de l'afficheur ebMS . . . | 74 |
| Recherche de processus ebMS | 74 |
| Affichage des caractéristiques des processus ebMS | 75 |
| Affichage des documents de base | 75 |
| Affichage de l'état des documents | 76 |
| Afficheur RosettaNet | 76 |
| Exécution des tâches de l'Afficheur RosettaNet | 76 |
| Recherche de processus RosettaNet | 77 |
| Affichage des caractéristiques du processus RosettaNet. | 78 |
| Affichage de documents bruts | 78 |
| Afficheur de documents | 79 |
| Recherche de documents | 79 |
| Affichage des caractéristiques du document, des événements et du document brut | 81 |
| Affichage des erreurs de validation des données | 82 |
| Utilisation de la fonction Arrêt du processus . . | 84 |
| File d'attente de destination | 84 |
| Affichage de la liste de destinations | 84 |
| Affichage des documents mis en file d'attente . . | 86 |
| Suppression de documents de la file d'attente de livraison | 87 |

| | |
|---|----|
| Affichage des détails relatifs à une destination. . . | 87 |
| Modification de l'état de la destination | 87 |

Chapitre 7. Analyse du type de document : Outils. 89

| | |
|---|-----|
| Analyse de document | 89 |
| Etats du document | 89 |
| Affichage de documents dans le système | 90 |
| Affichage des caractéristiques du processus et de l'événement | 91 |
| Traitement du fichier XML personnalisé | 91 |
| Rapport du volume de document | 92 |
| Création d'un rapport du volume de document | 92 |
| Exportation du rapport du volume de document | 93 |
| Impression de rapports | 93 |
| Test de la connexion du partenaire | 94 |
| Codes de résultat du serveur Web | 94 |
| Rapports EDI. | 96 |
| Recherche de retard EDI FA | 96 |
| Recherche de transactions d'EDI rejetées. | 98 |
| Rapports FTP | 100 |
| Statistiques FTP | 100 |
| Connexions FTP | 101 |

Chapitre 8. Boîte aux lettres Web . . . 103

| | |
|---|-----|
| Fonctions de la boîte aux lettres Web | 103 |
| Boîte de réception | 103 |
| Boîte d'envoi | 104 |
| Envoyer le fichier | 105 |
| Limitations de la boîte aux lettres Web | 105 |

Chapitre 9. Glossaire 107

Remarques 113

| | |
|--|-----|
| Documentation sur l'interface de programmation | 115 |
| Marques et services | 116 |

Index 117

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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








OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Chapitre 1. A propos de ce guide

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 commandes 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. |
| <i>Italique</i> | 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. |
| <i>Police monospace en italique</i> | 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) | (fichiers PDF uniquement) Des guillemets entourent les références croisées vers d'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, <code>option[,...]</code> 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, <code><nom_serveur><nom_connecteur>tmp.log</code> . |
| \, / | | 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'intégralité de la documentation disponible avec ce produit comprend des informations détaillées sur l'installation, la configuration, l'administration et l'utilisation de WebSphere Partner Gateway Enterprise Edition et Advanced Edition.

Vous pouvez télécharger cette documentation ou la consulter directement en ligne à l'adresse suivante :

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

Remarque : Des informations importantes relatives à ce produit peuvent être disponibles dans les notes techniques et les lettres d'informations du service d'assistance émises après la publication de ce document. 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 la zone correspondant au composant qui vous intéresse et consultez les sections Technotes (notes techniques) et Flashes (lettres d'informations).

Nouveautés de l'édition 6.2.1

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

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

Chapitre 2. Introduction

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 documents 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 le rapport |
|  | Destination désactivée |
|  | Masquer les critères de recherche |
|  | Modifier |
|  | Le dossier ne contient pas de donnée |
|  | Ouvrir l'agenda |
|  | Activer/désactiver le classement des documents |

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

| Icône | Nom de l'icône |
|---|---|
|  | Pause |
|  | 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 |
| Help | 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 : Seuls les utilisateurs dotés de droits d’affichage pour l’afficheur d’événements peuvent visualiser 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. Elle 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 Administrateur du compte de la console sont principalement utilisés lors de la configuration de WebSphere Partner Gateway, puis pour la maintenance.

Chapitre 3. 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 du profil de votre partenaire », à la page 10
3. « Création d'une destination », à la page 11
4. « Examen des fonctions B2B », à la page 11
5. « Création et installation de certificats », à la page 14
6. « Création d'utilisateurs », à la page 26
7. « Configuration d'un utilisateur FTP et SFTP », à la page 28
8. « Création des informations de contact », à la page 28
9. « Création d'alertes et ajout de contacts », à la page 30
10. « Création d'une adresse », à la page 37

Connexion à la console de communauté

Pourquoi et quand exécuter cette tâche

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

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

1. Ouvrez un navigateur Web et entrez l'URL suivante pour afficher la console :
`http://<nom d'hôte>.<domaine>:58080/console` (unsecure)
`https://<nom d'hôte>.<domaine>:58443/console` (secure)
Où <nom d'hôte> et <domaine> correspondent au nom et à l'emplacement de la machine hébergeant la console de communauté.

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

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

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

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

Remarque : Dans le navigateur Firefox, si vous enregistrez le nom d'utilisateur et le mot de passe dans la page de connexion, les valeurs enregistrées pour le nom d'utilisateur et le mot de passe sont insérées automatiquement dans les écrans de l'utilisateur qui comportent des zones de nom d'utilisateur et de mot de passe. Il en est ainsi qu'il s'agisse ou non d'une page de connexion. Par exemple, dans la page Créer un utilisateur, la zone Télécopie est pré-remplie avec les valeurs du mot de passe et du nom d'utilisateur.

6. Cliquez sur **Sauvegarder**. Le système affiche l'écran d'entrée de la console.

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

Vérification du profil de votre partenaire

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, Partenaire externe de simulateur RN et Partenaire interne de simulateur RN.

Remarque : Vous pouvez éditer votre propre profil en utilisation l'administration de compte uniquement si l'opérateur de concentrateur fournit un accès en lecture-écriture, ce qui n'est pas défini par défaut.

Affichage et édition de votre profil partenaire

Pourquoi et quand exécuter cette tâche

1. Cliquez sur **Administrateur du compte >Profils >Partenaire**. Le système affiche l'écran Caractéristiques du partenaire.
2. Editez votre profil si nécessaire (certaines valeurs ne peuvent pas être éditées). Pour l'explication des valeurs, voir le tableau 2.

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. |

Tableau 2. Valeurs sur les écrans Partenaires (suite)

| Valeur | Description |
|-------------------------------|---|
| 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 <code>bcg.allow.partner.type.edit</code> est définie sur <code>True</code> . Par défaut, cette propriété est définie sur <code>False</code> . |
| 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. <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • Mode de fonctionnement, par exemple, Partenaire externe du simulateur RN. • Adresse IP ou nom d'hôte du partenaire. |
| Partenaire interne par défaut | Un partenaire interne par défaut est utilisé pour échanger des documents si aucun partenaire n'est configuré comme partenaire par défaut. |

3. 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 4, «Création de destinations», à la page 39.

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.

Package. Identifie les formats de regroupement 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.

Définitions de type de document

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

Package. Il s'agit des formats d'emballage 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 : Pourquoi et quand exécuter cette tâche

1. Cliquez sur **Administrateur du compte > Profil > Fonctions B2B**. 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 fonction 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**.

Création et installation de certificats

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 la vérification de signature numérique pour vérifier l'authenticité des transactions de documents métier entre le partenaire interne et les partenaires externes. Ils servent aussi au chiffrement et au déchiffrement. Pour la fonction OpenPGP, la fonctionnalité de signature n'est pas disponible.

Pour des documents sortants avec des certificats X.509, indiquez un certificat principal et un certificat secondaire pour les documents sortants afin de garantir que l'échange de documents ne soit pas interrompu. Le certificat principal est utilisé pour toutes les transactions. Le secondaire est utilisé si le principal est expiré ou révoqué.

Important : Cette fonctionnalité n'est pas disponible pour les certificats OpenPGP.

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

Pour X.509, le certificat arrivé à expiration ou révoqué 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 arrivé à expiration est trouvé.

Important : Cette fonctionnalité n'est pas disponible pour les certificats OpenPGP.

L'option Utilisation du certificat est disponible en fonction du type de certificat sélectionné. Pour X.509, dans le profil Opérateur de concentrateur, Utilisation du certificat peut être défini pour les types de certificat Signature numérique ou Client SSL. Ce paramètre ne peut pas être défini pour d'autres types. Dans le profil du partenaire interne, il peut être défini pour les types de certificat Signature numérique et Client SSL, mais pas pour Chiffrement. Dans le profil du partenaire externe, il peut être défini pour Chiffrement, mais pas pour Signature numérique, Client SSL et serveur. 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 de 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. Si le certificat est désigné comme certificat serveur FTP et/ou certificat serveur SFTP, le Type de certificat doit être Serveur SSL et une des deux ou les deux cases à cocher pour l'authentification de serveur FTP et l'authentification de serveur SFTP doivent être sélectionnées. Les certificats OpenPGP ne peuvent pas être téléchargés dans le profil d'opérateur de concentrateur. L'utilisation du

chiffrement dans le profil du partenaire externe et du déchiffrement dans le profil du partenaire interne peuvent être définies pour les certificats OpenPGP.

Pour les certificats X.509, les certificats secondaires peuvent aussi être chargés deux fois, une fois pour la signature numérique et de nouveau pour le client SSL. Si tel est le cas, le même modèle doit être appliqué pour les certificats secondaires. Par exemple, si les certificats primaires ont été chargés comme certificats distincts pour la signature numérique et pour le client SSL, des certificats secondaires doivent alors également être chargés comme entrées de certificats distinctes (même si le certificat peut être le même).

Dans le cas de X.509, pour la création et la validation complètes de certpath, vous devez télécharger tous les certificats appartenant à la chaîne de certificats. Par exemple, si la chaîne 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 téléchargés 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.

Important : Les fonctionnalités de validation de certificat ne sont pas disponibles pour les certificats OpenPGP.

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 30. Les certificats expirés sont sauvegardés dans la base de données IBM WebSphere Partner Gateway. Ils ne peuvent pas être supprimés du système.

Pour plus d'informations, voir «Dispositions du certificat» et «Types de certificat et formats pris en charges», à la page 17.

Dispositions du certificat

Autorité de certification (AC) - autorité qui émet et gère les autorisations d'accès de sécurité et les clés publiques pour le chiffrement des messages. 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- un 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 et Vérification de 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- pour empêcher la dénégation d'engagements ou actions antérieurs. 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 qui a 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'émetteur.

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

OpenPGP- OpenPGP utilise une combinaison de clé publique solide et de cryptographie symétrique pour fournir des fonctions de sécurité. En général, OpenPGP fournit l'authentification, la confidentialité et l'intégrité des données au moyen de signatures numériques, du chiffrement, de la compression et de la conversion en radix-64. Dans cette édition, seuls le chiffrement, la compression et la conversion en radix-64 sont pris en charge pour OpenPGP. WebSphere Partner Gateway prend en charge la spécification OpenPGP pour échanger des documents avec des partenaires externes d'après RFC 4880. A partir de la console de WebSphere Partner Gateway, vous pouvez configurer les formats et les méthodes OpenPGP pour la confidentialité et l'intégrité des données.

Types de certificat et formats pris en charges

Tous les certificats doivent être au format DER ou ASCII PEM (Privacy Enhanced Mail). Ils peuvent être convertis d'un format à l'autre. Depuis la version 6.2.1, WebSphere Partner Gateway prend également en charge les certificats OpenPGP.

Il existe différents types de certificat :

- **Certificat client SSL (partenaires externes et partenaire interne).** Certificat de transport. Si votre transport de communication sortante est HTTPS et que l'authentification du client est requise, vous aurez besoin d'un certificat client SSL. Dans la plupart des cas, le certificat 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 serveur SSL-** active l'authentification de serveur SSL. L'AC du certificat du serveur SSL doit être échangée entre les partenaires.
- **Chiffrement et déchiffrement-** le chiffrement consiste à modifier les données de manière à ce qu'elles soient illisibles tant qu'elles n'ont pas été déchiffrées. WebSphere Partner Gateway utilise un système cryptographique appelé chiffrement de clé publique permettant de sécuriser la communication entre les partenaires et le concentrateur. Différents protocoles métier comme AS2 ou RosettaNet ont des exigences en matière de chiffrement. SSL utilise également le chiffrement. Sauf indication contraire, le terme *chiffrement* utilisé dans ce chapitre s'applique aux protocoles métier. Le déchiffrement est un moyen de déchiffrer les données chiffrées afin de les rendre lisibles. Le déchiffrement est effectué sur des documents entrants. WebSphere Partner Gateway est capable de recevoir des données chiffrées OpenPGP. Le paquet de données reçu est déchiffré à l'aide de la clé privée. Si vous recevez des données chiffrées avec protection de leur intégrité, après le déchiffrement, l'intégrité des données est vérifiée à l'aide du paquet Code de détection des modifications. Le dernier paquet déchiffré dans les données déchiffrées doit être un paquet de Code de détection des modifications. Dans un tel scénario, les données chiffrées se composent du paquet de données à intégrité protégée chiffrées de façon symétrique. L'intégrité du message est donc vérifiée. Pour le paquet OpenPGP, RFC 4880 est pris en charge. La fonctionnalité de données chiffrées avec protection de l'intégrité est uniquement définie dans RFC 4880.
- **Compression-** OpenPGP prend en charge la compression et la décompression lors de l'envoi et de la réception d'un document. Pour un paquet OpenPGP, la compression s'effectue conformément à RFC 4880.
- **Chiffrement et compression-** lorsque vous recevez un message, il doit être déchiffré. Après le déchiffrement est obtenu un paquet de données compressé auquel la décompression est appliquée. Le chiffrement est conforme à RFC 4880. Vous pouvez aussi envoyer et recevoir des données chiffrées et compressées avec protection de l'intégrité.
- **Certificat de signature numérique et vérification de signature numérique.** 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. La vérification de signature numérique vérifie qui a envoyé le document et s'il n'a pas été altéré en transit. Elle permet également de s'assurer de l'irréfutabilité. L'irréfutabilité signifie qu'un partenaire ne peut pas

nier avoir créé et envoyé un message. Elle permet également de s'assurer que le partenaire ne peut pas nier avoir reçu le message.

- **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 du certificat 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 du certificat 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 prend en charge ce format depuis la version 6.1. 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 entrants

Pourquoi et quand exécuter cette tâche

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.

Authentifier les clients

Pourquoi et quand exécuter cette tâche

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

Validation du certificat du client :

Pourquoi et quand exécuter cette tâche

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

1. Importez le certificat client.
 - a. Cliquez sur **Administrateur du compte > Profils > Partenaire**. Recherchez le profil du partenaire.
 - b. Sélectionnez le partenaire et 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 41.
 - 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 l'authentification du client :

Pourquoi et quand exécuter cette tâche

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

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

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

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

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

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

Installation de certificats de chiffrement sortants

Pourquoi et quand exécuter cette tâche

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

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

Etape 1 : Obtention du certificat du partenaire

Pourquoi et quand exécuter cette tâche

Procurez-vous le certificat de chiffrement de votre partenaire. Le certificat doit être au format X.509DER ou au format ASCII PEM (Privacy Enhanced Mail). Depuis WebSphere Partner Gateway 6.2.1, le format OpenPGP est également pris en charge. Remarquez que WebSphere Partner Gateway ne prend en charge aucun autre format de certificat.

Etape 2 : Installation du certificat du partenaire

Étapes pour télécharger un certificat pour un partenaire.

Pourquoi et quand exécuter cette tâche

Installez le certificat via la console de communauté sous le profil du partenaire, en procédant de la manière suivante :

Procédure

1. Accédez à **Administrateur du compte > Profils > Certificats > Charger le certificat**.
2. Dans la page **Sélectionner partenaire, emplacement de fichier, mot de passe** de l'assistant, entrez les valeurs suivantes :
 - a. **Emplacement du certificat**- cliquez sur **Parcourir** pour sélectionner l'emplacement du certificat public.
 - b. **Emplacement du fichier de clés sécurisées (ou) du fichier de clés** - cliquez sur **Parcourir** pour sélectionner l'emplacement du magasin de clés certifiées (ou) du fichier de clés. Le magasin de clés certifiées est un fichier contenant des certificats racines et de CA dignes de confiance. Le fichier de clés contient une collecte de clés privées avec les certificats racine et de CA

sécurisés. Le fichier de clés est une collection de certificats en format OpenPGP. Sélectionnez l'emplacement du certificat pour fournir le chemin du fichier de clés.

- c. **Mot de passe**- si l'emplacement du fichier de clés sécurisées (ou) du fichier de clés a un mot de passe, entrez-le. Dans le cas d'un fichier de clés, le mot de passe n'est pas nécessaire.
 - d. **Type** : sélectionnez le type de fichier de clés sécurisées (ou) de fichier de clés. Les valeurs disponibles dans la liste sont : JKS, JCEKS, PKCS12 et OpenPGP.
3. Cliquez sur **Suivant**.

Remarque : La page **Certificats d'entité finale et d'AC** de l'assistant s'ouvre lorsque vous téléchargez les certificats à l'aide d'un fichier de clés sécurisées comportant plusieurs certificats. La liste des certificats disponibles dans le magasin de clés certifiées s'affiche. **Sélectionner les clés/certifications OpenPGP à télécharger** s'affiche lorsque vous sélectionnez un fichier de clés de type OpenPGP dans la page **Sélectionner partenaire, emplacement de fichier, mot de passe** de l'assistant.

4. Sélectionnez un certificat dans la page **Certificat d'entité finale à télécharger** de l'assistant. Dans la page **Certificat d'entité finale et d'autorité de certification**, entrez les valeurs suivantes :
 - a. **Le fichier de clés comporte plusieurs certificats d'entité finale.**
Sélectionnez le certificat à télécharger - la liste déroulante contient tous les certificats d'entité finale. Sélectionnez le certificat à charger.
 - b. **Sélectionnez la liste des certificats d'autorité de certification racine et intermédiaires à télécharger** - Dans la zone de liste, sélectionnez les certificats racine et intermédiaires à télécharger.
5. Dans la page **Sélectionner les clés/certifications OpenPGP à télécharger** de l'assistant, les certificats associés au fichier de clés sélectionné sont renseignés dans la liste.

Remarque : Cliquez sur **Afficher les caractéristiques** pour afficher les caractéristiques du certificat sélectionné. En cas de certificat, chaque fois que l'ID clé et l'ID émetteur sont les mêmes, le certificat est un certificat auto-signé.

- a. Sélectionnez une clé de niveau supérieur dans la liste.

Remarque : S'il y a des sous-clés pour la clé de niveau supérieur, alors toutes les sous-clés sont affichées dans la liste **Sélectionner la sous-clé à télécharger**.

- b. Sélectionnez la sous-clé, si nécessaire.
6. Cliquez sur **Suivant** pour atteindre la page **Caractéristiques du certificat** de l'assistant.
 7. Sur la page **Caractéristiques du certificat** de l'assistant, entrez les caractéristiques suivants :
 - a. **Nom du certificat de feuille** - nom du certificat de 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).
 - b. **Description** - description du certificat de feuille.
 - c. **Ce certificat est-il destiné à l'authentification d'un serveur FTP** - cochez cette case si le certificat téléchargé est destiné à l'authentification d'un serveur FTP.

- d. **Ce certificat est-il destiné à l'authentification d'un serveur FTP** - cochez cette case si le certificat téléchargé est destiné à l'authentification d'un serveur FTP.

Important : L'authentification des serveurs FTP et SFTP ne s'applique pas aux certificats OpenPGP.

- e. **Type de certificat** - associez ce certificat à un type de certificat. Les différents types pris en charge sont Signature numérique, Vérification de signature numérique, Chiffrement, Serveur SSL et Client SSL.

A faire : Les types Client SSL, Serveur SSL, Signature numérique et Vérification de la signature numérique sont pas disponibles pour les certificats OpenPGP.

- f. **Utilisation du certificat** - Associez une utilisation au certificat. Les valeurs admises sont Principal et Secondaire.

Important : Cela ne s'applique ni à la vérification de la signature ni au certificat serveur SSL.

- g. **Mode de fonctionnement** - Entrez le mode de fonctionnement.

Important : Le mode de fonctionnement ne s'applique pas au chiffrement ni à la vérification de signature.

- h. **Etat** - Sélectionnez Activé ou Désactivé selon que vous souhaitez activer ou désactiver un certificat après l'avoir chargé. Le bouton Suivant est uniquement actif si le certificat est activé.
 - i. **Gestion des ensembles** - Vous pouvez associer un certificat à un ensemble existant ou créer un nouvel ensemble. Si le certificat est un certificat secondaire, il ne peut être associé qu'à un ensemble existant. Vous pouvez associer le certificat à n'importe quel ensemble, pour un partenaire interne de type Chiffrement ou pour un partenaire externe de type SSL (auth. client entrante) ou Signature (Vérification).
8. Cliquez sur **Suivant** pour accéder à la page Ensemble de l'assistant. Si le certificat est un certificat principal, vous n'avez pas besoin de créer d'ensembles et d'associer le certificat à un ensemble et à une connexion de participant. Si vous avez coché **Créer un ensemble**, la page **Créer un ensemble** de l'assistant s'ouvre. 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**.

Important : Le passage d'un certificat secondaire à un certificat principal n'est pas pris en charge pour les certificats OpenPGP.

9. Dans la page **Créer un ensemble** de l'assistant, entrez les caractéristiques du nouvel ensemble. Si le certificat est un certificat principal, vous n'avez pas besoin de créer d'ensembles et d'y associer le certificat. Entrez les valeurs suivantes :
- a. **Nom de l'ensemble** - nom de l'ensemble.
 - b. **Description** - Description de l'ensemble.
 - c. **Statut** - Sélectionnez activé ou désactivé. Si le statut est désactivé, le bouton **Suivant** ne sera pas activé.
 - d. **Utiliser comme paramètres par défaut** - Cochez cette case si vous voulez que cet ensemble soit l'ensemble par défaut.

10. Sur la page **Ajouter à l'ensemble existant** de l'assistant, sélectionnez l'ensemble ou les ensembles auxquels ajouter le certificat. Entrez les valeurs suivantes :
 - a. **Sélectionner dans la liste d'ensembles disponibles pour le type de certificat sélectionné** - Dans la liste, sélectionnez l'ensemble ou les ensembles auxquels ajouter le certificat.
 - b. **Utiliser comme paramètres par défaut** - Cochez cette case si vous voulez que cet ensemble soit l'ensemble par défaut.
11. Dans la page **Créer un nouvel ensemble** ou **Ajouter à un ensemble existant**, cliquez sur **Suivant** pour accéder à la page **Paramètres par défaut** de l'assistant. Le bouton **Suivant** n'est activé que si le statut de l'ensemble est activé.
12. Dans **Statut**, sélectionnez **Activé** ou **Désactivé** selon que vous souhaitez activer ou non le certificat après l'avoir chargé.

Remarque : Si vous avez coché **Paramétrer par défaut** à la page précédente (Créer un ensemble ou Ajouter à un ensemble existant), vous devez associer l'ensemble à un mode de fonctionnement. Ceci affiche les différents cas d'utilisation des certificats en fonction des modes de fonctionnement. Le client SSL et la signature numérique seront désactivés.

13. 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.
14. Sur la page Configuration de l'assistant, entrez les valeurs suivantes :
 - a. **Partenaire source** - cette liste déroulante est pré-remplie avec la liste des partenaires externes. Vous pouvez également sélectionner "Tous" pour inclure tous les partenaires externes.
 - b. **Partenaire cible** - cette zone est pré-remplie avec le nom du partenaire.
 - c. **Package source** - dans la liste déroulante, sélectionnez les objets du package Définitions de flux de documents du partenaire source.
 - d. **Package cible** - Dans la liste déroulante, sélectionnez les objets de votre package Définitions de flux de documents.
15. Cliquez sur **Ajouter plus de connexions** si vous souhaitez associer l'ensemble à d'autres connexions de participant.
16. Cliquez sur **Ajouter un certificat secondaire** pour ajouter un certificat secondaire à l'ensemble actuel.
17. 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.

Que faire ensuite

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

ATTENTION :

Pour OpenPGP, si un échec de téléchargement de certificat se produit malgré le chargement du bon certificat, alors redémarrez le serveur.

Etape 3 : Installation des certificats émis par une autorité de certification

Pourquoi et quand exécuter cette tâche

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

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

1. Accédez à **Administrateur du compte > Profils > Certificats**
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

Pourquoi et quand exécuter cette tâche

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

Par exemple, pour modifier les attributs d'une connexion de partenaire, cliquez sur **Administrateur du compte > Connexions**, 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

Installation d'un certificat de vérification de signature numérique de communication entrante

Pourquoi et quand exécuter cette tâche

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

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

1. Recevez le certificat de signature X.509 du partenaire au format DER.
2. Accédez à **Administrateur du compte > Profils > Certificats > Charger le 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 **Vérification de 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 page 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 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'utilisateurs

Cette section présente les étapes de la création d'un utilisateur.

Pourquoi et quand exécuter cette tâche

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

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

1. Veillez à ce que le profil du partenaire pour lequel vous voulez créer des utilisateurs soit sélectionné. Le profil sélectionné s'affiche en haut de la page après **Profil >**. Si le Nom de profil n'est pas sélectionné, suivez les étapes ci-dessous pour créer un profil :
 - a. Cliquez sur **Administrateur du compte > Profils > Partenaire**.
 - b. Entrez les critères de recherche et cliquez sur **Rechercher**, ou cliquez sur **Rechercher** sans entrer aucun critère pour afficher la liste de tous les partenaires.
 - c. Cliquez sur l'icône **Afficher les détails** pour afficher le profil du partenaire.
2. Cliquez sur **Utilisateurs**.

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

Remarque : Le nom d'utilisateur doit être unique pour chaque partenaire du système.

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

Remarque :

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

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

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

Configuration d'un utilisateur FTP et SFTP

Étapes pour créer des serveurs FTP et SFTP.

Pourquoi et quand exécuter cette tâche

Pour créer un utilisateur FTP et SFTP, procédez comme suit :

Procédure

1. Cliquez sur **Administrateur du compte > Gestion des utilisateurs FTP**.
 2. Cliquez sur **Créer**.
 3. Entrez les coordonnées de l'utilisateur et cliquez sur **Enregistrer**. Les informations sur l'utilisateur créé avec succès s'affichent en mode lecture seule.
 4. Cliquez sur le lien **Configuration FTP**.
 5. Dans l'écran Configuration FTP, sélectionnez **Activé** pour **Utilisateur FTP activé** ou pour **Utilisateur SFTP activé**. Vous pouvez activer un utilisateur à la fois pour le serveur FTP et pour le serveur SFTP.
 6. Entrez les caractéristiques suivantes de la configuration FTP :
 - a. Entrez le **Répertoire de base**, qui est le chemin relatif vers la valeur spécifiée pour `bcg.ftp.config.rootdirectory`.
 - b. Activez ou désactivez **Droit d'accès en écriture** sur le répertoire de base.
 - c. Activez ou désactivez le droit de **Créer/Supprimer le répertoire**.
 - d. Sélectionnez **Nombre de connexions max.**. C'est le nombre maximum de fois que vous pouvez effectuer la connexion simultanée.
 - e. Sélectionnez **Nombre max de connexions avec adresse IP identique**. C'est le nombre maximum de fois que vous pouvez effectuer la connexion simultanée à partir de la même adresse IP.
 - f. Sélectionnez **Délai d'inactivité max. (secondes)**. C'est le temps maximal d'inactivité, en secondes, au bout duquel la connexion utilisateur est abandonnée.
 - g. Sélectionnez **Maximum téléchargement vers l'amont (octets/sec)**. C'est le débit maximal de téléchargement vers l'amont en octets/sec.
 - h. Sélectionnez **Maximum téléchargement vers l'aval (octets/sec)**. Débit maximal de téléchargement vers l'aval en octets/sec.
- Remarque :** Certaines zones ont une valeur Limite personnalisée dans la liste déroulante. Si vous sélectionnez Limite personnalisée dans la liste déroulante, entrez la valeur personnalisée dans la zone de texte.
7. Pour la configuration SFTP, entrez **Clé (SFTP uniquement)**. Le fichier téléchargé est utilisé pour l'authentification par clé. L'icône du dossier indique qu'une clé est déjà téléchargée. Vous pouvez aussi utiliser **Parcourir** pour télécharger une clé.
 8. Cliquez sur **Sauvegarder**.

Création des informations de contact

Pourquoi et quand exécuter cette tâche

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.

Remarque : L'opérateur de concentrateur doit disposer d'un droit d'accès en lecture-écriture pour la création de contacts.

Pour créer des contacts :

1. Cliquez sur **Administrateur du compte > Profils > Contacts**. La liste des contacts actuels s'affiche. Une option de recherche vous permet de trouver un contact spécifique. Vous avez également la possibilité de masquer la section des critères de recherche. Si vous ne pouvez pas exécuter cette tâche, consultez votre administrateur de concentrateur.
2. Cliquez sur **Créer**.
3. Entrez les informations de contact :
 - **Nom donné** - Nom du contact.
 - **Nom de famille** - Nom de famille du contact.
 - **E-mail** - Adresse e-mail où les notifications d'alerte seront envoyées.
 - **Téléphone** - Numéros de téléphone.
 - **Numéro de fax** - Numéro de fax.
 - Environnement local de langue, environnement local de format et fuseaux horaires du contact.
 - **Visibilité au sein de la console** - Indicateur précisant si le contact n'est visible qu'au sein de votre organisation ou s'il peut également être vu par les partenaires internes.
 - **Fonctionnalités**
 - **Accéder à la console** - Sélectionnez Oui si vous voulez que le contact puisse accéder à la console.
 - Les détails d'authentification (Nom d'utilisateur, Mot de passe et Saisir à nouveau le mot de passe) sont obligatoires si vous sélectionnez Oui. Si vous voulez que le système génère un mot de passe pour vous, cliquez sur Générer automatiquement le mot de passe.
 - **Préférences utilisateur**
 - **Page d'accueil par défaut** - Permet de définir la page d'accueil par défaut à partir du menu déroulant.
 - **Lignes par page par défaut lors de l'affichage des résultats de la recherche** - permet de définir la valeur à partir du menu déroulant.
 - **Capacité à recevoir des alertes** - Indicateur précisant si le contact recevra des alertes. Si vous sélectionnez Non, le contact ne recevra pas de notifications.
 - **Configuration FTP**
 - **Peut utiliser FTP** - Indique si l'utilisateur (FTP/non FTP) est activé ou désactivé.
 - **Répertoire de base** - Répertoire de base du serveur FTP.

- **Droit d'accès en écriture** - Si cette option est activée, l'utilisateur dispose de droits d'accès en écriture. Vous pouvez désactiver cette option pour supprimer les droits d'accès en écriture.
 - **Créer/Supprimer un répertoire** - Si cette option est activée, l'utilisateur dispose de droits de création et de suppression de répertoire. Vous pouvez désactiver cette option pour supprimer les droits de création/suppression.
 - **Nombre max de connexions** - Nombre maximum de connexions autorisées. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. La limite personnalisée vous permet d'entrer la valeur de votre choix dans la zone de texte.
 - **Nombre max de connexions avec adresse IP identique** - Nombre maximum de connexions autorisées à partir d'une adresse IP identique. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. La limite personnalisée vous permet d'entrer la valeur de votre choix dans la zone de texte.
 - **Délai d'inactivité max (secondes)** - Délai d'inactivité maximum autorisé. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. La limite personnalisée vous permet d'entrer la valeur de votre choix dans la zone de texte.
 - **Téléchargement vers l'amont max (octets/sec)** - Débit maximal de téléchargement vers l'amont autorisé. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. La limite personnalisée vous permet d'entrer la valeur de votre choix dans la zone de texte.
 - **Téléchargement vers l'aval max (octets/sec)** - Débit maximal de téléchargement vers l'aval autorisé. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. Le nombre limite personnalisé vous permettra d'entrer une valeur personnalisée dans la zone de texte.
- Pour la configuration SFTP, entrez **Clé (SFTP uniquement)**. Le fichier téléchargé est utilisé pour l'authentification par clé. L'icône du dossier indique qu'une clé est déjà téléchargée. Vous pouvez aussi utiliser **Parcourir** pour télécharger une clé.
4. 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 36.
- Pour créer une alerte basée sur le volume et y ajouter des contacts, voir « Création d'une alerte dépendant du volume », à la page 32.
- Pour créer une alerte basée sur l'événement et y ajouter des contacts, voir « Création d'une alerte de type événement », à la page 34.

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 métier 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 basées 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 pour 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 documents 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 événements prédéfinis dans l'écran Alerte : Événements. Par exemple : 240601 Echec de la reprise AS ou 108001 Il ne s'agit pas d'un certificat.

Remarque : Le partenaire externe doit disposer d'un droit d'accès en lecture / écriture pour effectuer ces tâches. 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 dépendant du volume

Pourquoi et quand exécuter cette tâche

L'opérateur de concentrateur doit activer les droits en lecture-écriture pour la création de cette alerte.

1. Cliquez sur **Administrateur du compte > Alertes**.
2. Cliquez sur **Créer** dans l'angle supérieur droit de l'écran. Le système affiche l'onglet de définition des alertes.
3. Sélectionnez **Alerte de volume** pour **Type d'alerte** (paramètre par défaut). Le système affiche les zones de texte appropriées pour une alerte de volume.
4. Saisissez un **Nom d'alerte** pour l'événement.
5. Entrez le **texte commercial personnalisé**. Lorsque l'événement d'alerte est généré, ce message sera également envoyé.
6. Sélectionnez un **Partenaire** et un **Propriétaire d'alerte** (uniquement un partenaire interne et un administrateur du concentrateur).
7. 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.
8. Sélectionnez une des trois options de volume (Prévu, Plage ou Aucun volume) puis passez à l'étape 8.
 - **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. Entrez uniquement un nombre positif. L'alerte ne fonctionnera pas si vous entrez 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.
 - **Plage**. Sélectionnez Plage pour qu'une alerte soit déclenchée si le volume du flux de documents sort d'une plage minimale-maximale. Procédez comme suit pour créer une alerte basée sur une plage 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. Une alerte est déclenchée uniquement si le volume du flux de documents est inférieur à la valeur indiquée.

- 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 une plage de 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.
9. Sélectionnez Quotidien ou Plage 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).
 - **Plage** Sélectionnez Plage pour contrôler le volume du flux de documents entre deux jours de la semaine ou du mois. Par exemple, sélectionnez Plage 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.
 10. 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 de Plage est sélectionnée, le volume du flux de documents est contrôlé à partir de l'Heure de début du premier jour de la plage jusqu'à l'Heure de fin du dernier jour de la plage.
 11. Sélectionnez les jours appropriés de la semaine ou du mois pendant lesquels le contrôle de l'alerte aura lieu. Si vous avez choisi la fréquence Quotidien, sélectionnez les jours ouvrables de la semaine ou les jours du mois pendant lesquels le contrôle de l'alerte aura lieu. Si vous avez choisi la fréquence Plage, sélectionnez deux jours de la semaine ou du mois entre lesquels le contrôle de l'alerte aura lieu.
 12. Sélectionnez l'**Etat de l'alerte** sur Activé ou Désactivé pour cette alerte.
 13. Cliquez sur **Sauvegarder**.
 14. Cliquez sur l'onglet **Notification**.
 15. Cliquez sur l'icône Editer.
 16. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement).
 17. 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 en incrustation Création d'un contact.

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.
 18. Saisissez le nom, l'adresse électronique et les numéros de téléphone et de télécopie du contact.
 19. Choisissez l'état de l'alerte du contact.

- Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.
 - Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.
20. 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.
21. Cliquez sur **Sauvegarder** pour sauvegarder le contact. Cliquez sur **Sauvegarder & Abonner** pour ajouter le contact à la liste des contacts pour cette alerte.
22. 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 effectuée un contrôle entre 13h et 15h tous les mercredis et jeudis. Un mercredi à 16h, l'alerte est modifiée de façon à effectuer son contrôle entre 17h et 19h. L'alerte n'effectuera pas de contrôle le jour même : la modification prendra effet le jeudi suivant.

Création d'une alerte de type événement

Pourquoi et quand exécuter cette tâche

Remarque : Le serveur de message d'alerte doit être configuré. Reportez-vous au *Guide d'administration* pour la configuration du serveur de messagerie d'alerte. L'opérateur de concentrateur doit activer les droits en lecture-écriture pour la création de cette alerte.

1. Cliquez sur **Administrateur du compte**.
2. Cliquez sur **Alertes**. Le système affiche la page Recherche d'alerte.
3. Cliquez sur **Créer** dans l'angle supérieur droit de la page. Le système affiche l'onglet de définition des alertes.
4. Sélectionnez **Alerte d'événement** comme **Type d'alerte**. Le système affiche les zones de texte appropriées pour une alerte basée sur l'événement.
5. Saisissez un **Nom d'alerte** pour l'alerte. Il sera votre identifiant pour cette alerte.
6. Entrez le **texte commercial personnalisé**. Lorsque l'événement d'alerte est généré, ce message sera également envoyé.
7. Sélectionnez un **Propriétaire d'alerte** pour l'alerte.
8. Sélectionnez un **Partenaire d'alerte** 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.
9. 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**

10. 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
11. Cliquez sur **Sauvegarder**.
12. Cliquez sur l'onglet **Notification**.
13. Cliquez sur l'icône **Editer**.
14. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement).
15. Si le contact à ajouter se trouve dans la zone de texte **Contacts**, sélectionnez-le et cliquez sur **Abonner**. Allez à l'étape 20. 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 en incrustation **Création d'un contact**. 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.
16. 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.
17. Choisissez l'état de l'alerte du contact.
 - Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.
 - Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.
18. 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.
19. 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.
20. 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 où 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 conjointement : 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 (période 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.

21. Cliquez sur **Sauvegarder**.

Ajout d'un contact à une alerte existante

Pourquoi et quand exécuter cette tâche

L'opérateur de concentrateur doit activer les droits en lecture-écriture pour l'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, à la page 37.

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'état de l'alerte du contact.
 - Sélectionnez **Activé** pour que ce contact reçoive des messages électroniques lorsque le système génère cette alerte.
 - Sélectionnez **Désactivé** si vous ne voulez pas envoyer de message électronique à ce contact lorsque le système génère cette alerte.
11. Choisissez le niveau de visibilité du contact.
 - Sélectionnez **Local** pour que ce contact soit vu uniquement par votre organisation.
 - Sélectionnez **Global** 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

Pourquoi et quand exécuter cette tâche

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 :

Procédure

1. Cliquez sur **Administrateur du compte > Profils > Adresses**. Le système affiche l'écran Adresses.
2. Cliquez sur **Créer une nouvelle 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 4. Création de destinations

Les destinations définissent des points d'entrée dans le système. Le partenaire externe doit disposer d'un droit d'accès en lecture / écriture pour effectuer ces tâches. Ce chapitre indique les étapes à suivre pour créer des destinations et contient les rubriques suivantes :

- «Présentation»
- «Configuration d'une destination HTTP», à la page 40
- «Configuration d'une destination HTTPS», à la page 41
- «Configuration d'une destination FTP», à la page 42
- «Configuration d'une destination SMTP», à la page 44
- «Configuration d'une destination JMS», à la page 45
- «Configuration d'une destination fichier-répertoire», à la page 46
- «Configuration d'une destination FTPS», à la page 48
- «Configuration d'une destination de script FTP», à la page 49
- «Configuration d'une destination SFTP», à la page 53
- «Configuration de gestionnaires», à la page 55
- «Spécification d'une destination par défaut», à la page 55

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
- SFTP
- Répertoire de fichiers
- Script 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

Pourquoi et quand exécuter cette tâche

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

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

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

Détails de destination

Pourquoi et quand exécuter cette tâche

Dans la page **Caractéristiques de la destination**, 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

Pourquoi et quand exécuter cette tâche

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

1. Sélectionnez **HTTP/1.1** dans la liste **Transport**.
2. 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 est **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**.
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 de serveur>:<port facultatif>/<chemin>`

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. Sinon, 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. Sinon, 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 55. 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.

Remarque : WebSphere Partner Gateway ne prend pas en charge un proxy direct (HTTPS) sécurisé mais utilise plutôt un tunnel HTTPS.

Pour créer des destinations HTTPS, appliquez la procédure suivante.

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

Caractéristiques des destinations

Pourquoi et quand exécuter cette tâche

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

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

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, 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 de serveur>:<port facultatif>/<chemin>`
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. Sinon, 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. Sinon, 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 55. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination FTP

Pourquoi et quand exécuter cette tâche

Pour créer une destination FTP, appliquez la procédure suivante.

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

Détails de destination

Pourquoi et quand exécuter cette tâche

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

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

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, 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 de serveur ftp>:<numéro de 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. Sinon, 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. Sinon, 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 55. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination SMTP

Pourquoi et quand exécuter cette tâche

Pour créer une destination SMTP, appliquez la procédure suivante.

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

Détails de destination

Pourquoi et quand exécuter cette tâche

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

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

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, 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 de 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. Sinon, 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. Sinon, 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 55. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination JMS

Pourquoi et quand exécuter cette tâche

Pour créer des destinations JMS, appliquez la procédure suivante.

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

Détails de destination

Pourquoi et quand exécuter cette tâche

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

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

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, 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:///<user_defined_MQ_JNDI_bindings_path>
```

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 router le document vers sa 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. Sinon, 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. Sinon, 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 55. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination fichier-répertoire

Pourquoi et quand exécuter cette tâche

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

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

Détails de destination

Pourquoi et quand exécuter cette tâche

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

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

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, 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 est sur la même unité que sur laquelle WebSphere Partner Gateway est installé, le format est le suivant : `file:///<path to target directory>`
Par exemple :
`file:///répertoire_fichier_local`
où `répertoire_fichier_local` est un répertoire du répertoire racine.
Pour les systèmes Windows pour lesquels le répertoire de fichiers se trouve sur une unité distincte de celle sur laquelle WebSphere Partner Gateway est installé, le format est le suivant : `file://<drive letter>:/<path>`
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. Sinon, 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. Sinon, 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 55. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination FTPS

Pourquoi et quand exécuter cette tâche

Pour créer des destinations FTPS, appliquez la procédure suivante.

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

Détails de destination

Pourquoi et quand exécuter cette tâche

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

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

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, 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 de serveur ftp>:<numéro de 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. Sinon, 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. Sinon, 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 55. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination de script FTP

Pourquoi et quand exécuter cette tâche

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

Pourquoi et quand exécuter cette tâche

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

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

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

Lorsque la destination est mise en service, les paramètres fictifs (par exemple %BCGSERVERIP%) sont remplacés par les valeurs saisies lors de la création d'une instance spécifique d'une destination de script FTP, comme indiqué dans 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% | Optionx, sous Attributs définis par l'utilisateur |

Il peut y avoir jusqu'à 10 options définies par l'utilisateur.

2. Enregistrez le fichier.

Commandes de script FTP

Vous pouvez utiliser les commandes suivantes pour créer le script :

- `ascii`, `binary`, `passive`, `epsv`
Ces commandes ne sont pas envoyées au serveur FTP. Elles modifient le mode de transfert (`ascii`, `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`
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

Pourquoi et quand exécuter cette tâche

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

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

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

Détails de destination

Pourquoi et quand exécuter cette tâche

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

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

Configuration de la destination

Pourquoi et quand exécuter cette tâche

Dans la section **Configuration de la destination** de la page, 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

Pourquoi et quand exécuter cette tâche

Si vous souhaitez indiquer des attributs supplémentaires, exécutez les étapes ci-après. La valeur indiquée pour l'option remplacera %BCGOPTIONx% 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

Pourquoi et quand exécuter cette tâche

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

1. Indiquez si vous souhaitez procéder à une planification en fonction d'un intervalle ou du calendrier.
 - Si vous avez sélectionné **Planification en fonction de l'intervalle**, sélectionnez le nombre de secondes qui doivent s'écouler avant que 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 55. Sinon, cliquez sur **Sauvegarder**.

Configuration d'une destination SFTP

Pourquoi et quand exécuter cette tâche

Configurez une destination SFTP pour que des documents puissent être envoyés depuis le concentrateur à l'adresse IP de vos partenaires. L'adaptateur se connecte au serveur SFTP auquel il envoie le document. Les données de documents sont fournies à l'adaptateur en tant que flux.

Pour créer des destinations SFTP, procédez comme suit :

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

Création de destinations SFTP sur les systèmes sur lesquels la sécurité administrative WAS est activée

Pourquoi et quand exécuter cette tâche

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

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

- **bcg.RMICConnector.admin.password** : définissez cet attribut sur le mot de passe qui est utilisé pour la sécurité administrative WAS.
4. Cliquez sur **Sauvegarder**.

Caractéristiques de la destination

Pourquoi et quand exécuter cette tâche

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

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

Configuration de destination

Pourquoi et quand exécuter cette tâche

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

1. Entrez le **Protocole IP de l'hôte/Nom d'hôte SFTP**. Il acceptera les messages électroniques de 100 caractères au maximum. Vous pouvez aussi entrer les adresses IP, IPv4 et IPv6.
2. Entrez le **Numéro de port**. La valeur minimum est 1 et la valeur maximum est 65535. La valeur par défaut est 22.
3. Entrez le **Répertoire de sortie**. Il acceptera les messages électroniques de 100 caractères au maximum. Il peut contenir les caractères basés sur l'environnement local.
4. Dans la zone **Type d'authentification**, sélectionnez le nom utilisateur/mot de passe ou l'authentification de clé publique.
5. Entrez le **Nom d'utilisateur** et le **Mot de passe** pour nom utilisateur/mot de passe. Si le type d'authentification est l'authentification de clé publique, le **Fichier de clé privée** (clés) et la **Phrase de passe** (certificats configurés dans la Console) doivent être utilisés. Le **Fichier de clé privée** est le chemin d'accès complet au fichier de clé privée au format OpenSSH. Le chemin d'accès complet doit également inclure le nom du fichier de clé privée.
6. La clé privée doit être sauvegardée dans un fichier et le chemin doit être défini. Les certificats X.509 sont pris en charge mais, si l'adaptateur de ressources nécessite la clé privée au format OpenSSH, faites votre saisie au format OpenSSH.
7. Entrez le **Nombre de relances**. Indiquez le nombre de tentatives d'envoi d'un document par la destination avant que l'opération n'échoue. La valeur par défaut est 3.
8. Entrez l'**Intervalle entre les nouvelles tentatives**. Sélectionnez la durée pendant laquelle la destination doit attendre avant de faire une nouvelle tentative d'envoi de document. La valeur par défaut est 300 secondes.
9. Entrez le **Nombre d'unités d'exécution**. Entrez le nombre de documents qui peuvent être traités simultanément. La valeur par défaut est 3.
10. **Codage EIS** correspond au codage du serveur FTP. Utilisez cette valeur pour définir le codage de la connexion de contrôle au serveur FTP.

11. Entrez la configuration du gestionnaire et cliquez sur **Sauvegarder** pour sauvegarder les détails de la configuration.

Configuration de gestionnaires

Pourquoi et quand exécuter cette tâche

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

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

Remarque : Seul l'opérateur de concentrateur peut télécharger le gestionnaire.

Pour appliquer un gestionnaire écrit par l'utilisateur pour ces paramètres de configuration, téléchargez le gestionnaire. Après avoir téléchargé le gestionnaire, effectuez la procédure suivante :

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

Pourquoi et quand exécuter cette tâche

Après avoir créé 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 5. 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 des contacts», à la page 60

«Gestion des alertes», à la page 62

«Gestion des adresses», à la page 64

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 Pourquoi et quand exécuter cette tâche

Cliquez sur **Administrateur du compte > Profils > Destinations**. La page de liste des destinations s'affiche.

Affichage ou édition des caractéristiques de la destination

Pourquoi et quand exécuter cette tâche

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

Procédure

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

Pourquoi et quand exécuter cette tâche

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

Pourquoi et quand exécuter cette tâche

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 : L'icône **Supprimer** ne sera 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

Procédure

1. Cliquez sur **Administrateur du compte > Profil > Certificat > Gestion des 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

Procédure

1. Cliquez sur **Administrateur du compte > Profil > Certificat**. 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 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

Pourquoi et quand exécuter cette tâche

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

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

Tableau 6. Valeurs sur l'écran Liste des contacts

| Valeur | Description |
|--|---|
| Nom donné | Nom du contact. |
| Nom de famille | Nom de famille du contact. |
| Courrier électronique | Adresse électronique utilisée pour les notifications d'alerte. |
| Téléphone | Numéros de téléphone. |
| Numéro de télécopie | Numéro de télécopie |
| Environnement local de langue et de format | Environnement local de langue, environnement local de format et fuseau horaire du contact. |
| Visibilité au sein de la console | Indicateur précisant si le contact n'est visible qu'au sein de votre organisation ou s'il peut également être vu par les partenaires internes. |
| Accès à la console | Sélectionnez Oui si vous voulez que le contact puisse accéder à la console. Les détails d'authentification (Nom d'utilisateur, Mot de passe et Saisir à nouveau le mot de passe) sont obligatoires si vous sélectionnez Oui. Si vous voulez que le système génère un mot de passe pour vous, cliquez sur Générer automatiquement le mot de passe. |
| Page d'accueil par défaut | Permet de définir la page d'accueil par défaut à partir du menu déroulant. |
| Lignes par page par défaut lors de l'affichage des résultats de la recherche | Permet de définir la valeur à partir du menu déroulant. |

Tableau 6. Valeurs sur l'écran Liste des contacts (suite)

| Valeur | Description |
|---|--|
| Capacité à recevoir des alertes | Indique si le contact pourra recevoir des alertes. Si vous sélectionnez Non, le contact ne recevra pas de notifications. |
| Possibilité d'utiliser FTP | Indique si l'utilisateur (FTP/non FTP) est activé ou désactivé. |
| Répertoire de base | Répertoire de base du serveur FTP. |
| Droit d'accès en écriture | Si cette option est activée, l'utilisateur dispose de droits d'accès en écriture. Vous pouvez désactiver cette option pour supprimer les droits d'accès en écriture. |
| Créer/Supprimer le répertoire | Si cette option est activée, l'utilisateur dispose de droits de création et de suppression de répertoire. Vous pouvez désactiver cette option pour supprimer les droits de création/suppression. |
| Nombre de connexions max. | Nombre maximum de connexions autorisées. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. Le nombre limite personnalisé vous permettra d'entrer une valeur personnalisée dans la zone de texte. |
| Nb de connexions max. de la même adresse IP | Nombre maximum de connexions autorisées à partir d'une même adresse IP. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. Le nombre limite personnalisé vous permettra d'entrer une valeur personnalisée dans la zone de texte. |
| Délai d'inactivité max. (secondes) | Délai d'inactivité maximum autorisé. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. Le nombre limite personnalisé vous permettra d'entrer une valeur personnalisée dans la zone de texte. |
| Maximum téléchargement vers l'amont(octets/sec) | Débit maximal de téléchargement vers l'amont autorisé. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. La limite personnalisée vous permet d'entrer la valeur de votre choix dans la zone de texte. |
| Maximum téléchargement vers l'aval(octets/sec) | Débit maximal de téléchargement vers l'aval autorisé. Sélectionnez une valeur dans la liste déroulante ou sélectionnez une limite personnalisée. La limite personnalisée vous permet d'entrer la valeur de votre choix dans la zone de texte. |

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 7. 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, l'Etat et le code postal. |
| Type de contact | Décrit le rôle du contact, par exemple : Opportunité B2B ou Opportunité commerciale. |

Tableau 7. Caractéristiques du contact (suite)

| Valeur | Description |
|----------------------|--|
| 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. |
| Abonné | Cette valeur est définie par le système. |
| Visibilité | <ul style="list-style-type: none">• 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**.

Suppression d'un contact

Procédure

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 sont utilisées pour avertir le personnel clé au sujet de fluctuations inhabituelles dans le volume de transmissions que vous recevez, ou lorsque des erreurs de traitement de documents métier se produisent.

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

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

Pourquoi et quand exécuter cette tâche

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

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

7. Sélectionnez un partenaire (partenaire interne ou administrateur du concentrateur uniquement).
8. Si vous le souhaitez, éditez les contacts pour cette alerte.
9. Cliquez sur **Sauvegarder**.

Recherche d'alertes

Pourquoi et quand exécuter cette tâche

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

Tableau 8. 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. |
| Livraison | Mode de livraison |
| Partenaire contrôlé | Partenaire pour lequel vous avez défini une alerte. |
| Activé | Alertes activées, désactivées ou toutes les alertes. Cette option est indiquée par une marque de contrôle verte. |
| Contacts abonnés | Contacts affectés à l'alerte. Vous pouvez sélectionner Pour les abonnés, Aucun abonné ou Tous. |

Tableau 9. Critères de recherche d'alerte pour le partenaire interne

| Valeur | Description |
|-------------------|--|
| Partenaire source | 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 affectés à l'alerte. Vous pouvez sélectionner Pour les abonnés, Aucun abonné ou Tous. |

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

Désactivation ou activation d'une alerte

Procédure

1. Cliquez sur **Administrateur du compte** > **Alertes**. Le système affiche la page Recherche d'alerte
2. Sélectionnez les critères de recherche dans les listes déroulantes et entrez le Nom de l'alerte.
3. Cliquez sur **Rechercher**. Le système affiche la liste des alertes correspondant à vos critères de recherche, le cas échéant.

4. Localisez l'alerte et cliquez sur la colonne **Activé** pour supprimer la marque verte. 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.

Retrait d'une alerte

Procédure

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

Notification d'événement

Pourquoi et quand exécuter cette tâche

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

Pourquoi et quand exécuter cette tâche

1. Cliquez sur **Administrateur du compte** > **Profil** > **Adresse**.
2. Cliquez sur l'icône **Editer** et modifiez l'**Adresse**.
3. Effectuez les modifications requises. Le tableau suivant décrit les valeurs de l'adresse.

Tableau 10. 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

Procédure

1. Cliquez sur **Administrateur du compte > Profil > Adresse**.
2. Localisez l'adresse à supprimer, puis cliquez sur l'icône Supprimer.
3. Assurez-vous que vous souhaitez effectivement supprimer l'adresse.

Chapitre 6. 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 71
- « Afficheur RosettaNet», à la page 76
- « Afficheur de documents», à la page 79
- «Afficheur ebMS», à la page 74
- «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'événement

WebSphere Partner Gateway comprend les types d’événements suivants.

Tableau 11. 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 d'information sont générés lorsqu'une opération de système a abouti. Ils servent aussi à indiquer l'état des documents en cours de traitement. Les événements d'information ne nécessitent aucune action 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. Les événements critiques nécessitent l'intervention du personnel du support technique. |

Exécution des tâches de l’Afficheur d’événements

Tableau 12. Tâches de l’Afficheur d’événements

| Que souhaitez-vous faire ? | Voir |
|--|--|
| Rechercher des événements | page « Recherche d’événements », à la page 69 |
| Afficher les caractéristiques de l’événement | page « Affichage des caractéristiques de l’événement », à la page 70 |

Recherche d'événements

Pourquoi et quand exécuter cette tâche

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'événements. 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 événements 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 13. 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

Procédure

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.

Résultats

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.

Evénements d'erreur

Des informations détaillées concernant un événement d'erreur/avertissement peuvent s'afficher dans la page d'afficheur de votre console. Cette aide autonome vous indiquera le motif, le diagnostic et la solution pour l'incident.

L'exemple suivant fournit des informations détaillées sur un échec XML d'analyse syntaxique de connexion :

BCG240065-Echec XML d'analyse syntaxique de connexion L'analyse syntaxique de connexion XML a échoué : {0}

Raison de l'incident : L'erreur Echec XML d'analyse syntaxique de connexion est générée pour la raison suivante : les informations provenant du document entrant ne sont pas suffisantes pour l'analyse syntaxique de la connexion.

Explication : le concentrateur doit procéder à une analyse syntaxique du document entrant pour obtenir les attributs requis permettant de trouver la connexion pour le document XML entrant. Il est possible que la connexion ne soit pas configurée ou que les valeurs appropriées ne se trouvent pas dans le document XML entrant.

Solution : pour résoudre cet incident, procédez comme suit :

- Vérifiez que la connexion est correctement configurée.
- Vérifiez que le document entrant contient tous les attributs requis pour l'identification de la connexion.

Service d'assistance : Pour plus d'informations sur cet événement d'erreur, visitez le site de notre service d'assistance à l'adresse suivante : site du service d'assistance WebSphere Partner Gateway.

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 14. Tâches de l'Afficheur AS1/AS2

| Que souhaitez-vous faire ? | Voir |
|---------------------------------|--|
| Recherche de messages AS | page « Recherche de messages », à la page 72 |
| Affichage des documents de base | page « Affichage des détails relatifs à un message », à la page 73 |

Recherche de messages

Pourquoi et quand exécuter cette tâche

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

Tableau 15. 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. |
| Rechercher dans | 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, le regroupement, 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. |

Tableau 15. Critères de recherche de l'afficheur AS (suite)

| Valeur | Description |
|---|--|
| 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 détails relatifs à un message

Pourquoi et quand exécuter cette tâche

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 16. 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 : <ul style="list-style-type: none"> • 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. |

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

Afficheur ebMS

Le mécanisme ebMS (eXML Message Service) offre une méthode standard pour l'échange de messages entre partenaires d'échanges eXML. Il constitue un moyen fiable d'échanger des messages sans utiliser des solutions ou des technologies propriétaires. Un message eXML 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 eXML. Le message eXML est un protocole de communication indépendant de l'enveloppe de message MIME/Multipart.

Exécution des tâches de l'afficheur ebMS

Tableau 17. Tâches de l'afficheur ebMS

| Que souhaitez-vous faire ? | Voir |
|--------------------------------|---|
| Rechercher des processus ebMS | «Recherche de processus ebMS» |
| Afficher des processus ebMS | «Affichage des caractéristiques des processus ebMS», à la page 75 |
| Afficher des documents de base | «Affichage des documents de base», à la page 75 |
| Afficher l'état des documents | «Affichage de l'état des documents», à la page 76 |

Recherche de processus ebMS

Pourquoi et quand exécuter cette tâche

- Cliquez sur **Afficheurs > Afficheur ebMS**. Le système affiche l'écran de recherche de l'afficheur ebMS.
- 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. |

| Valeur | Description |
|--------------------------------------|--|
| ID de conversation | Numéro d'identification unique attribué au processus. Les critères de recherche peuvent inclure le caractère générique astérisque (*). |
| Trier par | Trie les résultats, 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

Pourquoi et quand exécuter cette tâche

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 18. 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

Pourquoi et quand exécuter cette tâche

Pour afficher le document de base :

1. Cliquez sur **Afficheur > Afficheur ebMS**.
2. Sélectionnez les critères de recherche dans les listes déroulantes, voir «Recherche de processus ebMS», à la page 74
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 82.
- L'afficheur du document de base présente l'en-tête HTTP avec le document de base.

Affichage de l'état des documents

Procédure

1. Cliquez sur **Afficheurs > Afficheur ebMS**.
2. Sélectionnez les critères de recherche dans les listes déroulantes, voir « Recherche de processus ebMS », à la page 74
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 19. Tâches de l'Afficheur RosettaNet

| Que souhaitez-vous faire ? | Voir |
|---|---|
| Rechercher des processus RosettaNet | page « Recherche de processus RosettaNet », à la page 77 |
| Afficher les caractéristiques du processus RosettaNet | page « Affichage des caractéristiques du processus RosettaNet », à la page 78 |

Tableau 19. Tâches de l’Afficheur RosettaNet (suite)

| Que souhaitez-vous faire ? | Voir |
|--------------------------------|--|
| Afficher des documents de base | page « Affichage de documents bruts», à la page 78 |

Recherche de processus RosettaNet

Pourquoi et quand exécuter cette tâche

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 20. 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 d’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

Pourquoi et quand exécuter cette tâche

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 21. 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 de documents bruts

Procédure

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.

Résultats

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 82.
- 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 de documents

Pourquoi et quand exécuter cette tâche

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 22. 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. . |
| Rechercher dans | 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'emballage, 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 23. 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. |
| 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 caractéristiques du document, des événements et du document brut

Pourquoi et quand exécuter cette tâche

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 brut avec l'en-tête HTTP, cliquez sur l'icône Afficher le document brut en regard du document. Le système affiche le contenu du document brut.

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

Tableau 24. Valeurs de traitement de document 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. |

Tableau 24. Valeurs de traitement de document disponibles à l'aide de l'Afficheur de documents (suite)

| Valeur | Description |
|----------------------------------|--|
| 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 bruts 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 ».

Affichage des erreurs de validation des données

Pourquoi et quand exécuter cette tâche

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 25. 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 |

Exemple d'erreurs de validation XML imbriquées :

L'élément de données ContactInformation est la première erreur de validation, car cette balise occupe une position incorrecte. Elle devrait se trouver directement après PartnerRoleDescription.

L'élément de donnée FreeFormText est la deuxième erreur de validation, car cette balise a été dupliquée.

L'élément de données Jean est la troisième erreur de validation, car cette zone requiert un nom comportant 6 caractères au minimum.

```

<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE PurchaseOrderUpdateNotification SYSTEM "3A7_MS_V02_00_PurchaseOrderUpdateNotification.dtd">
<Pip3A7PurchaseOrderUpdateNotification>
  <fromRole>
    <PartnerRoleDescription>
      <GlobalPartnerRoleClassificationCode>Seller</GlobalPartnerRoleClassificationCode>
      <PartnerDescription>
        <ContactInformation>
          <ContactName>
            <FreeFormText>John</FreeFormText>
          </ContactName>
          <FreeFormText>John</FreeFormText>
          </FreeFormText>
          <EmailAddress>John@example.com</EmailAddress>
          <telephoneNumber>
            <CommunicationsNumber>+1-234-567-8998-8</CommunicationsNumber>
            </telephoneNumber>
            <facsimileNumber>
              <CommunicationsNumber>+1-234-567-8998-7</CommunicationsNumber>
              </facsimileNumber>
            </facsimileNumber>
            <BusinessDescription>
              <GlobalBusinessIdentifier>123456789</GlobalBusinessIdentifier>
              <GlobalSupplyChainCode>InformationTechnology</GlobalSupplyChainCode>
              <BusinessDescription>
                <GlobalPartnerClassificationCode>Carrier</GlobalPartnerClassificationCode>
                </BusinessDescription>
              </GlobalSupplyChainCode>
            </GlobalBusinessIdentifier>
          </PartnerDescription>
        </ContactInformation>
      </PartnerRoleDescription>
    </fromRole>
    <?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE PurchaseOrderUpdateNotification SYSTEM "3A7_MS_V02_00_PurchaseOrderUpdateNotification.dtd">
    <Pip3A7PurchaseOrderUpdateNotification>
      <fromRole>
        <PartnerRoleDescription>
          <GlobalPartnerRoleClassificationCode>Vendeur</GlobalPartnerRoleClassificationCode>
          <PartnerDescription>
            <ContactInformation>
              <ContactName>
                <FreeFormText>Jean</FreeFormText>
              </ContactName>
              <FreeFormText>Jean</FreeFormText>
              </FreeFormText>
              <EmailAddress>Jean@example.com</EmailAddress>
              <telephoneNumber>
                <CommunicationsNumber>+1-234-567-8998-8</CommunicationsNumber>
                </telephoneNumber>
                <facsimileNumber>
                  <CommunicationsNumber>+1-234-567-8998-7</CommunicationsNumber>
                  </facsimileNumber>
                </facsimileNumber>
                <BusinessDescription>
                  <GlobalBusinessIdentifier>123456789</GlobalBusinessIdentifier>
                  <GlobalSupplyChainCode>Technologies de l'information</GlobalSupplyChainCode>
                  <BusinessDescription>
                    <GlobalPartnerClassificationCode>Télécommunications</GlobalPartnerClassificationCode>
                    </BusinessDescription>
                  </GlobalSupplyChainCode>
                </GlobalBusinessIdentifier>
              </PartnerDescription>
            </ContactInformation>
          </PartnerRoleDescription>
        </fromRole>
      </PartnerRoleDescription>
    </Pip3A7PurchaseOrderUpdateNotification>
  </Pip3A7PurchaseOrderUpdateNotification>

```

Exemple d'erreurs de validation XML non-imbriquées :

L'élément de données EmailAddress est la première erreur de validation non imbriquée, car cette balise occupe une position incorrecte. Elle devrait se trouver directement après ContactInformation.

```

<BillTo>
  <PartnerRoleDescription>
    <EmailAddress>france@example.com</EmailAddress>
    <ContactInformation>
      <contactName>
        <FreeFormText>Chaîne</FreeFormText>
      </contactName>
      <facsimileNumber>
        <CommunicationsNumber>Chaîne</CommunicationsNumber>
      </facsimileNumber>
      <telephoneNumber>
        <CommunicationsNumber>+888-999-0000</CommunicationsNumber>
      </telephoneNumber>
    </ContactInformation>
  </PartnerRoleDescription>
</BillTo>

```

L'élément de données du numéro de téléphone est la deuxième erreur de validation non imbriquée, car cette zone requiert deux caractères supplémentaires correspondant à l'indicatif du pays.

Pour afficher les erreurs de validation dans un document de base, voir « Affichage de documents bruts », à la page 78.

Restrictions : La console n'affiche que les cent premiers kilo-octets d'un document de base. Les erreurs de validation dépassant 100 Ko ne peuvent pas être affichées.

Utilisation de la fonction Arrêt du processus

Pourquoi et quand exécuter cette tâche

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'attente 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

Pourquoi et quand exécuter cette tâche

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

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

2. Entrez les paramètres indiqués dans le tableau 26.

Tableau 26. Fenêtre File d'attente de la destination

| Critères | Description |
|--------------------------------|--|
| Nom de partenaire | <p>Vous pouvez remplir ce champs de la manière suivante :</p> <ol style="list-style-type: none"> Entrez le nom du partenaire. Entrez une partie du nom du partenaire dans cette zone, puis cliquez sur Afficher les partenaires. Sélectionnez un partenaire dans la liste. Indiquez le caractère générique * et cliquez sur Afficher les partenaires. Sélectionnez un partenaire dans la liste. <p>Lorsque vous cliquez sur Afficher les partenaires, une zone Partenaire s'affiche. La zone Partenaire répertorie tous les partenaires disponibles par ordre alphabétique.</p> |
| Destination | <p>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.</p> <p>Remarque : Cette liste est automatiquement alimentée par les destinations de partenaires sélectionnées et présentée par ordre alphabétique.</p> |
| Mis en file d'attente au moins | <p>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.</p> |
| Trier par | <p>Les résultats de la recherche sont triés par partenaire (valeur par défaut) ou par nom de la destination.</p> |
| Régénérer | <p>Vous pouvez activer ou désactiver (valeur par défaut) la régénération.</p> |
| Nombre minimal de documents | <p>Nombre minimal de documents dans la file d'attente d'une destination. La valeur par défaut est 1.</p> |
| Sens | <p>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.</p> |
| Fréquence de régénération | <p>Nombre de secondes pendant lesquelles la Console attend avant de mettre à jour les données affichées.</p> |

3. Cliquez sur **Rechercher**. Le système recherche tous les documents situés sur la destination qui correspondent à vos critères de recherche. Le **tableau 27** contient les informations renvoyées suite à la recherche.

Tableau 27. 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 |

Tableau 27. Résultats de la recherche de la file d'attente de destination (suite)

| Critères | Description |
|-----------------------|---|
| 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

Pourquoi et quand exécuter cette tâche

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

1. Cliquez sur **Afficheurs > Files 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 28).

Tableau 28. Fenêtre de recherche des documents de la file d'attente

| Critères | Description |
|-------------------|--|
| Nom de partenaire | Vous pouvez remplir ce champs de la manière suivante : <ol style="list-style-type: none"> 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. <p>Remarque : Lorsque vous cliquez sur Afficher les partenaires, une zone Partenaire s'affiche. La zone Partenaire répertorie tous les partenaires disponibles par ordre alphabétique.</p> |
| 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. <p>Remarque : Cette liste est automatiquement alimentée par les destinations de partenaires sélectionnées et présentée par ordre alphabétique.</p> |
| 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. |

Tableau 28. Fenêtre de recherche des documents de la file d'attente (suite)

| Critères | Description |
|-----------------------------------|--|
| 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

Pourquoi et quand exécuter cette tâche

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 27, à la page 85).
4. Cliquez sur l'icône Supprimer pour supprimer le document.

Affichage des détails relatifs à une destination

Pourquoi et quand exécuter cette tâche

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 > Files d'attente de destination**.
2. Dans la fenêtre File d'attente de destination, entrez les critères de recherche (voir le tableau 26, à la page 85).
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

Pourquoi et quand exécuter cette tâche

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 26, à la page 85).
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 7. 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 29. Outils

| Quelle fonction voulez-vous utiliser ? | Voir |
|---|--|
| Analyse de document | page « Analyse de document » |
| Rapport du volume de document | page « Création d'un rapport du volume de document », à la page 92 |
| Test de la connexion du partenaire | page « Test de la connexion du partenaire », à la page 94 |
| Rapports EDI | page « Rapports EDI », à la page 96 |
| Rapports FTP | page « Rapports FTP », à la 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 du document

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

Tableau 30. 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 : <ul style="list-style-type: none"> • 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

Pourquoi et quand exécuter cette tâche

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 31. 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, le regroupement, 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). |

Tableau 31. Critères de recherche du document (suite)

| Valeur | Description |
|---------------------------|--|
| 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

Procédure

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. A partir de 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 32. 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

Pourquoi et quand exécuter cette tâche

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 33. 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 à l'initiative du processus métier (partenaire interne uniquement). |
| Partenaire cible | Partenaire ayant reçu le processus métier (partenaire interne uniquement). |
| Rechercher dans | 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, le regroupement, 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

Procédure

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. Accédez à l'emplacement souhaité pour sauvegarder le fichier.

Résultats

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

Impression de rapports

Procédure

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 34. 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

Cette section décrit la série 200, la série 300, la série 400 et la série 500.

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 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 retard EDI FA

La page Recherche de FA EDI en retard fournit des critères de recherche permettant d'effectuer une recherche sur les accusés de réception fonctionnels (FA) d'échanges de données informatisés (EDI ou Electronic Data Interchange) 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.

Recherche d'enregistrements de FA d'EDI en retard Pourquoi et quand exécuter cette tâche

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

1. Cliquez sur **Outils > Rapports EDI > Rapport FA EDI en retard**. L'écran de recherche FA d'EDI en retard s'affiche.
2. Sélectionnez un ou plusieurs critères de recherche dans la liste déroulante :

Tableau 35. Critères de recherche de retard de FA d'EDI en retard

| 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. |
| Rechercher dans | Recherche sur le type du document source ou le type du document cible. |
| Package | Décrit le format, le regroupement, 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.

Affichage des rapports de package de FA d'EDI en retard

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

Le cas échéant, les données suivantes sont affichées dans le rapport de FA d'EDI en retard.

Tableau 36. Rapport de FA d'EDI en retard

| Valeur | Description |
|--------|--|
| Date | Date à laquelle l'EDI a été envoyé par le partenaire source au partenaire cible. |

Tableau 36. Rapport de FA d'EDI en retard (suite)

| Valeur | Description |
|--|--|
| 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 envoyé 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

Pourquoi et quand exécuter cette tâche

La page Recherche de transaction rejetée EDI contient des critères permettant d'effectuer des recherches sur des transactions EDI (Electronic Data Interchange) dont l'accusé de réception fonctionnel (FA) 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 EDI > Rapport EDI rejeté**.
2. Sélectionnez un ou plusieurs critères de recherche dans la liste déroulante :

Tableau 37. Critères de recherche de transactions 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. |
| Rechercher dans | Recherche sur le type du document source ou le type du document cible. |

Tableau 37. Critères de recherche de transactions EDI rejetées (suite)

| Valeur | Description |
|--------------------|--|
| Package | Décrit le format, le regroupement, 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.

Le cas échéant, les données suivantes sont affichées dans le rapport de transactions EDI rejetées.

Tableau 38. Rapport de transactions 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

Etats FTP fournit les informations détaillées suivantes :

- Statistiques FTP et connexions FTP
- Statistiques SFTP et connexions SFTP

Statistiques FTP

La page Statistiques FTP affiche l'état des serveurs FTP et SFTP en mode lecture seule.

Remarque : Les statistiques ne s'affichent pas si le serveur FTP / SFTP ou le serveur de gestion FTP / SFTP ne sont pas disponibles.

Affichage de l'état du serveur FTP Pourquoi et quand exécuter cette tâche

Pour afficher l'état des serveurs FTP et SFTP, procédez comme suit :

1. Cliquez sur **Outils > Rapports FTP > Statistiques FTP**. La page des statistiques FTP et SFTP s'affiche.
2. Sélectionnez Serveur FTP ou Serveur SFTP sous **Type de serveur**.
3. Les informations suivantes s'affichent sur l'état du serveur :

Tableau 39. Statistiques FTP

| Valeur | Description |
|--|--|
| Heure de démarrage du serveur | Heure de démarrage du serveur FTP ou SFTP. |
| 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. |

Tableau 39. Statistiques FTP (suite)

| Valeur | Description |
|----------------------------|---|
| Nombre total de connexions | Nombre total de connexions depuis la dernière réinitialisation. |

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

Connexions FTP

Pourquoi et quand exécuter cette tâche

Affichez les connexions FTP et SFTP en suivant les étapes ci-dessous :

1. Cliquez sur **Outils > Rapports FTP > Connexions FTP**.
2. Sélectionnez **Serveur FTP** ou **Serveur SFTP** sous **Type de serveur**. Suivant votre sélection, les détails de toutes les connexions serveur FTP ou SFTP sont affichés :

Tableau 40. 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. |

Chapitre 8. Boîte aux lettres Web

Les nouvelles fonctions fournies dans l'édition de la boîte aux lettres Web complètent la prise en charge antérieure de WebSphere Partner Gateway. Cela vous permet d'interagir avec le concentrateur en utilisant uniquement les navigateurs pris en charge, c'est-à-dire la prise en charge Web de l'interaction business-to-business. La version Web de la console WebSphere Partner Gateway s'ouvre dans un navigateur et il n'y a pas besoin d'infrastructure externe, telle qu'un serveur FTP, une fonction de message, etc. Les tâches supplémentaires suivantes peuvent être exécutées dans cette version de WebSphere Partner Gateway :

- Télécharger des documents pour des transactions
- Surveiller l'état des documents commerciaux
- Télécharger le document commercial reçu

Les pages Boîte de réception et Boîte d'envoi de la console sont corrélées à la vue de la boîte de réception et de la boîte d'envoi des messages électroniques. Vous pouvez utiliser cette fonction si vous ne disposez pas d'une infrastructure vous permettant de participer aux transactions. Ce chapitre présente les pages Boîte de réception, Boîte d'envoi et Envoyer un fichier de la console. Pour connaître les produits prérequis nécessaires, reportez-vous au *chapitre sur la boîte aux lettres Web du Guide de configuration du concentrateur* .

Remarque : Cette édition prend en charge les documents uniquement dans le package "None".

Fonctions de la boîte aux lettres Web

Cette boîte aux lettres Web dispose des fonctions suivantes :

- «Boîte de réception»
- «Boîte d'envoi», à la page 104
- «Envoyer le fichier», à la page 105

Boîte de réception

Pourquoi et quand exécuter cette tâche

Dans la page Boîte de réception de la console, vous pouvez rechercher les documents disponibles dans la boîte de réception. En outre, vous pouvez aussi télécharger le document reçu du partenaire, du client, ou du fournisseur. Pour rechercher un document dans la boîte de réception, procédez comme suit :

1. Entrez `http://<ip de la machine hôte>:58080/console` dans le navigateur.
2. Connectez-vous à la console comme un partenaire externe.
3. Accédez à **Administrateur du compte > Profils > Boîte de réception**.

- Entrez les caractéristiques connues dans les critères de recherche :

Tableau 41. Critères de recherche dans la boîte de réception

| Nom de zone | Description |
|--------------------|--|
| Envoyé par | Entrez le nom du partenaire expéditeur. |
| Nom de dossier | Si vous avez stocké les documents entrants dans différents dossiers, sélectionnez le dossier dans la liste déroulante. |
| Résultats par page | Le nombre de lignes contenues dans une vue donnée des résultats de la recherche est dépend de cette zone. |

- Cliquez sur Rechercher. Les résultats de la recherche fournissent les informations suivantes sur les documents reçus :

Tableau 42. Résultats de la recherche dans la boîte de réception

| Nom de zone | Description |
|------------------|--|
| Envoyé par | Partenaire qui a envoyé le document. |
| Nom du document | Nom du document reçu. |
| Type de document | Type du document reçu. Par exemple, facture, bon de commande, etc. |
| Horodatage | Date et heure auxquelles ce document a été reçu. |

Pour télécharger vers votre ordinateur un document reçu, procédez comme suit :

- Entrez `http://<ip de la machine hôte>:58080/console` dans le navigateur.
- Connectez-vous à la console comme un partenaire externe.
- Accédez à **Administrateur du compte > Profils > Boîte de réception**.
- Entrez les caractéristiques connues dans les critères de recherche. Voir tableau 41

Boîte d'envoi

Pourquoi et quand exécuter cette tâche

Dans la page Boîte d'envoi de la console, vous pouvez rechercher les documents disponibles dans votre boîte d'envoi. Vous pouvez aussi surveiller l'état des documents dans la boîte d'envoi. Pour rechercher un document dans la boîte d'envoi, procédez comme suit :

- Entrez `http://<ip de la machine hôte>:58080/console` dans le navigateur.
- Connectez-vous à la console comme un partenaire externe.
- Accédez à **Administrateur du compte > Profils > Boîte d'envoi**.
- Entrez les caractéristiques connues dans les critères de recherche :

Tableau 43. Critères de recherche dans la boîte d'envoi

| Nom de zone | Description |
|--------------------|---|
| Envoyé à | Partenaire auquel le document est envoyé. |
| Résultats par page | Le nombre de lignes contenues dans une vue donnée des résultats de la recherche est dépend de cette zone. |

5. Cliquez sur Rechercher. Les résultats de la recherche fournissent les informations suivantes sur les documents reçus :

Tableau 44. Résultats de la recherche dans la boîte d'envoi

| Nom de zone | Description |
|------------------|---|
| Envoyé à | Partenaire visé auquel le fichier est envoyé. |
| Nom du document | Nom du document envoyé. |
| Type de document | Type du document envoyé. Par exemple, facture, bon de commande, etc. |
| Horodatage | Date et heure auxquelles ce document a été reçu. |
| État | Indique l'état du document envoyé. Par exemple Soumis, En cours de traitement, Echec, etc. |
| Action | Vous permet d'appliquer l'action appropriée aux documents envoyés - arrêter et supprimer Arrêter arrêtera la suite du traitement du document et Supprimer supprimera le document de la boîte d'envoi. |

Envoyer le fichier

Étapes pour envoyer des fichiers depuis la console.

Pourquoi et quand exécuter cette tâche

Dans la page Envoyer des fichiers de la console, procédez comme suit pour envoyer des fichiers aux partenaires :

1. Accédez à **Administrateur du compte > Profils > Boîte d'envoi > Envoyer un fichier**.
2. Entrez les caractéristiques suivantes :

Tableau 45. Zones Envoyer un fichier

| Nom de zone | Description |
|------------------------|---|
| Fichier | Entrez le nom du fichier se trouvant dans votre répertoire local ainsi que son chemin. Vous pouvez aussi utiliser le bouton Parcourir pour sélectionner le fichier. |
| Envoyer à | Sélectionnez dans la liste le partenaire auquel envoyer le fichier entré sous Fichier . |
| Type de document | Entrez le type de document. |
| Mode de fonctionnement | Dans la liste, sélectionnez un mode de fonctionnement. Il définit la nature de la transmission. |

3. Cliquez sur **Envoyer**.

Limitations de la boîte aux lettres Web

Pour qu'un partenaire externe puisse utiliser les fonctions de boîte aux lettres Web, l'administrateur du concentrateur doit fournir les droits suivants :

- Peut envoyer un maximum de 10 Mo aux partenaires internes.

Remarque : Cela peut être plus ou moins en fonction du réseau, du navigateur ou de la mémoire.

- Ne peut pas supprimer le récepteur de la boîte Web.
- Ne peut pas envoyer les documents EDI/XML en format binaire.

Chapitre 9. Glossaire

Termes du 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

Actions exécutées sur un document par le système pour vérifier sa compatibilité avec les exigences commerciales entre les partenaires.

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 Les documents traités par le système ont quatre états :
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 entrant**

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 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.

ID Instance du processus

Numéro d'identification unique d'un processus métier spécifique.

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 défectueux, les zones de données et les événements associés.

P

Packages

Permet d'identifier les formats de regroupement 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'agir 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. Le contenu et la séquence de la transaction sont les paramètres habituels.

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 détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

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

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Burlingame Laboratory Director
IBM Burlingame Laboratory
577 Airport Blvd., Suite 800
Burlingame, CA 94010
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 nécessairement 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 relative aux capacités 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. Ces noms sont fictifs et toute ressemblance avec des noms ou adresses de personnes ou de sociétés réelles serait purement fortuite.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Licence sur les droits d'auteur

Le présent logiciel peut contenir des exemples de programme d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de reproduire, modifier et 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 un code intitulé ICU4J. Il vous est concédé sous licence par IBM conformément aux Conditions internationales d'utilisation des logiciels IBM (IPLA) et aux dispositions de licence relatives aux "Composants exclus". Cependant, IBM est tenue de mentionner le texte suivant :

NOTICE DE DROITS D'AUTEUR ET AUTORISATION

Copyright (c) 1995-2008 International Business Machines Corporation and others

All rights reserved.

Toute personne possédant une copie de ce Logiciel et des fichiers de documentation associés (le "Logiciel") est autorisée gratuitement à exploiter le Logiciel sans restriction, y compris et sans limitation à utiliser, copier, modifier, fusionner, publier, distribuer et/ou vendre des copies du logiciel et à autoriser les personnes auxquelles le Logiciel est fourni à en faire de même, sous réserve que les notices de droits d'auteur et la présente autorisation apparaissent dans toutes les copies du Logiciel et dans la documentation l'accompagnant.

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 LES TITULAIRES DE DROITS D'AUTEURS INCLUS DANS CETTE NOTICE NE POURRONT ETRE TENUS RESPONSABLES DE TOUTE RECLAMATION OU DE TOUT DOMMAGE SPECIAL, INDIRECT OU CONSECUTIF, OU PROVENANT D'UNE PERTE DE DONNEES OU DE BENEFICES, RESULTANT DE TOUTE ACTION LIEE A L'UTILISATION OU AUX PERFORMANCES DE CE LOGICIEL.

Sauf indication contraire dans cette notice, le nom des titulaires de droits d'auteur ne doit pas être utilisé à des fins de publicité ou de promotion de ce Logiciel sans autorisation écrite préalable de ces titulaires.

Documentation sur l'interface de programmation

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

Les interfaces de programmation 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 et services

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 et Advanced Editions, version 6.2.

Index

A

- Action, définition 12
- Activer une alerte 63
- Activité, définition 12
- administrateur du concentrateur
 - description 5
- Adresses
 - description 37, 64
 - éditer 64
 - supprimer 65
 - valeurs 65
- Affichage
 - Caractéristiques de destination 87
 - caractéristiques de l'événement, Afficheur d'événements 70
 - caractéristiques du document 81
 - Caractéristiques du message, Afficheur AS1/AS2 73
 - caractéristiques du processus et de l'événement, Analyse de document 91
 - Caractéristiques du processus RosettaNet 78
 - caractéristiques du traitement de documents, Afficheur RosettaNet 78
 - documents
 - Analyse de document 90
 - documents bruts 81
 - Documents de base 78
 - documents mis en file d'attente 86
 - erreurs de validation 82
 - événements 81
 - liste de destinations 84
- Afficher
 - Caractéristiques de destination 58
 - caractéristiques de l'alerte et contacts 62
 - caractéristiques du contact 60
 - liste de destinations 57
- Afficher la console 9
- Afficheur AS1/AS2 79
 - affichage des caractéristiques du message 73
 - caractéristiques du package 73
 - critères de recherche 72
 - description 71
 - recherche de messages 72
- Afficheur d'événements 24
 - affichage des caractéristiques de l'événement 70
 - critères de recherche 69
 - description 67
- Afficheur de documents
 - caractéristiques du document 81
 - critères de recherche 80
 - description 79
 - valeurs 72, 73, 81
 - valeurs de traitement du document 81

- Afficheur RosettaNet
 - affichage des caractéristiques du processus 78
 - critères de recherche 77
 - description 76
 - recherche de processus 77
 - traitement de documents, caractéristiques 78
- Afficheurs
 - Afficheur AS1/AS2 71
 - Afficheur d'événements 67
 - Afficheur de documents 79
 - Afficheur RosettaNet 76
 - description 67
- Ajouter un contact à une alerte existante 36
- Alertes
 - afficher ou éditer les caractéristiques de l'alerte et les contacts 62
 - ajouter un contact à une alerte existante 36
 - créer une alerte basée sur le volume 32
 - créer une alerte de type événement 34
 - critères de recherche 63
 - critères de recherche, Partenaires 63
 - désactiver une alerte 63
 - description 30, 62
 - rechercher des alertes 63
 - supprimer une alerte 64
- Analyse de document
 - affichage des caractéristiques du processus et de l'événement 91
 - affichage des documents 90
 - critères de recherche 90
 - description 89
- attribut AS signé 26
- attribut Chiffrement AS 24
- Attributs AS
 - AS chiffré 24
 - AS signé 26
- authentification client
 - configuration 19
 - couche SSL entrante 19

B

- bcgClientAuth.jacl script
 - configuration de l'authentification du client 19

C

- caractéristiques de la destination, affichage 87
- Caractéristiques du package Afficheur AS1/AS2 73
- certificat
 - signature 25

- Certificat client SSL, définition 17
- Certificat de signature numérique, définition 17
- Certificat numérique VTP
 - définition 18
- Certificat X.509, définition 16
- Certificats
 - formats pris en charge 17
- certificats de signature
 - entrée 25
- certificats de signature de communication entrante 25
- certificats principaux
 - chiffrement des communications sortantes 20
- certificats secondaires
 - chiffrement des communications sortantes 20
- certificats SSL
 - authentification client, communications entrantes 19
 - entrée 18
- chiffrement
 - activation 24
 - déchiffrement 17
 - définition 16
 - description 17
- Clé, définition 16
- Clé auto-signée, définition 16
- Clé privée, définition 16
- Clé publique, définition 16
- Codes de résultat
 - Serveur Web 94
- Codes de résultat du serveur Web 94
- commandes
 - FTP 50
- commandes FTP 50
- Communauté de concentrateur
 - description 5
- Connexions FTP
 - rapport 101
- Console de communauté
 - afficher 9
 - utilisateurs 5
 - utilisation 8
- Contacts
 - afficher ou éditer les caractéristiques du contact 60
 - caractéristiques 61
 - description 28, 60
 - retirer le contact 62
 - valeurs 60, 61
- couche SSL entrante
 - authentification client 19
- Création
 - alerte basée sur le volume 32
 - alerte de type événement 34
 - passerelles 11
 - Rapport du volume de document 92
- Création de destinations SFTP 53

Création de destinations SFTP sur les systèmes sur lesquels la sécurité administrative WAS est activée 53
Critères de recherche
 Afficheur AS1/AS2 72
 Afficheur d'événements 69
 Afficheur de documents 80
 Afficheur RosettaNet 77
 alertes 63
 Analyse de document 90
 Rapport du volume de document 93
 retard de FA d'EDI 97
 Transactions EDI rejetées 98

D

Déchiffrement
 définition 16
Désactiver une alerte 63
destination
 affichage de la liste 84
 affichage des caractéristiques 87
 affichage des documents mis en file d'attente 86
 modification de l'état 87
 suppression de documents de la file d'attente 87
destination par défaut
 exemple de définition 55
Destination par défaut
 afficher 58
 éditer 58
 sélectionner 58
destinations
 afficher ou éditer les caractéristiques de la destination 58
 afficher une liste 57
 fichier-répertoire 46
 FTP 42, 43
 FTPS 48
 HTTP 40
 HTTPS 41
 JMS 45
 par défaut 55
 Script FTP 51
 Scripts FTP 49
 SFTP 53
 SMTP 44
 transports pris en charge 39
 valeurs 58
destinations FTP 43
destinations JMS 45
destinations SMTP 44
Document
 caractéristiques, Afficheur de documents 81
 valeurs de traitement, Afficheur de documents 81
Documents
 affichage des éléments mis en file d'attente 86
 suppression de la file d'attente 87
Documents de base
 affichage 78
Documents mis en file d'attente,
 affichage 86
DUNS+4 11

E

Editer
 adresse 64
 Caractéristiques de destination 58
 caractéristiques de l'alerte et contacts 62
 caractéristiques du contact 60
Erreurs de validation
 affichage 82
état de la destination, modification 87
Etats du document
 définitions 89
 Rapport du volume de document 92
Evénements
 critères de recherche 69
 recherche 69
événements d'erreur 70
Evénements Débogage 68
Exportation
 Rapport du volume de document 93

F

FA d'EDI en retard
 rapport 97
File d'attente, suppression de documents 87
fonctions B2B, description 11
Fonctions de l'Administrateur du compte 57

I

Icônes 6
Impression de rapports
 Rapport du volume de document 93
Irréfutabilité, définition 16

M

message Aucun certificat de chiffrement valide n'a été trouvé 24
message Certificat retiré ou arrivé à expiration 24
Modification
 état de la destination 87

N

Numéros DUNS 11
Numéros ID à format libre 11

O

OpenPGP 16
option Valider le certificat SSL du client 19
Outils
 Analyse de document 89
 description 89
 Rapport du volume de document 92
 Test de la connexion du partenaire 94

P

Package, définition 12
paramètres de configuration
 destinations 55
partenaire
 description 5
partenaire externe
 description 5
partenaire interne
 description 5
Passerelles
 création 11
 description 57
planification en fonction d'un intervalle
 destination de script FTP 52
planification en fonction du calendrier
 destination de script FTP 52
profil partenaire
 affichage 10
 description 10
 édition 10
 valeurs 10
Protocole, définition 12

R

Rapport
 Connexions FTP 101
 Connexions SFTP 101
 FA d'EDI en retard 97
 Statistiques FTP 100
 Statistiques SFTP 100
 Transactions d'EDI rejetées 99
Rapport du volume de document
 création 92
 critères de recherche 93
 description 92
 états du document 92
 exportation 93
 impression 93
Rechercher
 alertes 63
 des événements 69
 des processus RosettaNet 77
 messages, Afficheur AS1/AS2 72
retard de FA d'EDI
 critères de recherche 97
Retirer
 alerte 64
 contact 62

S

scripts FTP
 commandes autorisées dans 50
 destinations 49
Se connecter à la console 9
Se déconnecter de la console 9
signature numérique
 activation 26
Signature numérique, définition 16
Statistiques FTP
 rapport 100
Suppression de documents de la file d'attente 87

Supprimer
adresse 65

T

Test de la connexion du partenaire
Codes de résultat du serveur Web 94
description 94
valeurs 94
Transactions d'EDI rejetées
critères de recherche 98
rapport 99
transports
destination, fournie par le
système 39
Type d'événement Avertissement 68
Type d'événement Critique 68
Type d'événement Erreur 68
Type d'événement Information 68
type de document, définition 12
Types d'événements 68
descriptions 68

U

Utilisateurs
description 26

V

Valeurs
Adresses 65
Afficheur de documents 72, 73, 81
Contacts 60, 61
destinations 58
profil partenaire 10
Test de la connexion du
partenaire 94

Z

Zones d'erreur
erreurs de validation 82

