WebSphere®

IBM WebSphere Partner Gateway Enterprise und Advanced Edition

Version 6.2.1

Verwaltung

IBM

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen im Abschnitt „Bemerkungen" auf Seite 287 gelesen werden.

Februar 2011

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM WebSphere Partner Gateway Enterprise and Advanced Editions Version 6.2.1 Administration Guide,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
SW TSC Germany
Kst. 2877
Februar 2011

Inhaltsverzeichnis

Kapitel 1. Zu diesem Handbuch

Im vorliegenden Dokument wird beschrieben, wie WebSphere Partner Gateway eingesetzt werden kann, um die Anforderungen der B2B-Handelsgemeinschaft (Business-to-Business Trading Community) zu erfüllen. Hierbei wird davon ausgegangen, dass Sie die erforderlichen Tasks zur Konfiguration des Hubs, die im Handbuch *WebSphere Partner Gateway Hubkonfiguration* aufgelistet sind, bereits ausgeführt haben.

Zielgruppe

Administratoren, die WebSphere Partner Gateway anwenden. Im vorliegenden Handbuch werden die beiden folgenden Administratortypen unterschieden:

- Hubadministrator: Dies ist der Superuser in der Community. Er ist verantwortlich für die Konfiguration und Verwaltung der gesamten Hub-Community einschließlich der Partnerkonfiguration und der Verbindungsaktivierung.
- Kontenadministrator (Kontenadmin): Hat Zugriff auf eine Untergruppe der Funktionen des Hubadministrators und ist der wichtigste Benutzer mit Verwaltungsaufgaben für den internen Partner oder den externen Partner.
- Interner Partner: Das primäre Unternehmen und die treibende Kraft innerhalb der Hub-Community. Der interne Partner ist für den Erwerb und das Erstellen der Hub-Community verantwortlich. Darüber hinaus stellt der interne Partner die Definition der Transaktionen für die elektronischen Geschäftsprozesse, die zwischen dem internen Partner und seinen externen Partnern abgewickelt werden, bereit.
- Externer Partner: Das Unternehmen, das Geschäfte mit dem internen Partner über die Hub-Community abwickelt. Externe Partner müssen einen Konfigurationsprozess ausführen, damit sie eine Verbindung zur Hub-Community herstellen können. Wenn die Verbindung hergestellt ist, können externe Partner elektronische Geschäftsdokumente mit dem internen Partner austauschen.

Weitere Informationen zum Hubadministrator, dem internen Partner und dem externen Partner finden Sie im *WebSphere Partner Gateway Partnerhandbuch*.

Rollen, Zugriffsebenen und Zuständigkeiten

In WebSphere Partner Gateway richtet der Hubadministrator die Profile der Partner ein. Ein Partner verfügt immer über mindestens einen Administratorbenutzer, und der Administrator diese Profils kann weitere Benutzer hinzufügen.

Um das Konzept der Rollen darzustellen, wird im Folgenden eine einfache Implementierung von WebSphere Partner Gateway mit mindestens drei Profilen beschrieben:

Hubbetreiber

Dies ist ein vom System definiertes Profil, das bei der Installation auf der Maschine eingerichtet wird. Das Profil "Hubbetreiber" enthält den definierten Benutzernamen "hubadmin". Dieser Benutzer ist der Superuser des Systems, der alle Konfigurationstasks ausführen kann. Sie können diese Rolle der IT-Gruppe zuordnen, die den WebSphere Partner Gateway-Server betreibt; sie sendet jedoch keine Dokumente

aktiv hin und her. Es kann nur ein Teilnehmer des Typs "Hubbetreiber" vorhanden sein. Da 'hubadmin' ein Systembenutzer ist, dürfen Sie den Benutzerstartus von 'hubadmin' nicht ändern.

Interner Partner

Dieser Partner wird vom Benutzer "hubadmin" erstellt. Bei diesem Benutzer handelt es sich um das Unternehmen, das die WebSphere Partner Gateway-Software erworben hat und das System ausführt. Es können viele interne Partner vorhanden sein; allerdings gibt es nur einen internen Standardpartner. Ein Unternehmen fungiert sowohl als Hubbetreiber als auch als interner Partner, wenn es die Task der Konfiguration und Überwachung des WebSphere Partner Gateway-Systems nicht an eine interne IT-Gruppe oder an eine Fremdfirma delegiert.

Externer Partner

Dies ist der Partner, mit dem der interne Partner kommuniziert. Es können viele Partner dieses Typs vorhanden sein. Wenn der Partner eine eigene Implementierung von WebSphere Partner Gateway verwendet, ist er auf seinem eigenen System der interne Partner, aber auf dem aktuellen System der externe Partner.

Jedes dieser Profile verfügt über mindestens eine Benutzer-ID. Wie bereits beschrieben, ist der Benutzer "hubadmin" im Profil "Hubbetreiber" der Superuser des Systems. Den anderen beiden Profilen wird bei ihrer ersten Erstellung jeweils ein Benutzer mit Administratorberechtigung zugeordnet. Diese Benutzer können ihrerseits weitere Benutzer mit denselben oder weniger Fähigkeiten erstellen. Jeder dieser Benutzer mit Administratorberechtigung hat bestimmte Berechtigungen für die Konfiguration. So kann der Benutzer "hubadmin" beispielsweise alle Objekte auf dem System (zum Beispiel den internen Partner) erstellen oder systemweite Sicherheitszertifikate laden. Die Rolle des internen Partners kann Teilnehmer oder Verbindungen erstellen. Die Rolle des externen Partners hat die meisten Einschränkungen und kann eigene Dokumente anzeigen und die lokalen Ziele konfigurieren, an die der interne Partner Dokumente zustellen soll.

Typografische Konventionen

In diesem Dokument werden die folgenden Konventionen verwendet.

Tabelle 1. Typografische Konventionen

Konvention	Beschreibung
`Monospaceschrift`	In Monospaceschrift dargestellter Text kennzeichnet Elemente, die vom Benutzer eingegeben werden müssen, Werte für Argumente oder Befehlsoptionen, Beispiele und Codebeispiele sowie Informationen, die vom System am Bildschirm ausgegeben werden (Nachrichtentexte oder Systemanfragen).
Fettdruck	In Fettdruck dargestellter Text kennzeichnet Steuerelemente der grafischen Benutzerschnittstelle (z. B. die Namen von Schaltflächen, Menüs oder Menüoptionen) und Spaltenüberschriften in Tabellen und im Fließtext.
Kursivschrift	In Kursivschrift dargestellter Text kennzeichnet Hervorhebungen, Buchtitel, neue Termini und Termini, die im Text definiert werden. Darüber hinaus werden in Kursivschrift Variablennamen und alphabetische Zeichen dargestellt, die als Literalwerte benutzt werden.

Tabelle 1. Typografische Konventionen (Forts.)

Konvention	Beschreibung
Monospaceschrift in Kursivdruck	In kursiv gedruckter Monospaceschrift dargestellter Text kennzeichnet Variablennamen innerhalb von Textsegmenten, die in Monospaceschrift gedruckt sind.
ProductDir	*ProductDir* steht für das Verzeichnis, in dem das Produkt installiert wurde. Alle IBM WebSphere Partner Gateway-Programmpfadnamen beziehen sich auf das Verzeichnis, in dem das Programm IBM WebSphere Partner Gateway auf Ihrem System installiert ist.
%text% und *$text*	Text in Prozentzeichen (%) gibt den Wert für den Text der Windows(R)-Systemvariablen bzw. Benutzervariablen an. Analog ist die Notation in einer UNIX(R)-Umgebung $*text*, wodurch der Wert der UNIX-Umgebungsvariable *text* dargestellt wird.
Unterstrichener farbiger Text	Unterstrichener farbiger Text kennzeichnet Querverweise. Wenn Sie auf diesen Text klicken, springt das System zu dem Objekt, auf das verwiesen wird.
Text in einem blauen Rahmen	(Nur in PDF-Dateien:) Ein Rahmen um ein Textelement kennzeichnet einen Querverweis. Wenn Sie auf den umrandeten Text klicken, wird das Objekt aufgerufen, auf das sich der Verweis bezieht. Diese Konvention in PDF-Dateien entspricht der in der vorliegenden Tabelle bereits erläuterten Textkonvention mit dem unterstrichenen farbigen Text.
" " (Anführungszeichen)	(Nur in PDF-Dateien:) Querverweise auf andere Abschnitte des Dokuments stehen in Anführungszeichen.
{ }	In einer Zeile mit Syntaxelementen wird in geschweiften Klammern eine Gruppe von Optionen dargestellt, aus der eine Option ausgewählt werden muss.
[ ]	In einer Zeile mit Syntaxelementen wird in eckigen Klammern ein optionaler Parameter dargestellt.
< >	In spitzen Klammern stehen variable Elemente eines Namens, um diese voneinander zu unterscheiden. Beispiel: <*servername*><*connectorname*>tmp.log.
/ oder \	Backslashes (\) werden in Windows-Installationen zur Trennung der einzelnen Elemente eines Verzeichnispfads verwendet. In UNIX-Installationen müssen Sie anstelle der Backslashes Schrägstriche (/) angeben.

Referenzliteratur

Die gesamte, zum vorliegenden Produkt bereitgestellte Dokumentation enthält umfassende Informationen zur Installation, Konfiguration, Verwaltung und Verwendung von WebSphere Partner Gateway Enterprise Edition und Advanced Edition.

Diese Dokumentation kann aus dem Internet heruntergeladen oder direkt auf der folgenden Website angezeigt werden:

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

Hinweis: Die neuesten Informationen zu diesem Produkt finden Sie in den technischen Hinweisen (Technotes) der technischen Unterstützungsfunktion oder in Flashes auf der Unterstützungswebsite für WebSphere Partner Gateway.

Greifen Sie auf die folgende Website zu und wählen Sie den Bereich mit den für Sie relevanten Informationen aus:

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

Neuerungen in Release 6.2.1

WebSphere Partner Gateway Version V6.2.1 unterstützt die folgenden neuen Funktionen:

- Die Web-Mailbox stellt webbasiert Unterstützung für B2B-Interaktionen bereit. Partner, Kunden und Lieferanten interagieren einfach über einen Internet-Browser mit dem WebSphere Partner Gateway-Hub.
- Neben dem integrierten FTP-Server wird nun auch ein integrierte SFTP-Server unterstützt.
- OpenPGP-Zertifikate werden in WebSphere Partner Gateway unterstützt.
- Unterstützung für WebSphere Application Server ND V7.0.0.13, WebSphere Messaging Queue 7.0 und WTX 8.3 wurde hinzugefügt.
- Plattformunterstützung für Windows 2008, Windows 7 und SLES 11 wurde hinzugefügt.
- Unterstützung für Power 7 im Toleranzmodus (P6/P6+-kompatibler Modus).
- Unterstützung für Virtualisierung - VMware® ESX unter Windows und Linux, Power VM unter AIX.

Kapitel 2. Komponentenanwendungen von WebSphere Partner Gateway verwalten

Die Verwaltung der Komponentenanwendungen von WebSphere Partner Gateway umfasst das Starten, Stoppen und Konfigurieren der Anwendungsserver, die die Hosts für die WebSphere Partner Gateway-Komponenten sind. Für diese Verwaltungsaufgaben werden im Allgemeinen WebSphere Application Server-Schnittstellen verwendet, die eine Gruppe von Anwendungsservern steuern und konfigurieren, auf denen die WebSphere Partner Gateway-Komponenten durch den Installationsprozess implementiert werden.

Wie Sie die Komponentenanwendungen von WebSphere Partner Gateway verwalten, hängt davon ab, ob das Programm im Rahmen einer einfachen oder einer verteilten Topologie installiert wurde. Für dieses Dokument werden die Begriffe "Einfacher Modus" und "Verteilter Modus" verwendet, was sich jeweils auf die während der Produktinstallation gewählte Topologie bezieht.

Anmerkung: Details zu einfachen und verteilten Topologien finden Sie im Handbuch *WebSphere Partner Gateway Installation*.
Der Administrator, der die Komponenten von WebSphere Partner Gateway verwaltet, muss den Installationsmodus (einfach oder verteilt) kennen.

Bei einer Installation im einfachen Modus werden sämtliche WebSphere Partner Gateway-Komponenten auf demselben Computer installiert, und dazu wird ein Anwendungsserver mit der Bezeichnung `Server1` verwendet. Da Deployment Manager von einem System im einfachen Modus nicht verwendet wird, erfolgt das Starten und Stoppen der WebSphere Partner Gateway-Komponenten ähnlich wie bei der Basisimplementierung (und nicht die Netzimplementierung) von WebSphere Application Server.

Auf allen Computern kann WebSphere Application Server installiert sein, doch nur für Deployment Manager ist die Installation von WebSphere Application Server Network Deployment erforderlich.

Sämtliche Anwendungsserver, die die Hosts für die WebSphere Partner Gateway-Komponenten sind, sind logisch in einer Deployment Manager-Zelle enthalten, die über die Deployment Manager-Anwendung verwaltet wird. Diese Unterscheidung ist jedoch nicht sichtbar, wenn Sie Deployment Manager für Verwaltungstasks verwenden. Die Konsole von Deployment Manager enthält eine Sicht der verteilten Komponentenanwendungen von WebSphere Partner Gateway, in der die Details über den Installationsort der Komponenten ausgeblendet werden.

WebSphere Partner Gateway-Komponenten in einem System mit einfachem Modus verwalten

In einem System mit einfachem Modus müssen Sie wissen, wie der Anwendungsserver zu starten und zu stoppen ist, der der Host sämtlicher Komponenten von WebSphere Partner Gateway ist.

Führen Sie eins der folgenden Scripts aus, um die Komponenten von WebSphere Partner Gateway zu starten:

- UNIX(R)

<*installationsverzeichnis*>/bin/bcgStartServer.sh

- Windows(R)

  <*installationsverzeichnis*>\bin\bcgStartServer.bat

Führen Sie eins der folgenden Scripts aus, um die Komponenten von WebSphere Partner Gateway zu stoppen:

Anmerkung: Sie müssen dabei keinen Servernamen angeben. Wenn der einfache Modus verwendet wird, ist der Servername immer `Server1`.

- UNIX(R)

  <*installationsverzeichnis*>/bin/bcgStopServer.sh

- Windows(R)

  <*installationsverzeichnis*>\bin\bcgStopServer.bat

WebSphere Partner Gateway-Komponenten in einem System mit verteiltem Modus verwalten

In einem System mit verteiltem Modus wird die WebSphere Deployment Manager-Anwendung verwendet, um sämtliche Anwendungen von WebSphere Partner Gateway zu steuern. Während der Installation wird einer der Computer in dem System mit verteiltem Modus ausgewählt, der der Host des Deployment Managers sein soll. Wenn die WebSphere Partner Gateway-Anwendungen installiert werden, wird der bzw. werden die Anwendungsserver, auf dem/denen sie installiert werden, unter die Kontrolle und Steuerung des Deployment Managers gestellt. Als Systemadministrator verwalten Sie die WebSphere Partner Gateway-Komponenten über den Deployment Manager. Damit steht Ihnen ein zentraler Zugriff auf alle Komponenten zur Verfügung, selbst wenn diese sich auf unterschiedlichen Computern befinden.

In der Produktdokumentation von WebSphere Application Server Network Deployment finden Sie eine ausführliche Beschreibung, wie ein Deployment Manager verwendet wird, um Anwendungsserver zu verwalten. Für dieses Dokument werden einige Begriffe und Konzepte im Hinblick auf die Arbeitsweise des Deployment Managers verwendet.

Konzepte und Begriffe der verteilten Topologie

- Das System besteht aus einem oder aus mehreren Knoten.
- WebSphere Deployment Manager ist eine Anwendung, die auf einem der Knoten im System ausgeführt wird.
- Die WebSphere Partner Gateway-Komponenten (Konsole, Empfänger und Document Manager) werden auf Anwendungsservern auf den Knoten des Systems installiert.
- Die standardmäßige Nachrichtenunterstützung von WebSphere Application Server wird verwendet; daher enthält der Server "bcgmas" die von WebSphere Partner Gateway für die interne Nachrichtenunterstützung benötigten Nachrichtenwarteschlangen.
- Jeder Knoten, der der Host einer WebSphere Partner Gateway-Komponente ist, verfügt über eine spezielle Anwendung mit dem Namen Knotenagent. Der Knotenagent stellt eine Verbindung zwischen den Anwendungsservern auf dem Knoten und der Deployment Manager-Anwendung bereit.

- Die Knoten werden zu einer logischen Gruppierung kombiniert, die Zelle genannt wird. Der Deployment Manager stellt Ihnen eine Sicht der Zelle zur Verfügung, über die Sie die Anwendungen im System verwalten können.
- Die Anwendungsserver auf den Knoten innerhalb der Zelle sind in Clustern zusammengefasst. Sämtliche Anwendungsserver in einem Cluster haben dieselben WebSphere Partner Gateway-Komponenten.
- Die Zelle wird vom zentralen WebSphere Deployment Manager verwaltet. Dies bedeutet Folgendes:
  - Alle Server innerhalb einer Zelle können über den Deployment Manager gestartet, gestoppt und modifiziert werden.
  - Der interne Nachrichtenaustausch kann über den Deployment Manager verwaltet werden.
- Es gibt zwei Varianten des verteilten Modus, den einfachen verteilten Modus und den vollständigen verteilten Modus.
  - Im einfachen verteilten Modus sind alle drei WebSphere Partner Gateway-Komponenten Teil desselben Clusters. Hierzu gehört auch ein Cluster auf dem Server "bcgmas".
  - Im vollständigen verteilten Modus befindet sich jede Komponente üblicherweise in ihrem eigenen Cluster; so befindet sich z. B. die Konsole in einem `bcgconsole`-Cluster, der Empfänger in einem `bcgreceiver`-Cluster und Document Manager in einem `bcgdocmgr`-Cluster. Außerdem gibt es einen `bcgmas`-Cluster für den Nachrichtenaustausch, der für die interne Kommunikation zwischen den WebSphere Partner Gateway-Komponenten verwendet wird.

Deployment Manager

Aufgabe des Deployment Managers ist es, Ihnen eine zentrale Übersicht aller Anwendungsserver in einer Zelle zu bieten, über die Sie die Server verwalten können. Dazu muss ein Knotenagent auf jedem Knoten, der der Host von WebSphere Partner Gateway-Komponenten ist, aktiv sein. Der Deployment Manager verwendet die Knotenagenten, um mit den Anwendungsservern im System zu interagieren. Während der Installation im verteilten Modus wird für jeden Knoten im System ein Knotenagent installiert und konfiguriert, um mit dem Deployment Manager zu kommunizieren.

Über die Webschnittstelle des Deployment Managers können Sie die Anwendungen verwalten, die sich in einer Zelle befinden. Falls der Deployment Manager aus irgendeinem Grund nicht verfügbar ist, können die Komponenten von WebSphere Partner Gateway manuell über eine Befehlszeile gestartet oder gestoppt werden, jedoch können keine anderen Verwaltungsaufgaben ausgeführt werden, bis der Deployment Manager wieder verfügbar ist.

Die gängigsten ausgeführten Verwaltungsaufgaben sind das Starten und Stoppen der WebSphere Partner Gateway-Komponenten. Auch andere Verwaltungsaufgaben können mit dem Deployment Manager ausgeführt werden, wie etwa das Konfigurieren eines Servers für die Protokollierung und Traceerstellungoder das Ändern der Initialisierungsparameter für die vom Server verwendete Java Virtual Machine.

Gehen Sie wie folgt vor, um den Deployment Manager zu verwenden:

1. Starten Sie den Knotenagenten auf allen Knoten, die die Hosts von WebSphere Partner Gateway-Anwendungen sind und außerdem den Knoten, auf dem der Server bcgmas installiert ist. Führen Sie das WebSphere-Script `startNode` ohne Argumente aus, um den Knotenagenten auf einem Computer zu starten. Das

Script befindet sich im Verzeichnis *<WebSphere_Partner_Gateway_installationsverzeichnis>*/wasND/Profiles/bcgprofile/bin.

2. Starten Sie den Deployment Manager. Führen Sie das WebSphere Partner Gateway-Script bcgStartServer ohne Argumente aus, um den Deployment Manager zu starten. Das Script befindet sich im Verzeichnis *<Deployment_Manager_installationsverzeichnis>*\bin.
3. Öffnen Sie einen geeigneten Internet-Browser.
4. Navigieren Sie zu http://*<name_des_computers_oder_ip-adresse_des_deployment_managers>*:55090/ibm/console, um die Eingangs- und Anmeldeanzeige von WebSphere Integrated Solutions Console zu öffnen, und melden Sie sich an.

   Anmerkung: Für die Anmeldung ist keine Benutzer-ID erforderlich. Auf der linken Seite der Eingangsanzeige sehen Sie eine Liste der Tasks, die über diese Konsole ausgeführt werden können.
5. Gehen Sie wie folgt vor, um alle Server in einem Cluster zu starten oder zu stoppen:
   - Klicken Sie im linken Fensterbereich auf **Cluster**.
   - Wählen Sie im rechten Fensterbereich aus, ob der Cluster gestartet oder gestoppt werden soll.
   - Klicken Sie auf **Starten** oder **Stoppen**.

     Anmerkung: Diese Operation beansprucht möglicherweise einige Minuten. Sie können die Anzeige ab und zu aktualisieren, um den Status zu verfolgen.
6. Gehen Sie wie folgt vor, um einzelne Server zu starten oder stoppen:
   a. Klicken Sie im linken Fensterbereich auf **Anwendungsserver**.
   b. Wählen Sie im rechten Fensterbereich den Server aus, der von dem Knoten gestartet oder gestoppt werden soll.

      Anmerkung: Ein Knoten steht für eine Instanz von WebSphere Application Server, die auf einem Computer in Ihrem System implementiert ist.
   c. Klicken Sie auf **Starten** oder **Stoppen**.

Server über Befehlszeile starten oder stoppen

Wenn der Deployment Manager nicht verfügbar ist, können die Komponenten von WebSphere Partner Gateway in einem System mit verteiltem Modus auf den einzelnen Computern manuell gestartet oder gestoppt werden. Allgemeine Verwaltungsaufgaben, wie z. B. das Ändern von Protokoll- oder Traceeinstellungen können nicht ausgeführt werden, wenn der Deployment Manager nicht verfügbar ist.

Gehen Sie wie folgt vor, um die Befehlszeilenscripts zu verwenden:

1. Starten Sie den Knotenagenten auf allen Knoten, die die Hosts von WebSphere Partner Gateway-Anwendungen sind, und außerdem den Knoten, auf dem der Server bcgmas installiert ist. Führen Sie das WebSphere-Script startNode ohne Argumente aus, um den Knotenagenten auf einem Computer zu starten. Das Script befindet sich im Verzeichnis *WebSphere_Partner_Gateway_installationsverzeichnis*/wasND/Profiles/bcgprofile/bin.
2. Starten Sie jeden einzelnen WebSphere Partner Gateway-Server, indem Sie das Script startServer ausführen, das sich im Verzeichnis

<WebSphere_Partner_Gateway_installationsverzeichnis>/wasND/Profiles/bcgprofile/bin auf dem Computer befindet, auf dem der Server installiert wurde. Die Syntax lautet:

```
startServer <servername>
```

Dabei steht *servername* für "bcgconsole", "bcgreceiver", "bcgdocmgr" oder "bcgmas".

3. Stoppen Sie jeden einzelnen WebSphere Partner Gateway-Server, indem Sie das Script stopServer ausführen, das sich im Verzeichnis *WebSphere_Partner_Gateway_installationsverzeichnis*/wasND/Profiles/bcgprofile/bin auf dem Computer befindet, auf dem der Server installiert wurde.

   Die Syntax lautet:

   ```
   stopServer <servername>
   ```

   Dabei steht *servername* für "bcgconsole", "bcgreceiver", "bcgdocmgr" oder "bcgmas".

FTP-Management-Server über die Befehlszeile starten und stoppen

Der FTP-Management-Server muss aktiv sein, damit der FTP-Server über WebSphere Partner Gateway Console verwaltet werden kann. Verwenden Sie das Script **startftpmgmtserver**, um die FTP-Management-Server auf einem Computer zu starten. Dieses Script befindet sich im Verzeichnis '*installationsverzeichnis*/ftpserver/bin' von WebSphere Partner Gateway. Für das Script sind keine Befehlszeilenparameter erforderlich. Der integrierte FTP-Server wird implizit gestartet, wenn der FTP-Management-Server gestartet wird.

Verwenden Sie das Script **stopftpmgmtserver**, um die FTP-Management-Server auf einem Computer zu stoppen. Dieses Script befindet sich im Verzeichnis '*installationsverzeichnis*/ftpserver/bin' von WebSphere Partner Gateway. Für das Script sind keine Befehlszeilenparameter erforderlich. Der integrierte FTP-Server wird implizit gestoppt, wenn der FTP-Management-Server gestoppt wird.

Anmerkung: Dies gilt für alle Implementierungsmodi.

SFTP-Management-Server über die Befehlszeile starten und stoppen

SFTP wird im SFTP-Management-Server ausgeführt. Daher wird bei jedem Start des SFTP-Management-Servers auch der SFTP-Server automatisch gestartet. Der Standardport des SFTP-Management-Servers ist 2050. Wenn Sie den Server an einem anderen Port starten wollen, müssen Sie den Eintrag

```
bcg.config.ftpmanagement.sftpmgmt.port=<port>
```

zu Eigenschaftendatei

```
ftpserver.init
```

hinzufügen. Hierdurch wird der Standardwert für den Port durch den für <port> eingegebenen Wert ersetzt. Wenn Sie den Server starten, ohne den Hostschlüssel zu konfigurieren, wird die folgende Warnung angezeigt: “Warnung: Für den Server ist kein Hostschlüssel definiert.”

Um den SFTP-Server über die Befehlzeile zu starten oder zu stoppen, müssen Sie unter Linux den Befehl

```
./startsftpmgmtserver.sh
```

und unter Windows den Befehl

```
./startsftpmgmtserver.bat
```

ausführen.

Komponenten in einem System mit einfachem verteiltem Modus starten und stoppen

In einem System mit einfachem verteiltem Modus sind zwei Cluster vorhanden:

bcgmasCluster
: Der Cluster für den Nachrichtenaustausch, in dem die Nachrichtenserver enthalten sind. Mindestens ein Nachrichtenserver muss aktiv sein, damit die WebSphere Partner Gateway-Komponenten betrieben werden können.

bcgserverCluster
: Der Cluster für die WebSphere Partner Gateway-Komponenten, zu dem die Server mit dem Namen `bcgserver` gehören. Die drei Komponenten (Konsole, Empfänger und Router) sind auf `bcgserver` installiert.

Die hier verwendeten Namen sind die vom Installationsprogramm gewählten Standardnamen. Beachten Sie, dass das Installationsprogramm auch andere Namen ausgewählt haben kann und Sie dann diese Namen (anstelle der Standardnamen) verwenden müssen.

Server in einem System mit einfachem verteiltem Modus starten

Bevor Sie Ihren Server in einem System mit einfachem verteiltem Modus starten, müssen Sie die Nachrichtenserver noch vor den WebSphere Partner Gateway-Komponentenservern starten.

Alle Server mit Deployment Manager starten

1. Vergewissern Sie sich, dass der Knotenagent auf sämtlichen Knoten aktiv ist, auf denen die Server `bcgmas` und `bcgserver` installiert sind.
2. Wählen Sie über die Deployment Manager-Konsole den Nachrichtencluster `bcgmasCluster` aus und klicken Sie auf **Starten**.
3. Warten Sie, bis der Cluster `bcgmasCluster` gestartet wurde, bevor Sie den nächsten Schritt ausführen.
4. Wählen Sie den Cluster `bcgserverCluster` aus und klicken Sie auf **Starten**.

Einzelne Server auf allen Computern starten

1. Vergewissern Sie sich, dass die Knotenagenten auf sämtlichen Knoten aktiv sind, auf denen die Server `bcgmas` und `bcgserver` installiert sind.
2. Wählen Sie den Nachrichtenserver `bcgmas` aus und klicken Sie auf **Starten**.
3. Wiederholen Sie den vorherigen Schritt und starten Sie auch die anderen `bcgmas`-Server.

   Anmerkung: Warten Sie, bis mindestens einer der Nachrichtenserver gestartet wurde, bevor Sie die WebSphere Partner Gateway-Komponentenserver starten.
4. Wählen Sie den Server `bcgserver` aus und klicken Sie auf **Starten**.

5. Wiederholen Sie Schritt 4, um alle erforderlichen Komponentenserver zu starten. Ein Cluster kann mehrere Server enthalten. Sie können beliebige Server im Cluster auswählen und diese starten.

Server starten, wenn Deployment Manager nicht verfügbar ist

Falls der Deployment Manager zwischenzeitlich nicht verfügbar ist, können Sie den Nachrichtenserver `bcgmas` und den Server `bcgserver` folgendermaßen manuell starten:

1. Vergewissern Sie sich, dass die Knotenagenten auf sämtlichen Knoten aktiv sind, auf denen die Server `bcgmas` und `bcgserver` installiert sind.
2. Starten Sie jeden einzelnen WebSphere Partner Gateway-Server, indem Sie das Script `startServer` ausführen, das sich im Verzeichnis *<WebSphere_installationsverzeichnis>*`/wasND/Profiles/bcgprofile/bin` auf dem Computer befindet, auf dem der Server installiert wurde.

   Die Syntax für das Starten des Nachrichtenservers, der Konsole, des Empfängers oder Document Manager für die Komponentenserver lautet:

   ```
   startServer <servername>
   ```

   Dabei steht *servername* für `bcgmas`, wenn der Nachrichtenserver gestartet werden soll, und für `bcgserver`, wenn die Komponentenserver gestartet werden sollen.

Server in einem System mit einfachem verteiltem Modus stoppen

Wenn Sie Server in einem System mit einfachem verteiltem Modus stoppen, müssen Sie die WebSphere Partner Gateway-Komponentenserver noch vor den Nachrichtenservern stoppen.

Alle Server mit Deployment Manager stoppen

1. Wählen Sie den Cluster `bcgserverCluster` aus und klicken Sie auf **Stoppen**. Warten Sie, bis der Cluster gestoppt wurde, bevor Sie den nächsten Schritt ausführen.
2. Wählen Sie den Nachrichtencluster `bcgmasCluster` aus und klicken Sie auf **Stoppen**.

Einzelne Server auf allen Computern stoppen

Wenn Sie nicht sämtliche Server in allen Clustern stoppen möchten, können Sie die Server nur auf den Computern stoppen, auf denen sie installiert sind. Führen Sie die folgenden Schritte aus, um die Server auf allen Computern zu stoppen:

1. Wählen Sie den zu stoppenden Server `bcgserver` aus und klicken Sie auf **Stoppen**.
2. Wiederholen Sie den vorherigen Schritt, bis Sie alle gewünschten Server gestoppt haben. Warten Sie, bis die Server gestoppt wurden, bevor Sie den nächsten Schritt ausführen.
3. Wählen Sie den zu stoppenden Nachrichtenserver `bcgmas` aus und klicken Sie auf **Stoppen**.
4. Wiederholen Sie den vorherigen Schritt, bis Sie alle Server gestoppt haben. Falls einer der `bcgserver`-Server noch aktiv ist, lassen Sie zumindest einen der `bcgmas`-Server ebenfalls aktiv.

Server stoppen, wenn Deployment Manager nicht verfügbar ist

Stoppen Sie zunächst die bcgserver-Server vor den bcgmas-Nachrichtenservern.

1. Vergewissern Sie sich, dass die Knotenagenten auf sämtlichen Knoten aktiv sind, auf denen die Server bcgmas und bcgserver installiert sind.
2. Stoppen Sie jeden einzelnen WebSphere Partner Gateway-Server, indem Sie das Script stopServer ausführen, das sich im Verzeichnis *<WebSphere_Partner_Gateway_installationsverzeichnis>*/wasND/Profiles/bcgprofile/bin auf dem Computer befindet, auf dem der Server installiert ist.

   Die Syntax zum Stoppen des Nachrichtenservers oder zum Stoppen der Komponentenserver für 'bcgserver' lautet:

   ```
   stopServer <servername>
   ```

   Dabei steht *servername* für bcgmas, wenn der Nachrichtenserver gestoppt werden soll, und für bcgserver, wenn die Komponentenserver gestoppt werden sollen.

Komponenten in einem System mit vollständigem verteiltem Modus starten und stoppen

Vorbemerkung: Beachten Sie, dass es im System mit vollständigem verteiltem Modus vier Cluster gibt. Diese sind:

- bcgmasCluster

  Der Cluster für den Nachrichtenaustausch, in dem die Nachrichtenserver mit dem Namen bcgmas enthalten sind. Mindestens ein Nachrichtenserver muss aktiv sein, damit die WebSphere Partner Gateway-Komponenten betrieben werden können.
- bcgconsoleCluster

  Der Cluster für die WebSphere Partner Gateway-Konsolenkomponenten, zu dem die Server mit dem Namen bcgconsole gehören.
- bcgreceiverCluster

  Der Cluster für die WebSphere Partner Gateway-Empfängerkomponenten, zu dem die Server mit dem Namen bcgreceiver gehören.
- bcgdocmgrCluster

  Der Cluster für die Document Manager-Komponenten von WebSphere Partner Gateway, zu dem die Server mit dem Namen bcgdocmgr gehören.

Die hier verwendeten Namen sind die bei der Installation verwendeten Standardnamen. Beachten Sie, dass das Installationsprogramm während der Installation auch andere Namen ausgewählt haben kann und Sie dann diese Namen (anstelle der Standardnamen) verwenden müssen.

Server in einem System mit vollständigem verteiltem Modus starten

Wenn Sie Ihre Server in einem System mit vollständigem verteiltem Modus starten möchten, lautet die Startreihenfolge wie folgt:

1. Nachrichtenserver
2. Document Manager-Server von WebSphere Partner Gateway
3. Empfängerserver (oder Konsolenserver) von WebSphere Partner Gateway
4. Konsolenserver (oder Empfängerserver) von WebSphere Partner Gateway

Anmerkung: Sie können wählen, ob Sie zunächst die Empfängerserver oder die Konsolenserver starten möchten.

Alle Server mit Deployment Manager starten

1. Wählen Sie den Nachrichtencluster `bcgmasCluster` aus und klicken Sie auf **Starten**.

   Anmerkung: Warten Sie, bis der Cluster gestartet wurde, bevor Sie die WebSphere Partner Gateway-Komponentencluster starten.
2. Wählen Sie den Cluster `bcgdocmgrCluster` aus und klicken Sie auf **Starten**.
3. Wählen Sie den Cluster `bcgreceiverCluster` (oder den Cluster `bcgconsoleCluster`) aus und klicken Sie auf **Starten**.
4. Wählen Sie den Cluster `bcgconsoleCluster` (oder den Cluster `bcgreceiverCluster`) aus und klicken Sie auf **Starten**.

Einzelne Server auf allen Computern starten

1. Wählen Sie den zu startenden Nachrichtenserver `bcgmas` aus und klicken Sie auf **Starten**.

   Anmerkung: Warten Sie, bis mindestens einer der Server gestartet wurde, bevor Sie die WebSphere Partner Gateway-Komponentenserver starten.
2. Wiederholen Sie den vorherigen Schritt, bis Sie alle Server gestartet haben.
3. Wählen Sie den zu startenden Server `bcgdocmgr` aus und klicken Sie auf **Starten**.
4. Wiederholen Sie den vorherigen Schritt, bis Sie alle Server gestartet haben.
5. Wählen Sie den zu startenden Server `bcgreceiver` (oder den Server `bcgconsole`) aus und klicken Sie auf **Starten**.
6. Wiederholen Sie den vorherigen Schritt, bis Sie alle Server gestartet haben.
7. Wählen Sie den zu startenden Server `bcgconsole` (oder den Server `bcgreceiver`) aus und klicken Sie auf **Starten**.
8. Wiederholen Sie den vorherigen Schritt, bis Sie alle Server gestartet haben.

Anmerkung: Sollen mehrere Server gestartet werden, wählen Sie diese Server aus und klicken Sie auf **Starten**.

Server starten, wenn Deployment Manager nicht verfügbar ist

Anmerkung: Starten Sie die Server in der im vorherigen Abschnitt genannten Reihenfolge.

1. Vergewissern Sie sich, dass auf allen Knoten, auf denen die Server `bcgmas` und etwaige WebSphere Partner Gateway-Komponentenserver installiert sind, auch die Knotenagenten aktiv sind.
2. Starten Sie jeden einzelnen WebSphere Partner Gateway-Server, indem Sie das Script `startServer` ausführen, das sich im Verzeichnis *<WebSphere_Partner_Gateway_installationsverzeichnis>*`/wasND/Profiles/bcgprofile/bin` auf dem Computer befindet, auf dem der Server installiert wurde. Die Syntax lautet:

   `startServer <`*`servername`*`>`

   Dabei steht *servername* für `bcgmas`, wenn der Nachrichtenserver gestartet werden soll, und für `bcgconsole`, `bcgreceiver` und `bcgdocmgr`, wenn die Komponentenserver gesartet werden sollen.

Anmerkung: Starten Sie zuerst den Server "bcgmas" und anschließend die übrigen Server.

Anmerkung: Stellen sie sicher, dass der Benutzer, den Sie zum Starten und Stoppen des Servers verwenden, ein WPG-Benutzer und nicht der Rootbenutzer ist.

Server in einem System mit vollständigem verteiltem Modus stoppen

Beachten Sie, dass die Beendigungsreihenfolge genau umgekehrt verläuft, wie die Startreihenfolge. Gehen Sie beim Stoppen wie folgt vor:

1. Konsolen- oder Empfängerserver von WebSphere Partner Gateway.
2. Empfänger- oder Konsolenserver von WebSphere Partner Gateway.

   Anmerkung: Sie können wählen, ob Sie zuerst die Empfängerserver oder die Konsolenserver stoppen möchten.
3. Document Manager-Server von WebSphere Partner Gateway.
4. Nachrichtenserver.

Alle Server mit Deployment Manager stoppen

1. Wählen Sie den Cluster `bcgconsoleCluster` (oder den Cluster `bcgreceiverCluster`) aus und klicken Sie auf **Stoppen**.
2. Wählen Sie den Cluster `bcgreceiverCluster` (oder den Cluster `bcgconsoleCluster`) aus und klicken Sie auf **Stoppen**.
3. Wählen Sie den Cluster `bcgdocmgrCluster` aus und klicken Sie auf **Stoppen**.

   Anmerkung: Warten Sie, bis der Cluster gestoppt wurde, bevor Sie den Nachrichtencluster stoppen.
4. Wählen Sie den Nachrichtencluster `bcgmasCluster` aus und klicken Sie auf **Stoppen**.

Einzelne Server auf allen Computern gleichzeitig stoppen

Wenn Sie nicht sämtliche Server in allen Clustern stoppen möchten, können Sie die Server nur auf den Computern stoppen, auf denen sie installiert sind. Führen Sie die folgenden Schritte aus, um einen Server dort zu stoppen, wo er installiert ist:

1. Wählen Sie den Server `bcgconsole` (oder den Server `bcgreceiver`) aus und klicken Sie auf **Stoppen**.
2. Wiederholen Sie den vorherigen Schritt, bis Sie alle gewünschten Server gestoppt haben.
3. Wählen Sie den Server `bcgreceiver` (oder den Server `bcgconsole`) aus und klicken Sie auf **Stoppen**.
4. Wiederholen Sie den vorherigen Schritt, bis Sie alle gewünschten Server gestoppt haben.
5. Wählen Sie den zu stoppenden Server `bcgdocmgr` aus und klicken Sie auf **Stoppen**.
6. Wiederholen Sie den vorherigen Schritt, bis Sie alle gewünschten Server gestoppt haben.
7. Warten Sie, bis die Server gestoppt wurden, bevor Sie die Nachrichtenserver stoppen.
8. Wählen Sie den zu stoppenden Nachrichtenserver `bcgmas` aus und klicken Sie auf **Stoppen**.

9. Wiederholen Sie den vorherigen Schritt, bis Sie alle Server gestoppt haben.

Anmerkung: Falls einige der WebSphere Partner Gateway-Komponentenserver noch aktiv sind, lassen Sie zumindest einen der bcgmas-Server ebenfalls aktiv.

Server stoppen, wenn Deployment Manager nicht verfügbar ist

Beachten Sie, dass Sie die WebSphere Partner Gateway-Server vor den Nachrichtenservern bcgmas stoppen müssen.

1. Vergewissern Sie sich, dass auf allen Knoten, auf denen die Server bcgmas und etwaige WebSphere Partner Gateway-Komponentenserver installiert sind, auch die Knotenagenten aktiv sein müssen.
2. Stoppen Sie jeden einzelnen WebSphere Partner Gateway-Server, indem Sie das Script stopServer ausführen, das sich im Verzeichnis *<WebSphere_Partner_Gateway_installationsverzeichnis>*/wasND/Profiles/bcgprofile/bin auf dem Computer befindet, auf dem der Server installiert ist. Die Syntax lautet:

   ```
   stopServer <servername>
   ```

   Dabei steht *servername* für bcgmas, wenn der Nachrichtenserver gestoppt werden soll, und für bcgconsole, bcgreceiver und bcgdocmgr, wenn die Komponentenserver gestoppt werden sollen.

Kapitel 3. Grundlegende Community Console-Tasks

Die im vorliegenden Handbuch beschriebenen Tasks werden mit der Community Console von WebSphere Partner Gateway ausgeführt. Die Community Console ist eine Webanwendung, die einen sicheren Zugriffspunkt bietet und über einen Web-Browser zugänglich ist.

In diesem Kapitel werden die folgenden Themen behandelt:

An der Community Console anmelden

Für die Community Console sind unterstützte Web-Browser erforderlich. Weitere Informationen zu den unterstützten Browserversionen für WebSphere Partner Gateway 6.2.1 finden Sie unter der folgenden Adresse: http://www-01.ibm.com/support/docview.wss?rs=2311&uid=swg27020525.

Stellen Sie sicher, dass Sie die neusten verfügbaren Service-Packs und Updates für Ihren Browser installiert haben.

Anmerkung: Für die Community Console muss die Cookie-Unterstützung eingeschaltet werden, um die Sitzungsdaten zu verwalten. Es werden keine persönlichen Informationen in dem Cookie gespeichert, der verfällt, sobald der Browser geschlossen wird.

Verwenden Sie für eine optimale Anzeige mindestens die Bildschirmauflösung 1024 x 768.

Führen Sie die folgenden Schritte aus, um sich an der Community Console anzumelden:

1. Geben Sie im Adressfeld eines beliebigen Web-Browsers die folgende URL ein:

   `http://`*`hostname.domäne`*`:58080/console`
   `(nicht gesichert)`

   `https://`*`hostname.domäne`*`:58443/console (sicher)`

   Dabei sind *`hostname`* und *`domäne`* der Name und die Adresse des Computers, auf dem sich die Komponente Community Console befindet.
2. Geben Sie im Anmeldefenster der Community Console im Feld **Benutzername** den korrekten Namen an:
   - Der Standardbenutzername für den Hubadministrator lautet `Hubadmin`.
   - Der Standardbenutzername für den Operatoradministrator lautet `Admin`.
3. Geben Sie im Feld **Kennwort** das Kennwort für Ihre Site an. Das Standardkennwort ist `Pa55word`.
4. Geben Sie im Feld **Anmeldename des Unternehmens** den Admin-Anmeldenamen an. Der Standardanmeldename ist sowohl für den Benutzer "Hubadmin" als auch für den Benutzer "Operatoradministrator" `Operator`.

Anmerkung: Falls Benutzer-IDs und Kennwörter zentral über LDAP verwaltet werden (Lightweight Directory Access Protocol), wird das Feld **Anmeldename des Unternehmens** nicht angezeigt. Weitere Informationen zu LDAP finden Sie im Abschnitt Kapitel 7, „LDAP-Unterstützung für Authentifizierung der Anmeldung", auf Seite 85.

5. Klicken Sie auf **Anmelden**.
6. Wenn Sie sich zum ersten Mal anmelden, fordert das System Sie auf, ein neues Kennwort zu erstellen. Geben Sie ein neues Kennwort an, welches Sie dann im Feld **Bestätigen** erneut angeben.
7. Klicken Sie auf **Speichern**.

Anmerkung: Wenn Sie im Firefox-Browser den auf der Anmeldeseite verwendeten Benutzernamen und das Kennwort speichern, werden der Benutzername und das Kennwort in Benutzernazeigen, auf denen Felder für diese Werte vorhanden sind, automatisch ausgefüllt. Dieses Verhalten ist unabhängig davon, ob es sich um eine Anmeldeseite handelt. Auf der Seite zum Erstellen eines Benutzers wird beispielsweise das Feld für das Fax vorab mit den Werten für das Kennwort und den Benutzernamen gefüllt.

Durch die Community Console navigieren

Die Community Console enthält zahlreiche Menüs, über die Sie WebSphere Partner Gateway konfigurieren können.

Die folgenden beiden Links werden jeweils in der rechten oberen Ecke aller Fenster angezeigt:

- **Abmelden**

  Damit melden Sie sich von der aktuellen WebSphere Partner Gateway-Sitzung ab. Die Anwendung wird weiterhin auf dem Server ausgeführt. Führen Sie die Schritte wie in „ An der Community Console anmelden" auf Seite 17 beschrieben aus, um sich erneut anzumelden.
- **Hilfe**

  Öffnet die Onlinehilfe für WebSphere Partner Gateway.

  Anmerkung: Wird kein Hilfefenster angezeigt, nachdem Sie auf **Hilfe** geklickt haben, sollten Sie überprüfen, ob eventuell ein Programm zum Blockieren von Popup-Fenstern ausgeführt wird.

Symbole der Community Console

Tabelle 2 listet die Symbole auf, die in den Fenstern der Community Console verwendet werden.

Tabelle 2. Community Console-Symbole

Symbol	Name des Symbols
	Ausblenden
	Kopieren
	Daten enthalten
	Aktivieren

Tabelle 2. Community Console-Symbole (Forts.)

Symbol	Name des Symbols
	Löschen
	Ziel inaktiviert
	Unformatiertes Dokument anzeigen
	Dokument wird verarbeitet
	Dokumentverarbeitung fehlgeschlagen
	Dokumentverarbeitung erfolgreich
	Zuordnung herunterladen
	Bearbeiten
	Attributwerte bearbeiten
	Bearbeiten ausschalten
	RosettaNet-Attributwerte bearbeiten
	Erweitern
	Informationen exportieren
	Bericht exportieren
	Suchkriterien ausblenden
	Ändern
	Keine Daten enthalten
	Kalender öffnen
	Falsche Reihenfolge
	Anhalten
	Drucken
	Erforderliche Eingabe
	Rolle; Zum Erstellen hier klicken
	Starten
	Stopp übergeben
	Synchroner Datenfluss. Für asynchrone Transaktionen wird kein Symbol angezeigt
	Zuordnung hochladen

Tabelle 2. Community Console-Symbole (Forts.)

Symbol	Name des Symbols
	Ein zuvor gesendetes Dokument anzeigen, wenn ein Ereignis **Doppeltes Dokument** auftritt
	Details anzeigen
	Gruppenzugehörigkeiten anzeigen
	Hilfefunktion anzeigen **Anmerkung:** Das Symbol **Hilfe** wird übersetzt, wenn die Konsole mit einer der von IBM unterstützten Sprachlocales verwendet wird.
	Berechtigungen anzeigen
	Attributkonfiguration für die Dokumentdefinition anzeigen
	Benutzer anzeigen
	Validierungsfehler anzeigen
	Verwendet von

Von der Community Console abmelden

Wenn Sie Ihre Arbeit in der Community Console beendet haben, können Sie oben rechts in allen Community Console-Fenstern auf **Abmelden** klicken. Daraufhin werden Sie vom System abgemeldet und gelangen wieder zurück zum Community Console-Anmeldefenster.

Kapitel 4. Hubverwaltungstasks

In diesem Kapitel werden die Tasks beschrieben, die ausschließlich der Hubadministrator (Hubadmin) ausführen kann. Hierbei handelt es sich um die folgenden Tasks:

Kennwortrichtlinie verwalten

Sie können eine Kennwortrichtlinie für die Hub-Community definieren, wenn Sie andere Werte verwenden möchten, als jene, die vom System standardmäßig vorgegeben werden. Die Kennwortrichtlinie gilt für alle Benutzer, die sich an der Community Console anmelden.

Sie können die folgenden Elemente der Kennwortrichtlinie ändern:

- Mindestlänge - Gibt die Mindestzeichenanzahl an, die der Partner für das Kennwort verwenden muss. Der Standardwert ist 8 Zeichen.
- Ablaufzeit - Gibt die Anzahl von Tagen an, bis das Kennwort verfällt. Der Standardwert ist 30 Tage.
- Eindeutigkeit - Gibt die Anzahl von Kennwörtern an, die in einer Protokolldatei enthalten sein müssen. Ein Partner kann ein altes Kennwort nicht mehr verwenden, wenn es in der Protokolldatei vorhanden ist. Der Standardwert ist 10 Kennwörter.
- Sonderzeichen - Wenn dies ausgewählt ist, müssen die Kennwörter mindestens drei der folgenden Sonderzeichentypen enthalten:
  - Großbuchstaben
  - Kleinbuchstaben

– Numerische Zeichen
– Sonderzeichen

Mit dieser Einstellung können Sie strengere Sicherheitsanforderungen vorgeben, wenn Kennwörter verwendet werden, die aus dem einfachen ASCII-Zeichensatz (ohne Umlaute) bestehen. Die Standardeinstellung ist "Off". Es wird empfohlen, dass die Option für die Sonderzeichen ausgeschaltet (Off) bleibt, wenn die Kennwörter aus internationalen Zeichensätzen bestehen. Andere Zeichensätze enthalten möglicherweise nicht die erforderlichen drei der vier Zeichentypen.

Das System unterstützt die folgenden Sonderzeichen: '#', '@', '$', '&' und '+'.

- Prüfung auf Namensvariationen - Wenn Sie diese Option auswählen, können keine Kennwörter verwendet werden, die eine leicht zu erratende Variante des Anmeldenamens oder des vollständigen Namens des Benutzers sind. Dieses Feld ist standardmäßig ausgewählt.

Gehen Sie wie folgt vor, um die Standardwerte zu ändern:

1. Klicken Sie auf **Hubadmin** > **Konsolkonfiguration** > **Kennwortrichtlinie**. Die Seite **Kennwortrichtlinie** wird angezeigt.
2. Klicken Sie auf **Bearbeiten**.
3. Ändern Sie beliebig viele Standardwerte in die Werte, die Sie für Ihre Kennwortrichtlinie verwenden möchten.
4. Klicken Sie auf **Speichern**.

Datenbankkonnektivität, Datenbankbenutzer und Kennwort ändern

Nach der Installation können Sie die Datenbank der WebSphere Partner Gateway-Komponenten ändern. Sie können außerdem den Namen und das Kennwort des Datenbankbenutzers ändern.

Darüber hinaus haben Sie die Möglichkeit, die Konnektivitätseigenschaften der Datenbank zu ändern, indem Sie die Datenquellen ändern. Die Datenquellen werden in WebSphere Application Server für die Verwendung durch die Komponentenanwendungen konfiguriert. Verwenden Sie die Administrationskonsole von WebSphere Application Server, um die Datenquellen zu ändern.

Führen Sie die folgenden Schritte aus, um die von den Komponenten verwendeten Datenbankverbindungen zu konfigurieren:

1. Zeigen Sie die Administrationskonsole über einen Browser an.
2. Klicken Sie im linken Fensterbereich der Konsole auf **Ressourcen** > **JDBC** > **Datenquellen**.
3. Suchen Sie die Datenquellen, die Sie ändern möchten. Wählen Sie unter den JNDI-Namen der verfügbaren Quellen den Namen, den Sie ändern möchten, anhand des Knotens und des Servernamens aus.
4. Klicken Sie auf den Datenquellennamen, um den Datenbanknamen, den Host und die Portnummer anzuzeigen und zu ändern.
5. Klicken Sie auf **JAAS - J2C-Authentifizierungsdaten** und wählen Sie anschließend einen Aliasnamen, um die Benutzer-ID und das Kennwort, die bzw. das für die Verbindung zur Datenbank verwendet wird, anzuzeigen und zu ändern.
6. Klicken Sie auf **OK**, damit die Änderungen wirksam werden und anschließend auf **Speichern**, um die Änderungen zu speichern.

Ereigniscodes verwalten

Für wichtige Aktivitäten oder Informationen in WebSphere Partner Gateway wird ein Ereignis protokolliert. Eine Reihe vordefinierter Ereignisse mit bestimmten Ereigniscodes wird bereitgestellt. Klicken Sie auf **Hubadmin > Hubkonfiguration > Ereigniscodes**, um die Ereigniscodes anzuzeigen. Sie können die Ereigniscodes in andere Anwendungen exportieren oder den Alertstatus des Ereigniscodes festlegen. Darüber hinaus können Sie auch definieren, ob ein Alertcode alertfähig ist.

Ereigniscodes anzeigen und bearbeiten

Die folgende Prozedur beschreibt, wie Sie die Details eines Ereigniscodes anzeigen. Sie können die Sichtbarkeit und den Alertstatus des Ereigniscodes bearbeiten und seinen Schweregrad anzeigen.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Ereigniscodes**.
2. Klicken Sie im Fenster **Ereigniscodes** neben dem Ereigniscode, dessen Details Sie anzeigen möchten, auf das Symbol **Details anzeigen**.
3. Richten Sie im Fenster **Ereigniscodedetails** die Parameter ein, die in Tabelle 3 beschrieben werden:

Tabelle 3. Ereigniscodedetails

Parameter	Beschreibung
Ereigniscode	Ein Anzeigefeld, das die eindeutige Nummer dieses Ereigniscodes anzeigt.
Ereignisname	Ein Anzeigefeld, das den Namen enthält, mit dem das Ereignis mit Bezug auf die Aktion, durch die das Ereignis ausgelöst wurde, identifiziert wird.
Interne Beschreibung	Ein Anzeigefeld, das die Umstände beschreibt, die das Ereignis ausgelöst haben.
Sichtbarkeit	Wählen Sie die Benutzer aus, die den Ereigniscode anzeigen können: Hub-Administrator, interner Partner, Partner oder eine Kombination dieser drei Benutzertypen.

Tabelle 3. Ereigniscodedetails (Forts.)

Parameter	Beschreibung
Wertigkeit	Ein Anzeigefeld, das den Schweregrad anzeigt, der diesem Ereigniscode zugeordnet ist, von "Debugging" (weniger schwerwiegend) bis "Kritisch" (sehr schwerwiegend): **Debugging** Für Systembetrieb und Unterstützung auf der unteren Ebene. Sichtbarkeit und die Verwendung der Debuginformationen hängen von der Berechtigungsebene des Benutzers ab. **Information** Bei erfolgreichem Systembetrieb. Diese Ereignisse geben außerdem den Status des Dokuments wieder, das verarbeitet wird. Informationsereignisse erfordern keine Benutzeraktion. **Warnung** Bei nicht kritischen Unregelmäßigkeiten in der Dokumentverarbeitung oder in Systemfunktionen, bei denen der Betrieb trotzdem weiter läuft. **Fehler** Bei Unregelmäßigkeiten in der Dokumentverarbeitung, durch die das Ende des Prozesses verursacht wird. **Kritisch** Für Services, die aufgrund eines Systemausfalls beendet werden. Kritische Ereignisse erfordern das Eingreifen der Benutzerunterstützung.
Alertfähig	Wählen Sie die Option "Alertfähig" aus, um einen Ereignisalert zu erstellen. Dadurch wird der Ereignisname in der Liste auf der Registerkarte **Definieren** des Alertfensters angezeigt.

Ereigniscodenamen exportieren

Sie können auswählen, ob nur die Ereignisnamen in der Ereignisliste (**Namen exportieren**) oder die internen Beschreibungen in der Ereignisliste (**Liste exportieren**) im Textformat gespeichert werden sollen. Führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Ereigniscodes**.
2. Klicken Sie im Fenster **Ereigniscodes** auf **Namen exportieren**, um die Liste der Ereignisse nur mit den Ereignisnamen zu speichern. Klicken Sie alternativ auf **Liste exportieren**, um die Liste der Ereignisse nur mit deren internen Beschreibungen zu speichern.

Ereignisse angeben, für die Benachrichtigungen ausgegeben werden können

Für wichtige Aktivitäten oder Informationen in WebSphere Partner Gateway wird ein Ereignis protokolliert. Eine Reihe vordefinierter Ereignisse mit bestimmten Ereigniscodes wird bereitgestellt. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Ereigniscodes**, um die Ereigniscodes anzuzeigen. Wenn ein Ereignis als "alertfähig" festgelegt wurde, wird das Ereignis auf der Seite **Alerts** in der Liste **Ereignisname** angezeigt. Sie können dann einen Alert für das Ereignis festlegen.

Gehen Sie wie folgt vor, um Ereignisse als alertfähig zu definieren:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Ereigniscodes**.

Die Seite **Ereigniscodes** wird angezeigt.

2. Gehen Sie wie folgt vor, um die Alerts für das Ereignis zu aktivieren:
   - Klicken Sie neben dem Ereigniscode auf das Symbol **Details anzeigen**. Die Seite **Ereigniscodedetails** wird angezeigt.
   - Wählen Sie **Alertfähig** aus.

Dokumentvalidierungsfehler

Gehen Sie wie folgt vor, um Dokumentvalidierungsfehler anzuzeigen: Klicken Sie auf der Seite **Dokumentdetails**, Registerkarte **Dokumentanzeige**, auf das Symbol **Dokumente anzeigen**. Weitere Informationen zu Dokumentvalidierungsfehlern finden Sie im Abschnitt „Dokumentvalidierungsfehler" auf Seite 127.

Empfänger verwalten

Das Fenster **Empfängerliste** wird verwendet, um die Details vorhandener Empfänger anzuzeigen und zu bearbeiten, sowie Empfänger zu aktivieren, zu inaktivieren oder zu löschen.

Empfängerdetails anzeigen und bearbeiten

Die folgende Prozedur beschreibt, wie Sie die Details eines Empfängers anzeigen. Als Teil dieser Prozedur können Sie die Parameter des Empfängers bearbeiten.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Empfänger**.
2. Klicken Sie im Fenster **Empfängerliste** auf das Symbol **Details anzeigen** neben dem Empfänger, dessen Details Sie anzeigen möchten. In der Community Console wird das Fenster **Empfängerdetails** angezeigt.
3. Klicken Sie im Fenster **Empfängerdetails** auf das Symbol **Bearbeiten**.
4. Bearbeiten Sie die Parameter nach Bedarf.
5. Klicken Sie auf **Speichern**.

Empfänger aktivieren oder inaktivieren

Sie können Empfänger im Fenster **Empfängerliste** jeweils **Aktivieren** oder **Inaktivieren**, indem Sie auf die entsprechende Option in der Spalte **Status** klicken. Der Empfänger kann auch mit den folgenden Schritten aktiviert oder inaktiviert werden:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Empfänger**.
2. Klicken Sie im Fenster **Empfängerliste** auf das Symbol **Details anzeigen**, um die Details des Empfängers anzuzeigen.
3. Klicken Sie auf das Symbol **Bearbeiten**, um die Parameter des Empfängers zu bearbeiten.
4. Wählen Sie im Statusfeld die Option **Aktiviert** oder **Inaktiviert** aus, um den Status des Empfängers zu ändern.
5. Klicken Sie auf **Speichern**, um die Änderungen zu speichern.

Empfänger löschen

Sie können Empfänger löschen, die Sie nicht verwenden möchten.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Empfänger**.

2. Klicken Sie im Fenster **Empfängerliste** auf das Symbol **Löschen** neben dem Empfänger, den Sie löschen möchten.

   Anmerkung: Ein Fenster zum Bestätigen des Löschens wird geöffnet. Nachdem Sie die Aktion bestätigen, wird der ausgewählte Server gelöscht.

Synchrones Zeitlimit des HTTP-Ziels lokal definieren

WebSphere Partner Gateway ermöglicht Ihnen, ein lokal definiertes synchrones Zeitlimit und synchrone Verbindungen für jeden HTTP-Empfänger zu verwenden. Der Wert für die synchrone Verbindung darf das für den Container zulässige TCP-Verbindungslimit nicht überschreiten. Nur die maximalen synchronen Verbindungen pro Empfänger werden in der Obermenge des Limits für den Container gesteuert. Der Webcontainer (WebSphere Application Server) wird separat über die verwaltete Anwendung konfiguriert, um die Anzahl der HTTP-Verbindungen zuzulassen oder einzuschränken. Gehen Sie wie folgt vor, um die Werte für **Max. synchrones Zeitlimit** und **Max. synchrone Verbindungen** zu ändern:

1. Navigieren Sie durch die Auswahl von **Hubadministrator > Empfänger** zur Seite für die Erstellung eines Empfängers.
2. Klicken Sie auf das Symbol **Bearbeiten** für den gewünschten HTTP-Empfänger.
3. Modifizieren Sie die Werte für **Max. synchrones Zeitlimit** und **Max. synchrone Verbindungen**.

Anmerkung: Für **Max. synchrones Zeitlimit** dürfen keine negativen Werte eingegeben werden. Wenn Sie den Wert Null für **Max. synchrone Verbindungen** eingeben, wird die Einschränkung **Max. synchrone Verbindungen** für alle Empfänger entfernt.

Interaktionen und Dokumentdefinitionen verwalten

Führen Sie die folgenden Schritte aus, um Interaktionen zwischen zwei Dokumentdefinitionen zu aktivieren, zu inaktivieren oder zu bearbeiten:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.
3. Geben Sie die Suchkriterien an, die WebSphere Partner Gateway verwenden soll, um die Interaktion zu suchen, die Sie aktivieren, inaktivieren oder bearbeiten möchten.
4. Klicken Sie auf **Suchen**. Das System sucht nach allen Interaktionen, die Ihren Suchkriterien entsprechen.
5. Klicken Sie zum Aktivieren einer Interaktion auf das Symbol **Aktivieren** neben der Interaktion, die aktiviert werden soll. Klicken Sie auf **OK**, um die Aktion zu bestätigen. WebSphere Partner Gateway ersetzt das Symbol **Aktivieren** durch das Symbol **Inaktivieren**. Hierdurch wird angezeigt, dass die Interaktion aktiviert ist.
6. Klicken Sie zum Inaktivieren einer Interaktion auf das Symbol **Inaktivierte Standarddefinition** neben der Interaktion. Klicken Sie auf **OK**, um die Aktion zu bestätigen. WebSphere Partner Gateway ersetzt das Symbol **Inaktivierte Standarddefinition** durch das Symbol **Aktivierte Standarddefinition**. Hierdurch wird angezeigt, dass die Interaktion inaktiviert ist.
7. Klicken Sie zum Bearbeiten einer Interaktion auf das Symbol **Bearbeiten** neben der betreffenden Interaktion. Bearbeiten Sie die Interaktion im Fenster **Bearbeiten** und klicken Sie anschließend auf **Speichern**.

Führen Sie die folgenden Schritte aus, um anzuzeigen, wo eine Interaktion verwendet wird:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.
3. Geben Sie Suchkriterien an, die WebSphere Partner Gateway verwenden soll, um die anzuzeigende Interaktion zu suchen.
4. Klicken Sie auf **Suchen**. Das System sucht nach allen Interaktionen, die Ihren Suchkriterien entsprechen.
5. Klicken Sie auf das Symbol **Verwendet von**. Alle Verbindungen, in denen diese Interaktion verwendet wird, werden angezeigt. Auf jeder Seite werden Informationen für höchstens 10 Verbindungen für die jeweilige Interaktion angezeigt.

Gehen Sie wie folgt vor, um eine Interaktion zu löschen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
2. Klicken Sie auf **Interaktionen verwalten**.
3. Geben Sie Suchkriterien an, die WebSphere Partner Gateway verwenden soll, um die zu löschende Interaktion zu suchen.
4. Klicken Sie auf **Suchen**. Das System sucht nach allen Interaktionen, die Ihren Suchkriterien entsprechen.
5. Klicken Sie auf das Symbol **Löschen**. Wird die Interaktion von einem der Kanäle verwendet, wird eine Warnung angezeigt.
6. Klicken Sie auf **OK**, um die Interaktion zusammen mit den zugehörigen Kanälen zu löschen.

Führen Sie die folgenden Schritte aus, um zu ermitteln, wo eine Dokumentdefinition verwendet wird:

Über das Symbol **Verwendet von** können Informationen dazu angezeigt werden, wo die ausgewählte Dokumentdefinition verwendet wird.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
2. Klicken Sie auf das Symbol **Verwendet von** für die Dokumentdefinition, für die Informationen angezeigt werden sollen. Hierdurch werden alle Interaktionen und B2B-Funktionalitäten aufgelistet, in denen diese Dokumentdefinition verwendet wird.

Führen Sie die folgenden Schritte aus, um eine Dokumentdefinition zu löschen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
2. Klicken Sie auf das Symbol **Löschen** für die Dokumentdefinition, die gelöscht werden soll. Eine Warnung wird nur angezeigt, wenn die Dokumentdefinition von einer Interaktion oder B2B-Funktionalität verwendet wird.
3. Klicken Sie im Fenster mit der Warnung auf **OK**. Hierdurch werden die zugehörigen Kanäle, Interaktionen und B2B-Funktionalitäten aller Partner sowie alle zugehörigen Attribute für die Dokumentdefinition gelöscht.
4. Klicken Sie im Warnfenster auf **Abbrechen**, um das Löschen abzubrechen.

XML-Formate verwalten

Über das Fenster `XML-Formate verwalten` können Sie auf die im System vorhandenen XML-Formate zugreifen. XML-Formate werden unter Verwendung von XML-Dokumentfamilien verwaltet. XML-Dokumentfamilien können über die Community Console hinzugefügt, gelöscht und geändert werden. Außerdem können für jede

Familie die XML-Formate innerhalb einer Dokumentfamilie hinzugefügt, gelöscht und geändert werden. Innerhalb einer Familie können auch Formate kopiert und von Familie zu Familie versetzt werden.

Vollständige Informationen zum Erstellen von XML-Dokumentfamilien und XML-Formaten finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Unterstützung für große Dateien

WebSphere Partner Gateway kann in Formaten Ausdrücke von XPath (Version 1.0) verwenden. Die Verarbeitungsleistung der XPath-Unterstützung begrenzt die Größe der Dateien, die mit vollständigen XPath-XML-Formaten verwendet werden können. Damit auch große Dateien verarbeitet werden können, müssen Sie bei der Definition der Dokumentfamilie die Option für die Verarbeitung großer Dateien festlegen.

Die Liste **Option für große Datei** enthält die folgenden Optionen:

- Keine.
- Prozessor für große Dateien verwenden.
- Namespace-abhängigen Prozessor für große Dateien verwenden.

Wählen Sie eine der Optionen für große Dateien aus, wenn Sie XML-Formate für große Dokumente schreiben, die nicht mit dem vollständigen XPath-Prozessor verarbeitet werden können. Die Option für namespace-abhängige Prozessoren legt fest, dass die Elementpfade Namespacepräfixe enthalten sollen, wenn sie in einem Dokument angezeigt werden.

Anmerkung: Sobald die Familie erstellt ist, kann diese Option nicht mehr geändert werden. Der Grund dafür ist, dass die Dokumentfamilie möglicherweise bereits XML-Formate enthält, die durch das Ändern des Familientyps nicht mehr korrekt sind.

Für Formate in einer Familie, in der die Option für die Verarbeitung großer Dateien ausgewählt wurde, ist die XPath-Verarbeitungsleistung begrenzt. Wenn die Option für die Verarbeitung großer Dateien für eine Dokumentfamilie verwendet wird, gelten die folgenden Begrenzungen für die Ausdrücke, die in den in der Familie gespeicherten XML-Formaten verwendet werden:

1. Es können nur einfache Elementpfade verwendet werden, die im Stammelement des Dokuments beginnen.
2. Elementpfade dürfen keine Namespacepräfixe enthalten, selbst wenn diese im Dokument angezeigt werden können.

Aktionen aktivieren oder inaktivieren

Das Fenster **Aktionen** zeigt alle verfügbaren Aktionen an, die für eine Verbindung verwendet werden können. Es werden sowohl vom System zur Verfügung gestellte Aktionen aufgelistet (gekennzeichnet in der Spalte **Provider** mit **Produkt**), als auch benutzererstellte Aktionen.

Führen Sie die folgenden Schritte aus, um die Aktionen zu aktivieren oder zu inaktivieren:

- Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Aktionen**, um das Fenster **Aktionen** anzuzeigen.
- Ändern sie den Status (**Aktiviert** oder **Inaktiviert**) der Aktion. Klicken Sie auf **Speichern**.

Handler verwalten

Das Fenster `Handlerliste` zeigt alle Handler an, die für die Verwendung mit einer Aktion, einem Empfänger, einem Ziel oder einem festgelegten Arbeitsablauf verfügbar sind. Es werden sowohl vom System zur Verfügung gestellte Handler aufgelistet, die in der Spalte **Provider** mit **Produkt** gekennzeichnet sind, als auch benutzerdefinierte Handler, die hochgeladen wurden.

Im Fenster `Handlerliste` können Sie Informationen zu den verfügbaren Handlern anzeigen. Hierzu gehören z. B. der Handlertyp, sein Klassenname und die Angabe, ob der Handler von WebSphere Partner Gateway oder vom Benutzer zur Verfügung gestellt wurde. Außerdem können Sie einen Handler importieren oder löschen.

Handler importieren

Führen Sie die folgenden Schritte aus, um einen neuen Handler in Ihre Umgebung zu importieren:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Handler**.
2. Klicken Sie im Fenster **Handlerliste** auf **Importieren**.
3. Geben Sie für **Datei** den Namen einer XML-Datei an, die den Handler repräsentiert, den Sie importieren möchten, oder verwenden Sie die Option **Durchsuchen**, um zu der Datei zu navigieren.
4. Geben Sie wahlweise an, ob der Handler in der Datenbank festgeschrieben werden soll. Wenn Sie auf **Ja** klicken, kann der Handler verwendet werden. Wenn Sie auf **Nein** klicken, kann der Handler nicht verwendet werden. Der Standardwert ist **Ja**.
5. Geben Sie wahlweise an, ob die Datei eine Datei desselben Namens überschreiben soll. Wenn Sie auf **Ja** klicken und der Name der Datei, die Sie gerade hochladen, mit dem Namen einer vorhandenen Handlerdatei übereinstimmt, wird die vorhandene Datei durch die hochgeladene Datei ersetzt. Diese Funktion wird hauptsächlich verwendet, wenn Änderungen an einem Handler vorgenommen wurden, der von einem Benutzer bereitgestellt wurde, und Sie den vorhandenen Handler durch eine aktualisierte Version ersetzen möchten. Der Standardwert ist **Nein**.
6. Klicken Sie auf **Hochladen**.

Nachdem eine Handlerdatei hochgeladen wurde, wird sie in der Liste verfügbarer Handler aufgeführt.

Handler löschen

Führen Sie die folgenden Schritte aus, um einen Handler zu löschen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Handler**.
2. Klicken Sie auf der Seite `Handlerliste` neben dem Handler, den Sie löschen möchten, auf das Symbol **Löschen**.

Attribut 'content-type' in Handlern konfigurieren

In einigen Fällen kann Document Manager möglicherweise bestimmte EDI-X12-Dokumente mit Textattributen oder einfachen Attributen ('text/plain') erst dann weiterleiten, wenn sie konfiguriert wurden. Die Handler, wie beispielsweise **BinaryChannelParseHandler**, **XMLRouterBizHandler** oder **EDIRouterBizProcessHand-**

ler, unterstützen durch Kommata getrennte Werte für das Attribut 'content-type'. Diesen Handlern muss der Inhaltstyp 'text/plain' manuell hinzugefügt werden.

Anmerkung: Sie sollten die Handlerwerte nur ändern, wenn Ihnen Ihr IBM Ansprechpartner dazu geraten hat.

Führen Sie die folgenden Schritte aus, um das Attribut 'text/plain' den Handlern hinzuzufügen.

1. Klicken Sie auf **Hubadmin** > **Fester Arbeitsablauf** > **ChannelParseFactory**.
2. Wählen Sie **EDIRouterBizProcessHandler** aus und klicken Sie auf das Symbol **Bearbeiten**.
3. Wählen Sie in der **Konfigurationsliste** den Eintrag **EDIRouterBizProcessHandler** aus und klicken Sie auf **Konfigurieren**.
4. Bearbeiten Sie das Attribut 'content-type', indem Sie dem Inhaltstyp **text/plain** hinzufügen.
5. Klicken Sie auf **Speichern**.

Zuordnungen verwalten

Dieser Abschnitt beschreibt, wie Sie die verschiedenen Zuordnungstypen verwalten, die Ihnen für die Verwendung mit WebSphere Partner Gateway zur Verfügung stehen.

Validierungszuordnungen aktualisieren

Verwenden Sie das folgende Verfahren, um eine momentan im System vorhandene Validierungszuordnung zu aktualisieren:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Zuordnungen** > **Validierungszuordnungen**.

   Die derzeit im System vorhandenen Validierungszuordnungen werden angezeigt.
2. Klicken Sie auf das Symbol **Zuordnung herunterladen**, um die Zuordnung auf Ihren lokalen Computer herunterzuladen. Aktualisieren Sie die Zuordnung wie erforderlich.
3. Klicken Sie auf das Symbol **Zuordnung hochladen**, um die aktualisierte Zuordnung in Ihr System hochzuladen.

Verwendungsorte von Validierungszuordnungen anzeigen

Gehen Sie wie folgt vor, um die Verwendungsorte von Validierungszuordnungen anzuzeigen (d. h., um anzuzeigen, wo eine Validierungszuordnung verwendet wird):

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Zuordnungen** > **Validierungszuordnungen**.

   Die derzeit im System vorhandenen Validierungszuordnungen werden angezeigt.
2. Klicken Sie auf das Symbol **Verwendet von**, um alle Routing-Objekte anzuzeigen, die die Validierungszuordnung verwenden.

Validierungszuordnungen löschen

Gehen Sie wie folgt vor, um eine Validierungszuordnung zu löschen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Zuordnungen** > **Validierungszuordnungen**.

   Die derzeit im System vorhandenen Validierungszuordnungen werden angezeigt.
2. Klicken Sie auf das Symbol **Löschen**.

   Anmerkung: Eine Warnung wird angezeigt, mit der eine Bestätigung angefordert wird, wenn die Validierungszuordnung von einer der Dokumentdefinitionen verwendet wird. Wird die Validierungszuordnung von keinem Routing-Objekt verwendet, wird keine Warnung angezeigt.
3. Klicken Sie im Warnfenster auf **OK**, um das Löschen zu bestätigen. Vor dem Löschen wird die Validierungszuordnung aus den Dokumentdefinitionen dereferenziert. Klicken Sie auf **Abbrechen**, um die Löschoperation abzubrechen.

Transformationszuordnungen verwalten

Über die Seite zum Verwalten von Transformationszuordnungen können Sie eine Liste der Transformationszuordnungen anzeigen, die sich derzeit im System befinden, oder nach einer bestimmten Zuordnung suchen.

Über diese Seite können Sie die folgenden Tasks ausführen:

- Suche nach einer bestimmten Zuordnung durchführen (Name, Beschreibung)
- Momentan im System vorhandene Transformationszuordnungen anzeigen

1. Klicken Sie auf das Symbol **Details**, um die Details einer Zuordnung anzuzeigen.
2. Klicken Sie auf das Symbol **Zuordnung herunterladen**, um eine Transformationszuordnung auf Ihren lokalen Computer herunterzuladen. Dies ist hilfreich, wenn Sie eine Zuordnung aktualisieren müssen.
3. Klicken Sie auf das Symbol **Zuordnung hochladen**, um eine aktualisierte Zuordnung in Ihr System hochzuladen.

Informationen zum Erstellen einer neuen Transformationszuordnung finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

EDI-Zuordnungen der Funktionsbestätigungen verwalten

Über die Seite **EDI-Zuordnungen der Funktionsbestätigungen verwalten** können Sie eine Liste der Funktionsbestätigungszuordnungen (FA-Zuordnungen) anzeigen, die sich derzeit im System befinden, oder nach einer bestimmten Zuordnung suchen. Eine FA-Zuordnung kann Routing-Objekten zugeordnet werden, die Attributwerte können jedoch nicht bearbeitet werden.

Über diese Seite können Sie die folgenden Tasks ausführen:

- Suche nach einer bestimmten Zuordnung durchführen (Name, Beschreibung)
- Momentan im System vorhandene FA-Zuordnungen anzeigen

1. Klicken Sie auf das Symbol **Details anzeigen**, um die Details einer Zuordnung anzuzeigen.
2. Klicken Sie auf das Symbol **Verwendet von**, um festzustellen, wo bzw. von wem eine FA-Zuordnung verwendet wird.
3. Klicken Sie auf das Symbol **Löschen**, um eine FA-Zuordnung zu löschen.

EDIs verwalten

Sie können viele der Attribute ändern, die zum EDI-Austausch gehören. Sie können beispielsweise die Standardwerte ändern, die für alle Umschläge angegeben werden, oder spezielle Umschläge für bestimmte Arten des Austauschs definieren, Sie können Kontrollnummern festlegen, die den verschiedenen Abschnitten eines Austauschs zugeordnet werden, und Sie können Verbindungsprofile einrichten, sodass ein Austausch auf unterschiedliche Weise ausgeführt werden kann. Diese Tasks werden im folgenden Abschnitt beschrieben.

Umschlagsprofil

Über das Fenster **Umschlagsprofile** können Sie einen Umschlagsprofilsatz anzeigen, bearbeiten, erstellen oder löschen. Für jedes aufgelistete Profil wird der EDI-Standard angezeigt (X12, UCS, EDIFACT).

Eine Beschreibung der Attribute für das Umschlagsprofil für die EDI-Standards enthält das Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Umschlagsprofilsätze bearbeiten

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Umschlagsprofil**.
2. Klicken Sie neben dem Namen des Umschlagsprofils, das Sie bearbeiten möchten, auf das Symbol **Details anzeigen**.
3. Wählen Sie den Umschlagsprofiltyp aus, den Sie ändern möchten, und klicken Sie auf das Symbol **Bearbeiten**.

   Die Attributwerte der ausgewählten Umschlagsprofile werden angezeigt ("Allgemein", "Austausch", "Gruppe" oder "Transaktion"). Die Attributbeschreibungen sind im Handbuch *WebSphere Partner Gateway Hubkonfiguration* enthalten.
4. Aktualisieren Sie die Attributwerte des Umschlagsprofils und klicken Sie auf **Speichern**. Die Attributbeschreibungen sind im Handbuch *WebSphere Partner Gateway Hubkonfiguration* enthalten.

Umschlagsprofilsätze erstellen

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Umschlagsprofil**.
2. Klicken Sie im Fenster **Umschlagsprofile** auf **Erstellen**.
3. Für die folgenden Felder sind Werte einzugeben:
   - **Name des Umschlagsprofils**: Geben Sie einen eindeutigen Namen für das neue Umschlagsprofil ein. Dies ist ein erforderliches Feld.

     Anmerkung: Falls der Name nicht eindeutig ist (also ein Umschlagsprofil mit demselben Namen bereits vorhanden ist), wird eine Fehlernachricht zurückgegeben, wenn Sie versuchen, das neue Umschlagsprofil zu speichern.
   - **Beschreibung**: Dies ist ein optionaler Wert. Geben Sie eine Kurzbeschreibung des Umschlagsprofils ein.
4. Wählen Sie in der Liste den EDI-Standardtyp aus (X12, UCS oder EDIFACT), der auf das neue Profil angewendet werden soll. Dies ist ein erforderliches Feld.

   Nachdem Sie in der Liste **EDI-Standard** einen Wert ausgewählt haben, werden die Umschlagsprofilattribute, die zu diesem Standard gehören, automatisch angezeigt ("Allgemein", "Austausch", "Gruppe" oder "Transaktion").
5. Aktualisieren Sie die Attributwerte des Umschlagsprofils und klicken Sie auf **Speichern**. Die Attributbeschreibungen sind im Handbuch *WebSphere Partner Gateway Hubkonfiguration* enthalten.

Umschlagsprofilsätze löschen

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Umschlagsprofil**.
2. Klicken Sie neben dem Namen des Umschlagsprofils, das Sie löschen möchten, auf das Symbol **Löschen**.

Programm zur Umschlagsgenerierung

Über die Seite des Programms zur Umschlagsgenerierung ("Enveloper") können Sie die Umschlagsgenerierungswerte für **Sperren und in die Warteschlange stellen** sowie für **Zeitplanung** anzeigen und bearbeiten.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Programm zur Umschlagsgenerierung**.
2. Klicken Sie auf das Symbol **Bearbeiten**, um die Attribute für die Zeitplanungsfunktion zu bearbeiten.
   - Geben Sie für **Maximale Sperrenzeit (Sekunden)** die maximale Zeit in Sekunden für die Datenbanksperre an. Dieser Wert wird in Sekunden angegeben. Die Sperre wird verwendet, um zu verhindern, dass mehrere Instanzen des Programms zur Umschlagsgenerierung gleichzeitig auf dieselben Daten zugreifen.
   - Geben Sie für **Höchstalter der Warteschlange (Sekunden)** die maximale Zeit in Sekunden an, bevor für Anforderungen in der Warteschlange eine Datenbanksperre erfolgt. Dieser Wert wird in Sekunden angegeben.
   - **Stapelbetrieb verwenden** ist eine globale Einstellung und wird standardmäßig ausgewählt. Wenn der Stapelbetrieb aktiviert ist, generiert das EDI-Programm zur Umschlagsgenerierung die Umschläge für die Transaktionen im Stapelbetrieb. Inaktivieren Sie das Kontrollkästchen **Stapelbetrieb verwenden**, um den Stapelbetrieb zu inaktivieren.
   - Klicken Sie entweder auf **Intervallgestützte Zeitplanung** (standardmäßig ausgewählt) oder auf **Kalendergestützte Zeitplanung**. Geben Sie für **Intervallgestützte Zeitplanung** die Zeit in Sekunden für das Intervall an. Klicken Sie in **Kalendergestützte Zeitplanung** auf **Täglicher Zeitplan**, **Wöchentlicher Zeitplan** oder auf **Angepasster Zeitplan**, wodurch der Zeitplan entsprechend definiert wird.
3. Klicken Sie auf **Speichern**.

Verbindungsprofile

Verbindungsprofile können für Transaktionen eingesetzt werden, die aus ihrem Umschlag entfernt wurden, und darüber hinaus für EDI-Austauschelemente, die vom Programm zur Umschlagsgenerierung erstellt wurden. Bei Transaktionen legt das Verbindungsprofil fest, wie die Transaktion verarbeitet werden soll, nachdem sie aus ihrem Umschlag entfernt wurde. Bei Austauschelementen gibt das Verbindungsprofil an, wie der Austausch zugestellt werden soll.

Über das Fenster **Verbindungsprofile** können Sie ein neues Profil erstellen oder die vorhandenen Profilinformationen bearbeiten. In der **Liste der Verbindungsprofile** finden Sie die Namen der derzeit definierten Profile und eine Beschreibung, falls vorhanden. Weitere Informationen zu Verbindungsprofilen finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Verbindungsprofile bearbeiten

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Verbindungsprofile**.

2. Klicken Sie auf das Symbol **Details anzeigen**, um die Seite **Details des Verbindungsprofils** anzuzeigen, in der eine Liste aller Attributwerte für das Verbindungsprofil enthalten ist.
3. Klicken Sie auf das Symbol **Bearbeiten** und bearbeiten Sie die Attribute.
4. Klicken Sie auf **Speichern**.

Verbindungsprofile erstellen

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Verbindungsprofile**.
2. Klicken Sie auf **Verbindungsprofil erstellen**, um ein neues Verbindungsprofil zu erstellen.
3. Geben Sie die jeweils zutreffenden Informationen in die folgenden Profilattributfelder ein:
   - **Name des Verbindungsprofils** - Eine eindeutige Namenskennung für das neue Profil. Dies ist das einzige erforderliche Feld.
   - **Beschreibung** - Eine Kurzbeschreibung des Verbindungsprofils.
   - **Qualifikationsmerkmal1** - Ein Wert, der festlegt, welche Verbindung für einen EDI-Austausch verwendet wird.
   - **EDI-Verwendungstyp** - Gibt an, ob es sich um einen Test-, Produktions- oder Informationsaustausch handelt.
   - **Anwendungsabsender-ID** - Die Anwendung oder der Unternehmensbereich, der dem Absender der Gruppe zugeordnet ist.
   - **Anwendungsempfänger-ID** - Die Anwendung oder der Unternehmensbereich, der dem Empfänger der Gruppe zugeordnet ist.
   - **Kennwort** - Das Kennwort, wenn für den Datenaustausch zwischen dem Anwendungsabsender und dem Anwendungsempfänger ein Kennwort erforderlich ist.
4. Klicken Sie auf **Speichern**. Die Seite **Details des Verbindungsprofils** wird für das neu erstellte Verbindungsprofil angezeigt.

Verbindungsprofile löschen

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Verbindungsprofile**.
2. Klicken Sie auf das Symbol **Löschen**, um das Verbindungsprofil zu löschen.

Initialisierung der Kontrollnummer

Auf der Seite **Konfiguration der Kontrollnummer** können Sie Kontrollnummern konfigurieren, die vom Programm zur Umschlagsgenerierung verwendet werden. Darüber hinaus können Sie dort nach einem oder mehreren Kontrollnummernpartnern suchen, indem Sie deren Namen bzw. einen Suchbegriff mit Platzhalterzeichen sowie (optional) die EDI-Funktionalität angeben. Die Suche mit Platzhalterzeichen kann eine beliebige Kombination von Buchstaben sowie Sternen (*) anstelle von Buchstaben enthalten. Eine Suche, bei der nur der Stern (*) als Suchbegriff verwendet wird, gibt eine Liste aller EDI-fähigen Partner zurück. Weitere Informationen zu Kontrollnummern und den entsprechenden Masken finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Initialisierung der Kontrollnummer**.
2. Geben Sie die Suchkriterien im Feld **Partnername** an. Als Kriterien können Sie entweder den Namen eines Partners oder Platzhaltersuchkriterien verwenden. Wenn Sie nicht nach EDI-fähigen Partnern suchen, inaktivieren Sie das Kontrollkästchen **EDI-fähig**. Das Kontrollkästchen ist standardmäßig ausgewählt. Wenn Sie nach EDI-fähigen Partnern suchen, lassen Sie das Kontrollkästchen

ausgewählt. Klicken Sie auf **Suchen**, um die Informationen anzuzeigen, die Ihre Suchkriterien in der Liste **Konfiguration der Kontrollnummer** erfüllen.

Anmerkung: Wenn Ihre Suche keine Ergebnisse erbringt, wird die folgende Nachricht angezeigt: "Nach Ihren Suchkriterien wurden keine Ergebnisse gefunden." Klicken Sie auf **Suchen**, um zur Seite **Konfiguration der Kontrollnummer** zurückzukehren und eine neue Suche anhand anderer Suchkriterien auszuführen.

3. Klicken Sie neben dem Partner auf das Symbol **Details anzeigen**.
4. Daraufhin werden die aktuellen Kontrollnummernzuordnungen des Partners (sofern vorhanden) auf der Seite **Konfigurationsdetails der Kontrollnummer** aufgelistet. Klicken Sie auf das Symbol **Bearbeiten**, um die Werte hinzuzufügen oder zu ändern.
5. Geben Sie den Wert neben **Austausch** ein, um die Nummer zu definieren, die zum Initialisieren der Kontrollnummerngenerierung für Austauschelemente verwendet werden soll, oder ändern Sie den vorhandenen Wert.
6. Geben Sie den Wert neben **Austausch** ein, um die Nummer zu definieren, die zum Initialisieren der Kontrollnummerngenerierung für Gruppen verwendet werden soll, oder ändern Sie den vorhandenen Wert. Alternativ hierzu können Sie auf **Maske** klicken und dann die Maske eingeben, die anstelle eines festen Wertes verwendet werden soll.
7. Geben Sie den Wert neben **Transaktion** ein, um die Nummer zu definieren, die zum Initialisieren der Kontrollnummerngenerierung für Transaktionen verwendet werden soll, oder ändern Sie den vorhandenen Wert. Alternativ hierzu können Sie auf **Maske** klicken und dann die Maske eingeben, die anstelle eines festen Wertes verwendet werden soll.
8. Klicken Sie auf **Speichern**.

Aktuelle Kontrollnummern

Über die Seite **Suche nach Status der Kontrollnummer** können Sie nach dem Status der Kontrollnummer eines Partnerpaares suchen.

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **EDI** > **Aktuelle Kontrollnummern**.
2. Verwenden Sie die folgenden Optionen, um nach einem einzelnen oder mehreren Absender- und Zielpartnern zu suchen.
   - **Partnername**: Der Name eines bestimmten Partners. Bei der Suchfunktion ist die Groß-/Kleinschreibung zu beachten. Geben Sie daher den Partnernamen genau so ein, wie er im System angezeigt wird.

     Anmerkung: Wählen Sie einen Absenderpartner und einen Zielpartner aus.
   - **EDI-fähige suchen**: Dieses Kontrollkästchen ist standardmäßig ausgewählt. Wenn Sie nicht nach EDI-fähigen Partnern suchen, inaktivieren Sie das Kontrollkästchen **EDI-fähig**. Wenn Sie nach EDI-fähigen Partnern suchen, lassen Sie das Kontrollkästchen ausgewählt.
   - Klicken Sie auf **Suchen**, um eine Suche zu starten.
   - **Suchergebnisse**: In diesem Feld werden die Suchergebnisse angezeigt. Das Feld **Suchergebnisse** enthält standardmäßig den vorausgewählten Eintrag **Alle Partner**. Wenn Sie nach allen Partnern suchen möchten, lassen Sie das Feld für den Partnernamen unausgefüllt, und klicken Sie auf **Suchen**. Wenn Sie nach einem bestimmten Partner suchen möchten, geben Sie den Namen in das Feld für den Partnernamen ein, und klicken Sie auf **Suchen**.

- **Aktuellen Status anzeigen**: Klicken Sie auf dieses Feld, um die Statuswerte der Kontrollnummern für das ausgewählte Partnerpaar anzuzeigen.

3. Klicken Sie auf das Symbol **Bearbeiten**, damit die Änderungen wirksam werden.

   Vorsicht:
   Verwenden Sie die Optionen Bearbeiten und Alle zurücksetzen nur in Ausnahmefällen, da die Kontrollnummern durch diese Optionen dupliziert werden könnten.

4. Wählen Sie eine der folgenden Aktionen:
   - Klicken Sie auf **Speichern**, um alle Änderungen zu speichern und zur Liste mit dem Status der Kontrollnummern zurückzukehren.
   - Klicken Sie auf **Zurückkehren**, um alle Änderungen zu verwerfen und zur Liste mit dem Status der Kontrollnummern zurückzukehren.
   - Klicken Sie auf **Alle zurücksetzen**, um den Status für das Partnerpaar zurückzusetzen, sodass beim nächsten Austausch von Nachrichten zwischen den Partnern die Statuswerte zurückgesetzt werden.

Systemkonfigurationsdaten verwalten

Über die Systemkonfigurationsdaten wird festgelegt, wie die Komponenten von WebSphere Partner Gateway auf die Systemressourcen zugreifen. Abhängig von Ihrer Installation variieren diese Ressourcen. Einige der Konfigurationsdaten werden für das Herstellen der Verbindung zwischen den Komponenten verwendet, andere Daten legen fest, wie die Systemressourcen auf die einzelnen Komponenten verteilt werden.

In WebSphere Partner Gateway werden die Systemkonfigurationsdaten in der Datenbank gespeichert und vom Benutzer "Hubadmin" über die Konsole konfiguriert.

Da die Datenbank von allen Instanzen der Hubkomponenten gemeinsam genutzt wird, ist es möglich, dass Komponenteninstanzen eine eigene Konfiguration benötigen und die gemeinsam genutzten Konfigurationsdaten nicht verwenden können. Um diese Situation zu handhaben, werden die Komponenten immer unter Verwendung des Servergeltungsbereichs auf die Attributwerte in der WebSphere Application Server-Umgebung geprüft, bevor die attributiven Daten von der zentralen Datenbank abgerufen werden.

Lesen Sie die WebSphere Application Server-Dokumentation im Hinblick auf die Schritte zur Definition von Variablen mit Servergeltungsbereich. Sie können die Aktionen über die Administrationskonsole von WebSphere Application Server oder über speziell dafür entworfene Scripts implementieren.

Auf Systemkonfigurationsdaten zugreifen

Führen Sie die folgenden Schritte aus, um auf die Systemkonfigurationsdaten zuzugreifen:

1. Melden Sie sich als "Hubadmin" an.
2. Klicken Sie in den Registerkarten des Menüs auf **Systemverwaltung**.

   Anmerkung: In der zweiten Zeile der Navigationsregisterkarten können Sie aus **Gemeinsame Eigenschaften**, **Konsolenverwaltung**, **DocMgr-Verwaltung**, **Funktionsverwaltung** oder **Empfängerverwaltung** auswählen. Über diese Registerkarten ist es möglich, auf die entsprechenden Anzeigen für Konfigurationsdaten oder auf weitere Navigationsregisterkarten zuzugreifen. Ausführliche

Informationen über bestimmte Konfigurationsdaten und über ihre Suche mithilfe der Konsole finden Sie in „Anhang C - Komponentenspezifische Systemattribute" auf Seite 253.

3. Navigieren Sie zu der Konfigurationsseite, die Sie bearbeiten möchten.
4. Klicken Sie auf dieser Seite auf **Bearbeiten** und ändern Sie die betreffenden Daten.
5. Klicken Sie auf **Speichern**, um die Änderungen in der Datenbank zu speichern, oder auf **Abbrechen**, um sie zu verwerfen.

Die meisten Änderungen werden unverzüglich wirksam, ohne dass das System erneut gestartet werden muss. Änderungen, für die ein Neustart einer oder mehrerer Komponenten erforderlich ist, werden in „Anhang C - Komponentenspezifische Systemattribute" auf Seite 253 aufgeführt.

Anmerkung: Sie sollten keinen dieser Werte ändern, wenn Sie mit der Arbeitsweise von WebSphere Partner Gateway nicht sehr vertraut sind. Normalerweise werden die Systemkonfigurationsdaten nur von erfahrenen System- oder Supportentwicklern geändert. Falls Sie diese Daten dennoch ändern möchten, sollten Sie die ursprünglichen Werte dokumentieren, damit Sie gegebenenfalls darauf zurückgreifen können.

Alert-Mail-Server konfigurieren

Alerts sind textbasierte E-Mail-Nachrichten, die die Partner über ein Systemereignis benachrichtigen. Wenn Sie diese Alerts verwenden möchten, konfigurieren Sie den SMTP-Server zusammen mit den Antwort-E-Mail-Adressen. Sie müssen die Antwort-E-Mail-Adressen für den Fall konfigurieren, dass Schwierigkeiten bei der Zustellung auftreten.

Sie finden die Konfigurationsattribute, indem Sie in der Konsole von WebSphere Partner Gateway zu **Systemverwaltung > DocMgr-Verwaltung > Alertengine** navigieren.

Diese Attribute sind:

- bcg.alertNotifications.mailHost
- bcg.alertNotifications.mailFrom
- bcg.alertNotifications.mailReplyTo
- bcg.alertNotifications.mailEnvelopeFrom

Weitere Erläuterungen im Hinblick auf den Zweck und die Werte für diese Attribute finden Sie in Tabelle 59 auf Seite 270.

Systemaktivität anzeigen

WebSphere Partner Gateway fasst regelmäßig Daten über die Systemaktivität zusammen. Die Daten dieses Zusammenfassungsservices sind die Informationen, die Sie sehen, wenn Sie die Funktionen für Dokumentanalyseberichte oder Dokumentvolumenberichte verwenden.

Über das Fenster **Merkmale für Zusammenfassungsservice** können Sie festlegen, wie oft die Daten generiert werden sollen. In diesem Fenster finden Sie außerdem Datum und Uhrzeit der letzten Aktualisierung der Zusammenfassungsdaten.

Führen Sie die folgenden Schritte aus, um das Zeitintervall zu ändern:

1. Klicken Sie auf **Systemverwaltung** > **DocMgr-Verwaltung** > **Andere** > **Zusammenfassungsengine**. In der Community Console wird das Fenster **Merkmale für Zusammenfassungsservice** geöffnet.
2. Klicken Sie im Fenster **Merkmale für Zusammenfassungsservice** neben **Verarbeitungsintervall (in Minuten)** auf das Symbol **Bearbeiten**.
3. Geben Sie einen Wert (zwischen 1 und 60) für die Anzahl von Minuten an, nach deren Ablauf die Daten erneut zusammengefasst werden sollen. Der Standardwert ist 15.
4. Klicken Sie auf **Speichern**.

Ereigniszustellung verwalten

In WebSphere Partner Gateway können Sie systemgenerierte Ereignisse für eine Anwendung bereitstellen (z. B. eine Überwachungsanwendung). Diese Ereignisse stellen Sie in einer JMS-Warteschlange bereit. Auf der Seite **Merkmale für Ereignisveröffentlichung** können Sie den Status der Ereignisveröffentlichung und (sofern vorhanden) die zugehörige JMS-Konfiguration anzeigen oder diesen Status ändern.

Anmerkung: Unter bestimmten Windows-Versionen (vor Windows XP) müssen Sie möglicherweise die Standardwerte des JMS-Warteschlangenfactorynamens und den JMS-Warteschlangennamen ändern, wenn Sie die Standardfunktion für die Ereigniszustellung verwenden wollen. Sie müssen den Wert für den JMS-Warteschlangenfactorynamen von `WBIC/QCF` in `WBIC\\QCF` und den Wert für den JMS-Warteschlangennamen von `jms/bcg/queue/deliveryQ` in `jms\\bcg\\queue\\deliveryQ` ändern.

Führen Sie die folgenden Schritte aus, um die Ereignisveröffentlichung zu aktivieren:

1. Klicken Sie auf **Systemverwaltung** > **Ereignisverarbeitung** > **Informationen zur Ereigniszustellung**.
2. Klicken Sie im Fenster **Merkmale für Ereignisveröffentlichung** neben **Ereignisveröffentlichung aktivieren** auf das Symbol **Bearbeiten**. Anschließend können Sie die Werte für die JMS-Eigenschaften eingeben oder ändern.

   Informationen zu Eigenschaftsbeschreibung finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.
3. Klicken Sie auf **Speichern**.

API-Aufrufe verwalten

Partner können API-Aufrufe (API - Application Programming Interface) für die Ausführung bestimmter Tasks ausführen, anstatt die Community Console zu verwenden.

Führen Sie die folgenden Schritte aus, um die Einstellungen der Administrations-API zu ändern:

1. Klicken Sie auf **Systemverwaltung** > **Funktionsverwaltung** > **Administrations-API**.
2. Klicken Sie im Fenster **Merkmale für Administrations-API** neben **Die XML-basierte API aktivieren** auf das Symbol **Bearbeiten**.

3. Wählen Sie das Kontrollkästchen aus, um die Verwendung der API zu aktivieren, oder löschen Sie den Inhalt des Kontrollkästchens, um die Verwendung der API zu inaktivieren.
4. Klicken Sie auf **Speichern**.

Anmerkung: Die XML-basierte Administrator-API wird nicht weiter unterstützt.

Für die Erstellungs- und Aktualisierungstasks kann anstelle der Administrator-API das in WebSphere Partner Gateway bereitgestellte Migrationsprogramm verwendet werden. Die Tasks im Zusammenhang mit der Erstellung und Aktualisierung, die früher nur über die Administrator-API ausgeführt werden konnten, sind jetzt mittels einer Migrationsimportdatei ausführbar, in der die neuen oder aktualisierten Informationen enthalten sind.

Die Importdatei wird durch das XML-Schema beschrieben, das mit dem Migrationsprogramm bereitgestellt wird. Sie können ein Entwicklungstool wie z. B. Rational Application Developer verwenden, um eine XML-Importdatei zu erstellen, die dem Schema entspricht. Durch den Import dieser Datei mit dem Migrationsprogramm können Sie neue Partnerdefinitionen sowie Kontakte und Geschäfts-IDs für diese Partner laden. Außerdem können Sie vorhandene Partnerdefinitionen aktualisieren, indem Sie diese mit dem Migrationsprogramm importieren. Mit der Administrator-API können Sie einige der Konfigurationsartefakte in einem System auflisten. Bei einem vollständigen Systemexport mithilfe des Migrationsprogramms werden in der exportierten XML-Datei Listen erstellt, in denen die Leistungsmerkmale der Partner, die Partnerverbindungen und die Empfänger (Ziele) aufgeführt sind.

Document Manager-Informationen verwalten

Mit der Administrationskonsole können Sie die Eigenschaften für die Document Manager-Verwaltung anzeigen und ändern. Document Manager ruft die zu verarbeitenden Dateien ab, indem er eine Abfrage an drei Dateisystemordner sendet, die von den anderen Komponenten des WebSphere Partner Gateway-Systems gemeinsam benutzt werden. Da mehrere Document Manager-Prozesse (mit jeweils mindestens einem Thread) auf die Dateisystemordner zugreifen können, sperrt WebSphere Partner Gateway die Dokumente, sodass nur ein Prozess (Thread) das Dokument in dem gemeinsam benutzten Ordner verarbeiten kann.

Max. Sperrendauer

Legen Sie die Werte für die maximale Sperrendauer für jeden der drei Ordner (Hauptordner, Ordner für synchrone Nachrichten und Ordner für Signalnachrichten) fest, um die maximale Sperrzeit zu konfigurieren, für die einer der DAE-Prozesse (Threads) die Dokumentsperre für die Verarbeitung des Dokuments aufrechterhalten kann.

- Im **Hauptordner** müssen Sie einen (in Sekunden angegebenen) Wert definieren, der die maximal zulässige Sperrendauer für die DAE-Instanz angibt, die eine Abfrage an das Hauptverzeichnis für eingehende Nachrichten (z. B. Ordner router_in unter Common) absetzt. Der Standardwert ist **3** Sekunden.
- Im **Ordner für synchrone Nachrichten** müssen Sie einen (in Sekunden angegebenen) Wert definieren, der die maximal zulässige Sperrendauer für die DAE-Instanz angibt, die eine Abfrage an das Verzeichnis für synchrone Nachrichten (z. B. Ordner sync_in unter Common) absetzt. Der Standardwert ist **3** Sekunden.
- Im **Ordner für Signalnachrichten** müssen Sie einen (in Sekunden angegebenen) Wert definieren, der die maximal zulässige Sperrendauer für die DAE-Instanz

angibt, die eine Abfrage an das Verzeichnis für Signalnachrichten (z. B. Ordner signal_in unter Common) absetzt. Der Standardwert ist **3** Sekunden.

Max. Anzahl Dateien pro Abfrageintervall

Legen Sie die Werte für die maximale Anzahl der Dateien pro Abfrageintervall für jeden der drei Ordner (Hauptordner, Ordner für synchrone Nachrichten und Ordner für Signalnachrichten) fest, um die maximale Anzahl der Dateien zu konfigurieren, die von einem zu verarbeitenden DAE-Thread (DAE = Document Acquisition Engine) verarbeitet werden können.

- Geben Sie im **Hauptordner** einen Wert größer als 0 ein, der die maximal zulässige Anzahl von Dateien für die DAE-Instanz angibt, die eine Abfrage an das Hauptverzeichnis für eingehende Nachrichten (router_in) absetzt. Der Standardwert ist **5**.
- Geben Sie im **Ordner für synchrone Nachrichten** einen Wert größer als 0 ein, der die maximal zulässige Anzahl von Dateien für die DAE-Instanz angibt, die eine Abfrage an das Verzeichnis für synchrone Nachrichten (sync_in) absetzt. Der Standardwert ist **5**.
- Geben Sie im **Ordner für Signalnachrichten** einen Wert größer als 0 ein, der die maximal zulässige Anzahl von Dateien für die DAE-Instanz angibt, die eine Abfrage an das Verzeichnis für Signalnachrichten (signal_in) absetzt. Der Standardwert ist **5**.

Gehen Sie wie folgt vor, um die Verwaltungseigenschaften anzuzeigen oder zu ändern:

1. Klicken Sie auf **Systemverwaltung** > **DocMgr-Verwaltung** > **BPE-DAE**.
2. Wählen Sie eine der unter **BPE-DAE** angezeigten Registerkarten aus, um entweder auf die Eigenschaftswerte **Haupteigenschaften**, **Signaleigenschaften** oder **Synchrone Eigenschaften** zuzugreifen.

   Daraufhin werden die Eigenschaften im Nur-Lesen-Modus auf der Seite **Verwaltung von Document Manager** angezeigt.
3. Klicken Sie auf das Symbol **Bearbeiten**, um die Eigenschaften zu bearbeiten.
4. Klicken Sie auf **Speichern**.

Unterstützung für ebMS

WebSphere Partner Gateway Version unterstützt den Mechanismus ebXML Message Service (ebMS). ebMS definiert das Schema für das Verpacken von Nachrichten in einen Umschlag und das Headerdokumentschema, mit dem ebXML-Nachrichten in einem Kommunikationsprotokoll übertragen werden. ebMS wird als ein Satz von Erweiterungen in mehreren Schichten definiert, die an die Basisspezifikationen "SOAP" und "SOAP mit Anhängen" gehängt werden. ebMS enthält Strukturen für einen Nachrichtenheader, mit dem eine Nachricht weitergeleitet und zugestellt wird und einen Nutzdatenbereich. ebMS hat als Schwerpunkt den Transport von Nutzdaten von einer PArtei zu einer anderen, was auch Vermittler ("Intermediäre") einschließen kann. Es ist wichtig zu beachten, dass ebMS nicht die Geschäftsprozesse oder die Korrektheit des gesendeten ebXML-Inhalts validiert. Die Funktion von ebMS besteht darin, dem Absender eine verlässliche und intakte Übertragung der ebXML-Nutzdaten zuzusichern. ebMS verwendet CPAs (Collaboration Protocol Agreements), um festzustellen, wie und welche Art von Daten zwischen zwei Parteien übermittelt werden.

CPA in WebSphere Partner Gateway hochladen

Ein CPA definiert sämtliche gültigen, sichtbaren und aktivierbaren elektronischen Dateninteraktionen zwischen zwei Parteien. Das CPA ist eine Vereinbarung zwischen zwei Parteien darüber, wie sie untereinander elektronische Daten austauschen wollen. Wenn ein CPA vorhanden ist, kann es in WebSphere Partner Gateway geladen werden und Sie bei der Konfiguration des Programms unterstützen. Wenn kein CPA vorhanden ist, kann das Programm manuell konfiguriert werden.

Es gibt zwei Möglichkeiten, ein CPA hochzuladen: über die Seite **Dokumentdefinition** oder über die Seite **Hubadmin**.

CPA über Seite 'Dokumentdefinition' hochladen

Gehen Sie wie folgt vor, um ein CPA hochzuladen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**.
2. Klicken Sie oben in der Anzeige auf den Link **Pakete hoch-/herunterladen**.
3. Wählen Sie als Pakettyp **ebMS CPA** aus und klicken Sie auf **Übergeben**.
4. Klicken Sie oben in der Anzeige auf den Link **CPA hochladen**.
5. Klicken Sie auf **Durchsuchen**, suchen Sie die betreffende Datei und klicken Sie auf **Öffnen**.
6. Stellen Sie sicher, dass die ebMS-Version 2.0 ausgewählt ist.
7. Klicken Sie auf **Hochladen**.

Mit dem erfolgreichem Abschluss des Hochladens haben Sie die internen und externen Partner erstellt. Die B2B-Funktionalitäten für interne und externe Partner sind aktiviert, Interaktionen und Verbindungen hergestellt und die jeweiligen Ziele erstellt. Beachten Sie, dass beim eventuellen Auftreten von Fehlern während des Hochladens eines CPAs die dabei durchgeführten Konfigurationen bis zum Auftreten des Fehlers nicht zurückgesetzt werden.

Anmerkung: Sie müssen etwaige Zertifikate im CPA manuell hochladen, die anschließend im Dateisystem gespeichert werden, damit bereits vorhandene Zertifikate nicht versehentlich ausgetauscht werden.

Während der Erstellung der Interaktion ist die Standardaktion auf **Pass-Through** gesetzt. Folgende zusätzlichen Verarbeitungsabläufe werden zur Unterstützung von ebMS durchgeführt:

- Ping
- Statusanforderung
- Fehler

WebSphere Partner Gateway prüft während der Laufzeit und bei Verarbeitung eines ebMS-Dokuments von einem WebSphere Partner Gateway-Partner, ob die ebMS-Interaktion der ebMS-Konfiguration entspricht (ob z. B. eine Verschlüsselung erforderlich ist). Bei Auftreten einer Nichtübereinstimmung schlägt das Dokument fehl. Die einzelnen Fehlerereignisse können in der Dokumentanzeige oder der ebMS-Anzeige angezeigt werden.

CPA über ebMS-Seite hochladen

Gehen Sie wie folgt vor, um ein CPA hochzuladen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **ebMS**.
2. Klicken Sie auf **CPA hochladen**.

3. Klicken Sie auf **Durchsuchen** und wählen Sie das betreffende CPA-Paket aus.
4. Stellen Sie sicher, dass die ebMS-Version 2.0 ausgewählt ist.
5. Klicken Sie auf **Hochladen**.

Während des Hochladens des CPAs werden Sie aufgefordert, unter den im CPA vorhandenen Partnern den internen Partner auszuwählen.

Nicht vorab ausgefüllte Attribute

Attributwerte werden auf Verbindungsebene während des Hochladens des CPAs festgelegt. Einige Attribute verfügen jedoch nicht über vorab ausgefüllte Werte. Im Folgenden sehen Sie eine Liste dieser Attribute sowie Beispielwerte:

- MIME-Parameter für Verschlüsselung.

  Die Werte können wie folgt lauten:

  ```
  i. smime-type="enveloped-data"
  ii. type="text/xml" version="1.0"
  ```

- Bestandteile verschlüsseln.

  Die Werte können wie folgt lauten:

  ```
  i. text/xml:application/binary:application/edi
  ii. */xml
  ```

  Anmerkung: Die Werte werden durch den Doppelpunkt (**:**) als Begrenzer getrennt.

- MIME-Parameter für Paket

  Die Werte können wie folgt lauten:

  ```
  i. type="text/xml" version="1.0"
  ii. type="multipart/related"
  ```

- Bestandteile verpacken.

  Die Werte können wie folgt lauten:

  ```
  i. text/xml:application/pkcs7-mime
  ii. text/xml:application/binary:application/edi
  ```

  Anmerkung: Das erste Element muss "text/xml" sein.

- Von Signatur ausschließen.

  Die Werte können wie folgt lauten:

  ```
  i. application/binary:text/xml:application/pkcs7-mime
  ii. application/pkcs7-mime
  ```

Von ebMS-unterstützte Algorithmen

ebMS unterstützt die folgenden verschiedenen Algorithmen:

- „Auszugs- und Signaturalgorithmen"
- „Algorithmen für XML-Verschlüsselung und SMIME-Verschlüsselung" auf Seite 43

Auszugs- und Signaturalgorithmen

Die folgenden Auszugsalgorithmen werden unterstützt:

- SHA1
- SHA256
- SHA512
- RIPEMD160

Die folgenden Signaturalgorithmen werden unterstützt:

- DSA-SHA1
- RSA-SHA1

Wenn die Signatur aufgrund eines Konfigurationsproblems fehlschlägt, wird das Ereignis `Unterzeichnen ist fehlgeschlagen` protokolliert. Ebenso wird bei fehlgeschlagener Signaturprüfung das Ereignis `Signaturprüfung ist fehlgeschlagen` protokolliert, und eine ebMS-Fehlernachricht wird generiert, die mögliche Ursachen für den fehlgeschlagenen Signaturprüfungsprozess enthält.

Algorithmen für XML-Verschlüsselung und SMIME-Verschlüsselung

Es gibt zwei unterstützte Protokolle für die ebMS-Verschlüsselung: XML-Verschlüsselung und SMIME-Verschlüsselung.

Wenn Sie die XML-Verschlüsselung verwenden, können Sie die folgenden Algorithmen einsetzen:

1. 3-des-cbc
2. aes-128-cbc
3. aes-192-cbc
4. aes-256-cbc

Wenn Sie die SMIME-Verschlüsselung verwenden, können Sie die folgenden Algorithmen einsetzen:

1. 3-des-cbc
2. aes-128-cbc.
3. aes-192-cbc
4. aes-256-cbc
5. rc2-128-cbc

Konfigurationsdetails zum Validieren von Web-Services

Mit dieser Funktion werden der SOAP-Hauptteil oder die Nutzdaten, die innerhalb des SOAP-Umschlags verfügbar sind, validiert. Die Validierung der Nutzdaten wird nur für XML-Nutzdaten in einem SOAP-Umschlag unterstützt. Hierdurch wird auch das Entfernen eines SOAP-Umschlags ermöglicht, bevor der SOAP-Hauptteil zur weiteren Verarbeitung eingeführt wird. Das Entfernen des SOAP-Umschlags wird nur bei asynchroner Kommunikation ausgeführt. Weitere Informationen zum Validieren von Web-Services finden finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*. Um Nutzdaten in einem SOAP-Umschlag zu validieren, müssen Sie neben der Konfiguration des Kanals für die Web-Services die folgenden zusätzlichen Konfigurationsschritte ausführen:

- Laden Sie die erforderliche Validierungszuordnung auf WebSphere Partner Gateway hoch. Weitere Informationen zum Hochladen der Validierungszuordnungen auf WebSphere Partner Gateway finden Sie im Kapitel "Dokumenttypen konfigurieren" des Handbuchs *WebSphere Partner Gateway Hubkonfiguration*.
- Ordnen Sie für die DTD-basierte Validierung die DTD der Validierungszuordnung unter dem jeweiligen Web-Service-Kanal zu. Weitere Informationen zum Zuordnen der Validierungszuordnung zu einem Kanal finden Sie im Kapitel "Dokumenttypen konfigurieren" des Handbuchs *WebSphere Partner Gateway Hubkonfiguration*.
- Für die schemabasierte Validierung können Sie die Validierungszuordnung optional unter ihrem jeweiligen Web-Service-Kanal zuordnen.

- Verwenden Sie beim Hochladen des Schemas auf WebSphere Partner Gateway die System-ID als Dateinamen. Wenn Sie die Schemapositionsfunktionalität in WebSphere Partner Gateway und den Industriestandard für die Angabe der Schemaposition in XML befolgen, muss das Schema der Validierungszuordnung unter dem jeweiligen Web-Service-Kanal nicht extern zugeordnet werden.
- Wählen Sie die integrierte Aktion **Validierung des SOAP-Hauptteils** aus, um den SOAP-Hauptteil unter dem Kanal für die Web-Service-Anforderung zu validieren.
- Sie können optional angeben, dass die Antwort nicht validiert werden soll, indem Sie das Attribut **Antwortvalidierung** für das Routing-Objekt auf "No" (Nein) festlegen. Modifizieren Sie auf der Zielseite das Attribut **Antwortvalidierung** für das Routing-Objekt.
- Indem Sie das Attribut **Inhaltsvalidierung** des Routing-Objekts aktivieren oder inaktivieren, können Sie die Inhaltsvalidierung über die Nutzdaten-XML ändern. Standardmäßig ist die Inhaltsvalidierung aktiviert.

Unbestreitbarkeitsprotokollierung verwenden

In WebSphere Partner Gateway sind jetzt mehr Konfigurationsoptionen für die Verwendung der Unbestreitbarkeit vorhanden, da ein Handelspartner oder ein interner Partner die Unbestreitbarkeit nun auf Paket-, Protokoll- und Dokumenttypebene konfigurieren kann. Durch die Verwendung dieser Konfiguration können Sie die Unbestreitbarkeit für jede einzelne Verbindung starten oder stoppen, anstatt alle Verbindungen starten oder stoppen zu müssen.

Beispiel: Führen Sie die folgenden Schritte aus, um die Unbestreitbarkeit für eine AS2-Verbindung zwischen einem Handelspartner und einem internen Partner einzuleiten:

1. Erstellen Sie eine Partnerverbindung zwischen **AS** > **None**.
2. Listen Sie die Partnerverbindung zwischen Handelspartner und internem Partner auf.
3. Bearbeiten Sie die Attribute für das AS2-Paket, indem Sie das Attribut `NonRepudiationRequired` auf `Ja` setzen.
4. Bearbeiten Sie die Attribute für das Paket "None", indem Sie das Attribut `NonRepudiationRequired` auf `Nein` setzen.

Weitere Informationen zur Einrichtung der Unbestreitbarkeitsattribute für das Paket, das Protokoll und den Dokumenttyp finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Nachrichtenspeicher verwenden

In WebSphere Partner Gateway sind jetzt mehr Konfigurationsoptionen für die Verwendung des Nachrichtenspeichers verfügbar, da ein Handelspartner oder ein interner Partner den Nachrichtenspeicher nun auf Paket-, Protokoll- und Dokumenttypebene konfigurieren kann. Durch die Verwendung dieser Konfiguration haben Sie die Flexibilität, zu entscheiden, welche Dokumente im Nachrichtenspeicher aufbewahrt werden sollen. Sie können auswählen, dass eingehende, ausgehende oder sowohl eingehende als auch ausgehende WebSphere Partner Gateway-Dokumente nicht im Nachrichtenspeicher gespeichert werden sollen.

Beispiel: Führen Sie die folgenden Schritte aus, um die Option für den Nachrichtenspeicher für eine AS2-Verbindung zwischen einem Handelspartner und einem internen Partner zu konfigurieren:

1. Erstellen Sie eine Partnerverbindung zwischen **AS** > **None**.
2. Listen Sie die Partnerverbindung zwischen Handelspartner und internem Partner auf.
3. Bearbeiten Sie die Attribute für das AS2-Paket und setzen Sie das Attribut `Nachrichtenspeicherung erforderlich` auf `Ja`.
4. Bearbeiten Sie die Attribute für das Paket `None` und setzen Sie das Attribut `Nachrichtenspeicherung erforderlich` auf `Nein`.

Weitere Informationen zum Einrichten der Attribute für den Nachrichtenspeicher auf der Paket-, Protokoll- und Dokumenttypebene finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Voraussetzungen zum Einrichten der Integrationsumgebung für WebSphere Partner Gateway - WebSphere Transformation Extender

Im Folgenden werden die Voraussetugen aufgelistet, die erfült sein müssen, damit die Integrationsumgebung für WebSphere Partner Gateway und WebSphere Transformation Extender eingerichtet werden kann:

1. WebSphere Partner Gateway V6.2.1 muss installiert sein und ausgeführt werden.
2. WebSphere Transformation Extender V8.2 muss installiert sein und ausgeführt werden.
3. Der WebSphere Transformation Extender-Server muss über Zugriff auf das gemeinsame Dateisystem von WebSphere Partner Gateway verfügen.
4. Kopieren Sie die Datei **dtxpi.jar** aus dem Installationsverzeichnis für WebSphere Transformation Extender in das Verzeichnis `<WebSphere Partner Gateway-Installationsverz>\router\lib\userexits`. Diese JAR-Datei enthält Laufzeitklassen für WebSphere Transformation Extender, die erforderlich sind, um WebSphere Transformation Extender zum Ausführen der Transformation aufzurufen.
5. Starten Sie den WebSphere Partner Gateway-Server "bcgdocmgr" neu, um die neuen JAR-Dateien zu aktivieren.
6. Fügen Sie das Installationsverzeichnis für WebSphere Transformation Extender zum Systempfad hinzu. Führen Sie diesen Schritt auch dann aus, wenn Sie den WebSphere Transformation Extender-RMI-Server nicht verwenden und stattdessen die Umgebung lokal ausführen. Starten Sie WebSphere Partner Gateway neu, um die neuen Pfadeinstellungen zu aktivieren.
7. Starten Sie den WebSphere Transformation Extender-RMI-Server, wenn Sie diesen Server verwenden.
8. Öffnen Sie eine Eingabeaufforderung und wechsln Sie in das Installationsverzeichnis für WebSphere Transformation Extender. Geben Sie den folgenden Befehl ein: `startRMIServer.bat -verbose`. Mit der Option 'verbose' wird die Portnummer für den RMI-Server angezeigt, an der der RMI-Server empfangsbereit ist.
9. Geben Sie in der WebSphere Partner Gateway-Konsole Werte für die folgenden Attribute an:
   - wtx.rmihostname
   - wtx.rmiport

- rmiuseserver
- bcg.wtx.mapLocation - Dieses Attribut befindet sich auf der Registerkarte 'Systemverwaltung'

Kapitel 5. Kontenverwaltungstasks

In diesem Kapitel werden die Tasks beschrieben, die der Kontenadministrator (Kontenadmin) ausführen kann. Hierbei handelt es sich um die folgenden Tasks:

Partnerprofile verwalten

Mit der Funktion für die Kontenadmin-Partner können Sie allen Benutzern, die Hubadministratoren sind, das Erstellen, Anzeigen, Bearbeiten und Löschen von Partnerprofilen ermöglichen. Ein Partnerprofil dient der Identifikation von Unternehmen (Partnern) gegenüber dem System. Weitere Informationen zum Erstellen von Partnerprofilen finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Anmerkung: Die Benutzer "interner Partner" und "externer Partner" können lediglich ihre eigenen Partnerprofile bearbeiten.

Partnerprofile anzeigen und bearbeiten

Führen Sie die folgenden Schritte aus, um Partnerprofile anzuzeigen und zu bearbeiten:

1. Klicken Sie auf **Kontenadmin**.
2. Klicken Sie auf **Suchen**.
3. Klicken Sie neben dem Namen des Partners, dessen Details Sie anzeigen möchten, auf das Symbol **Details anzeigen**.
4. Klicken Sie im Fenster mit den Partnerdetails auf das Symbol **Bearbeiten**.
5. Ändern Sie das Partnerprofil nach Bedarf.

   Anmerkung: Wenn Sie auf **Benutzerkennwörter zurücksetzen** klicken, zeigt die Community Console ein Bestätigungsfenster an. Klicken Sie auf **OK**, um fortzufahrenoder auf **Abbrechen**, um die Kennwörter beizubehalten. Das Zurücksetzen der Kennwörter zwingt alle Benutzer, für diesen Partner beim nächsten Anmelden ein neues Kennwort einzugeben.
6. Klicken Sie auf **Speichern**.

Partner suchen

Über das Fenster **Partner** können Sie nach Partnern suchen, die Ihren Suchkriterien entsprechen. Führen Sie die folgenden Schritte aus, um nach einem Partner zu suchen:

1. Klicken Sie auf **Kontenadmin**.
2. Geben Sie den Namen oder die Geschäfts-ID des Partners in das entsprechende Feld ein.

3. Klicken Sie auf **Suchen**. Das System sucht nach den Partnern, die mit Ihren Kriterien übereinstimmen.
4. Klicken Sie in der Spalte **Status** auf **Aktiviert** oder **Inaktiviert**, um den Status des gewünschten Partners zu ändern.
5. Wenn Sie die Details eines Partners anzeigen möchten, klicken Sie neben dem betreffenden Partner auf das Symbol **Details anzeigen**.
6. Klicken Sie auf das Symbol **Bearbeiten**, um das Profil des Partners zu bearbeiten.
7. Klicken Sie auf **Speichern**.

Partner löschen

Führen Sie die folgenden Schritte aus, um einen Partner zu löschen:

1. Klicken Sie auf **Kontenadmin**.
2. Geben Sie den Namen oder die Geschäfts-ID des Partners in das entsprechende Feld ein.
3. Klicken Sie auf **Suchen**. Das System sucht nach den Partnern, die mit Ihren Kriterien übereinstimmen.
4. Klicken Sie auf das Symbol **Löschen**, um einen Partner zu löschen.
5. Bestätigen Sie den Löschvorgang und speichern Sie Ihre Änderungen.

Zielkonfigurationen verwalten

Ziele verwalten die Transportinformationen, die für das korrekte Routing von Dokumenten zu ihrem Bestimmungsort innerhalb der Hub-Community sorgen. Das Transportprotokoll für ausgehende Dokumente legt fest, welche Informationen während der Zielkonfiguration verwendet werden. Informationen zum Erstellen von Zielen finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Erforderliche Angaben für die Zielkonfiguration

Der Transporttyp bestimmt die für die Einrichtung des Ziels erforderlichen Parameterdaten. In Tabelle 4 sind für die mit einem "X" markierten Felder Konfigurationsdaten erforderlich; mit einem "O" markierte Felder sind optional. Informationen zu Zielparameterbeschreibungen finden Sie in Tabelle 5 auf Seite 50.

Anmerkung: Die Möglichkeit, bestimmte Zielkonfigurationswerte zu bearbeiten, variiert mit der Berechtigungsstufe des Benutzers.

Tabelle 4. Erforderliche Transportinformationen

Erforderliche Transportinformationen	HTTP-Transport	HTTPS-Transport	FTP-Transport	FTPS-Transport	FTP-Scripting-Transport	Datei- verzeichnis-transport	JMS-Transport	SMTP-Transport
Authentifizierung erforderlich							O	O
Autom. Warteschlange	O	O	O	O			O	O
Verbindungszeitlimit	X	X	X	X	X			
FTPS-Modus					O			
JMS-Factory-Name							X	
JMS-JNDI-Factory-Name							X	
JMS-Nachrichtenklasse							X	
JMS-Nachrichtentyp							O	
JMS-Warteschlangenname							X	
Benutzer sperren					O			

Tabelle 4. Erforderliche Transportinformationen (Forts.)

Erforderliche Transportinformationen	HTTP-Transport	HTTPS-Transport	FTP-Transport	FTPS-Transport	FTP-Scripting-Transport	Datei- verzeichnis-transport	JMS-Transport	SMTP-Transport
Anzahl Threads	X	X	X			X	X	X
Kennwort	O	O	O	O	O	O	O	O
Provider-URL-Paket							O	
Wiederholungszahl	X	X	X	X	X	X	X	X
Wiederholungsintervall	X	X	X	X	X	X	X	X
Server-IP					X			
Empfänger-URI	X	X	X	X		X	X	X
Benutzer-ID					O			
Benutzername	O	O	O	O		O	O	O
Client-IP prüfen	O	O	O	O				
Client-SSL-Zertifikat prüfen		O						

Anmerkung:

1. Wenn die Option **Authentifizierung erforderlich** eines Ziels aktiviert ist und Benutzername und Kennwort zur Verfügung gestellt werden, gibt das Ziel den Benutzernamen und das Kennwort an das externe System weiter, zum dem es eine Verbindung herstellt, um Dokumente zuzustellen. Bei einem JMS-Ziel werden Benutzername und Kennwort als Berechtigungsnachweis für die JNDI-Suche der JMS-Warteschlangenverbindungsfactory verwendet. Beachten Sie, dass JMS über WebSphere MQ die JNDI-Authentifizierung nicht umsetzt, wenn die dateibasierte JNDI (Java Naming and Directory Interface) verwendet wird, um eine Verbindung zu einer JMS-Warteschlange herzustellen.
2. Für die FTPS-Authentifizierung sind Benutzername und Kennwort erforderlich, es sei denn, der FTPS-Server, mit dem Sie in Verbindung stehen, ordnet den Benutzer auf der Basis eines vorgelegten Clientzertifikats zu. Sprechen Sie mit dem FTPS-Serveradministrator wegen der Implementierungsdetails.

Ziele anzeigen und bearbeiten

Führen Sie die folgenden Schritte aus, um Ziele anzuzeigen und zu bearbeiten:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **{Partner}** > **Ziele**.
2. Klicken Sie in der Spalte **Zugriff** auf **Online** oder **Offline**, um den Zugriff auf ein Ziel zu ändern.
3. Klicken Sie in der Spalte **Status** auf **Aktiviert** oder **Inaktiviert**, um den Status eines Ziels zu ändern.
4. Klicken Sie auf das Symbol **Details anzeigen**, um die Details eines Ziels anzuzeigen.
5. Klicken Sie auf das Symbol **Bearbeiten**.
6. Bearbeiten Sie im Fenster **Zieldetails** die Zielparameter, die in Tabelle 5 auf Seite 50 beschrieben werden.
7. Klicken Sie auf **Speichern**.

   Sie können das Ziel auch löschen, indem Sie auf **Löschen** klicken.

Tabelle 5. Beschreibungen der Zielparameter

Parameter	Beschreibung
Authentifizierung erforderlich	Wenn aktiviert, werden Benutzername und Kennwort mit JMS- oder SMTP-Nachrichten übermittelt.
Autom. Warteschlange	Wenn die automatische Warteschlange aktiviert ist und die Zustellung des Dokuments beim ersten Mal fehlschlägt, wird das Ziel in den Offline-Modus versetzt, und das Dokument sowie alle weiteren Dokumente werden zur späteren Zustellung in die Warteschlange eingereiht. Das Ziel muss manuell in den Online-Modus versetzt werden. Ist die automatische Warteschlange inaktiviert und schlägt die Zustellung des Dokuments fehl, werden die Zustellungsversuche wiederholt. In diesem Fall wird das Ziel nicht in den Offline-Modus versetzt.
Kalendergestützte Zeitplanung	Wenn diese Option ausgewählt ist, werden die Dokumente, die dem Ziel zugeordnet sind, auf der Basis des ausgewählten Zeitplans verarbeitet.
Konfigurationspunkt-Handler	Gibt an, welche Handler für die Vor- und Nachbearbeitung verwendet werden.
Verbindungszeitlimit	Anzahl der Sekunden, die ein Socket geöffnet bleibt, wenn kein Datenverkehr auftritt. Der Standardwert ist 120 Sekunden (2 Minuten).
Beschreibung	Optionale Beschreibung des Ziels.
FTPS-Modus	Wählen Sie "Ja" oder "Nein" aus, um festzulegen, ob eine sichere Verbindung verwendet werden soll.
Zielname	Name, der zum Identifizieren des Ziels verwendet wird. **Anmerkung:** Der Zielname ist ein benutzerdefiniertes Feld mit freiem Format. Zwar ist die Eindeutigkeit der Namen nicht zwingend erforderlich, der Benutzer sollte aber unterschiedliche Namen für die einzelnen Ziele verwenden, um mögliche Unklarheiten zu vermeiden.
Intervallgestützte Zeitplanung	Wenn diese Option ausgewählt ist, verarbeitet das Ziel die Dokumente in den angegebenen Zeitintervallen.
JMS-Factory-Name	Name der Java(TM)-Klasse, den der JMS-Provider verwendet, um eine Verbindung zur JMS-Warteschlange herzustellen.
JMS-JNDI-Factory-Name	Factory-Name, mit dem die Verbindung zum Namensservice hergestellt wird.
JMS-Nachrichtenklasse	Die Klasse der Nachricht.
JMS-Nachrichtentyp	Der Typ der JMS-Nachricht. Da die Zuordnung des JMS-Nachrichtentyps durch die Empfängerkomponente festgelegt wird, ist der Wert für den JMS-Nachrichtentyp optional.
JMS-Warteschlangenname	Der Name der Warteschlange, in der JMS-Nachrichten gespeichert werden.
Wiederholungsintervall für Sperren (Sekunden)	Der Zeitraum, für den die FTP-Scriptkomponente zwischen den Wiederholungen der Sperren abwartet.
Wiederholungszähler für Sperren	Anzahl der Versuche der FTP-Scriptkomponente, die Sperre zu erhalten.
Benutzer sperren	Wählen Sie "Ja" oder "Nein" aus, um festzulegen, ob gleichzeitig bestehende Verbindungen möglich sein sollen.
Maximale Sperrenzeit (Sekunden)	Maximaler Zeitraum, über den die FTP-Scriptkomponente die Sperre aufrechterhält. Nach Ablauf des maximalen Zeitraums wird die Sperre an die Datenbank zurückgegeben.
Höchstalter der Warteschlange (Sekunden)	Maximaler Zeitraum, über den die FTP-Scriptkomponente in der Anforderungswarteschlange für Sperren bleibt. Sie wird in die Anforderungswarteschlange für Sperren gestellt, wenn die Anforderung für die Sperre verweigert wurde.

Tabelle 5. Beschreibungen der Zielparameter (Forts.)

Parameter	Beschreibung
Anzahl Threads	Anzahl der Threads, die für das Routing eines Dokuments zugeordnet wurden. Der Standardwert ist "3". Dieser Parameter steht den Benutzern zur Verfügung, die Hubadministratoren sind.
Online / Offline	Gibt an, ob das Ziel sich im Onlinestatus oder Offlinestatus befindet. Wenn es offline ist, werden die Dokumente in eine Warteschlange gestellt, bis das Ziel wieder online gesetzt wird.
Kennwort	Kennwort für den sicheren Zugriff durch die Partnerfirewall.
Provider-URL-Paket	Name von Klassen oder JAR-Dateien, mit denen Java die JMS-Kontext-URL verstehen kann.
Wiederholungszahl	Maximale Anzahl der Versuche des Systems, ein Dokument zu senden, bevor es fehlschlägt. Der Standardwert ist "3".
Wiederholungsintervall	Zeitraum, den das Ziel zwischen zwei Wiederholungsversuchen abwarten soll. Der Standardwert ist "300" (5 Minuten).
Scriptdatei	Das FTP-Script, das die FTP-Befehle enthält.
Server-IP	Server-IP-Adresse.
Status	Gibt an, ob das Ziel aktiviert oder inaktiviert ist. Falls das Ziel inaktiviert ist, schlägt die Verarbeitung von Dokumenten fehl, die über dieses Ziel geleitet werden.
Empfänger-URI	Uniform Resource Identifier (URI) des Partners.
Threadanzahl	Anzahl der Dokumente, die gleichzeitig verarbeitet werden sollen.
Transport	Protokoll für das Routing von Dokumenten (siehe „Erforderliche Angaben für die Zielkonfiguration" auf Seite 48).
Eindeutigen Dateinamen verwenden	Erstellt einen eindeutigen Dateinamen.
Benutzerdefinierte Attribute	Benutzer können für FTP-Scriptdateien eigene Attribute hinzufügen, die in der Community Console definiert werden können. Diese Attribute werden im Ziel gelesen und in der Scriptdatei ersetzt.
Benutzer-ID	Ist erforderlich, um auf den FTP-Server zuzugreifen.
Benutzername	Benutzername für den sicheren Zugriff durch die Partnerfirewall.
Client-IP prüfen	Prüft die IP-Adresse des sendenden Partners, bevor das Dokument verarbeitet wird. Wird mit dem Ziel verwendet, das als Quellenziel für eine Verbindung ausgewählt wurde.
Client-SSL-Zertifikat prüfen	Prüft und vergleicht das digitale Zertifikat des sendenden Partners mit der Geschäfts-ID, die dem Dokument zugeordnet ist, bevor das Dokument verarbeitet wird. Wird mit dem Ziel verwendet, das als Quellenziel für eine Verbindung ausgewählt wurde.

Standardziel anzeigen und bearbeiten

Führen Sie die folgenden Schritte aus, um die für das System konfigurierten Standardziele anzuzeigen und zu bearbeiten:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **{Profile}** > **Ziele**.
2. Klicken Sie in der oberen rechten Ecke des Fensters auf **Standardziele anzeigen**. Die Community Console zeigt eine Liste aller Betriebsmodi mit den ihnen zugeordneten Zielen an.
3. Klicken Sie auf das Symbol **Details anzeigen** neben einem Standardziel, um die dazugehörigen Informationen anzuzeigen.

4. Bearbeiten Sie die Informationen wie erforderlich und klicken Sie anschließend auf **Speichern**.

Verwendungsposition eines Ziels anzeigen

Gehen Sie wie folgt vor, um Details dazu anzuzeigen, wo ein bestimmtes Ziel eingesetzt wird:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **{Partner}** > **Ziele**.
2. Klicken Sie in der Liste der Ziele auf das Symbol **Verwendet von** für das gewünschte Ziel. Eine Liste wird angezeigt, in der aufgeführt wird, wo das ausgewählte Ziel verwendet wird.

   Anmerkung: Diese Anzeige enthält die Informationen auf verschiedenen Seiten, da das Ziel von vielen Kanälen verwendet werden kann. Auf jeder Seite werden maximal 10 Verbindungen angezeigt.

Ziel löschen

Die Funktion zum Löschen eines Ziels ist für alle Ziele mit Ausnahme des Standardziels verfügbar. Gehen Sie wie folgt vor, um ein Ziel zu löschen:

1. Klicken Sie auf **Kontenadmin** > **Profile** > **{Partner}** > **Ziele**.
2. Klicken Sie in der Liste der Ziele auf das Symbol **Löschen** für das Ziel, das gelöscht werden soll.

   Anmerkung: Das Symbol **Löschen** steht für das Standardziel nicht zur Verfügung. Darüber hinaus wird eine Warnung angezeigt, wenn das Ziel von einem Kanal verwendet wird. Weitere Informationen zur Verwendung von Zielen finden Sie im Abschnitt „Verwendungsposition eines Ziels anzeigen".
3. Klicken Sie im Warnfenster auf **OK**, um das Löschen zu bestätigen.

Transporte hochladen

Verwenden Sie die folgende Prozedur, um einen Transport hochzuladen.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **{Partner}** > **Ziele**.
2. Wählen Sie **Transporttypen verwalten** aus.
3. Klicken Sie auf **Durchsuchen** und wählen Sie den betreffenden Transport aus.
4. Wählen Sie aus, ob Sie den neuen Transport in der Datenbank festschreiben möchten.
5. Wählen Sie aus, ob die vorhandenen Daten überschrieben werden sollen.
6. Klicken Sie auf **Hochladen**.

Transporte löschen

Wenn Sie einen Transport nicht mehr benötigen, können Sie ihn mit der folgenden Prozedur löschen.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Ziele**.
2. Wählen Sie **Transporttypen verwalten** aus.
3. Klicken Sie neben dem aufgelisteten Transport auf das Symbol **Löschen**.

Transport- und Zielwiederholungen

Wenn die Zustellung eines Dokuments an ein Partnerziel fehlschlägt, versucht WebSphere Partner Gateway, das Dokument erneut zuzustellen. Jeder Versuch wird als *Wiederholung* (Retry) bezeichnet. Die Wiederholungsfunktionalität ist in WebSphere Partner Gateway auf zwei Ebenen vorhanden: Transport und Ziel.

Transportwiederholungen

Transportwiederholungen sind integrierte Wiederholungen der unteren Ebene, die für alle Ziele Anwendung finden. Der Grund für die Wiederholungen der unteren Ebene besteht darin, dass in den Netzwerken, über die die Zustellung versucht wird, vorübergehende Fehler auftreten, insbesondere im Internet. Daher ist das Zustellsystem so konzipiert, dass automatische Wiederholungen durchgeführt werden, ohne dass der Benutzer zur Definition der Wiederholungsparameter explizit aufgefordert wird. Die Anzahl der Transportwiederholungen (bcg.delivery.gwTransportMaxRetries) und das Zeitintervall zwischen den Wiederholungen (bcg.delivery.gwTransportRetryInterval) sind in der Konsole unter **Systemverwaltung** > **DocMgr-Verwaltung** > **Zustellmanager** definiert. Als Standardwert sind drei Wiederholungen im Abstand von je drei Sekunden festgelegt. Wenn das Wiederholungsintervall auf Null (0) gesetzt wurde, wird zwar keine Transportwiederholung, aber trotzdem eine Zielwiederholung versucht.

Zielwiederholungen (auch "Dokumentwiederholungen" genannt)

Die Parameter der Zielwiederholungen (die Anzahl der Wiederholungen und das Zeitintervall zwischen Wiederholungen) werden vom Benutzer in den Zieleigenschaften konfiguriert. Wenn das Wiederholungsintervall auf Null (0) gesetzt wurde, findet ungeachtet der Einstellungen für die Transportwiederholung keine Wiederholung statt. Das Zielwiederholungsintervall ist üblicherweise länger als die integrierten Transportwiederholungen. Dahinter steht die Absicht, dem Benutzer ausreichend Zeit vorzugeben, um das Problem zu beheben, das die Zustellung verhindert. So kann z. B. der Ziel-Web-Server inaktiv sein, oder die Ziel-URL ist nicht korrekt. Zum Festlegen der Parameterwerte muss der Benutzer jedem Ziel Werte zuweisen.

WebSphere Partner Gateway führt für jede (benutzerdefinierte) Zielwiederholung automatisch die Transportwiederholungen aus. Wenn z. B. drei Zielwiederholungen angegeben wurden, sieht das Wiederholungsmuster des Systems folgendermaßen aus:

- Erster Versuch schlägt fehl
- Zielwiederholung 1 schlägt fehl
  - Transportwiederholung 1 schlägt fehl
  - Transportwiederholung 2 schlägt fehl
  - Transportwiederholung 3 schlägt fehl
- Zielwiederholung 2 schlägt fehl
  - Transportwiederholung 1 schlägt fehl
  - Transportwiederholung 2 schlägt fehl
  - Transportwiederholung 3 schlägt fehl
- Zielwiederholung 3 schlägt fehl
  - Transportwiederholung 1 schlägt fehl
  - Transportwiederholung 2 schlägt fehl
  - Transportwiederholung 3 schlägt fehl
- Dokumentzustellung fehlgeschlagen

Jeder fehlgeschlagene Zustellversuch generiert ein Warnereignis, das in der Community Console aufgelistet wird.

Beispiel für Wiederholung

Im folgenden Beispiel wird die Interaktion für eine Wiederholung mit einem HTTP-Ziel beschrieben.

Konfiguration

Transport: Wiederholungen = 2, Intervall = 3000 Millisekunden (3 Sekunden).

HTTP-Ziel der Konsole: Wiederholungen = 3, Intervall = 20 Sekunden, Verbindungszeitlimit = 120 Sekunden.

1. Der Zustellmanager ruft den Absender des HTTP-Ziels auf. Daraufhin sendet der Absender des HTTP-Ziels die Anforderung, erhält jedoch innerhalb von 120 Sekunden, d. h. dem vorher in **Verbindungszeitlimit** festgelegten Wert für das Verbindungszeitlimit, keine Antwort.
2. Wiederholung 1 von 3 des Konsolengateways.

   Der Zustellmanager prüft die Wiederholungen auf der Ebene des Konsolengateways. Wenn es mehr als 0 sind, wartet der Zustellmanager das festgelegte Konsolenintervall ab (in diesem Fall 20 Sekunden).

   a. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.
   b. Der Zustellmanager wartet das in der Eigenschaft für die Wartezeit pro Transport festgelegte Intervall von 3000 Millisekunden ab.
   c. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.

      Dies ist Transportwiederholung 1 von 2.
   d. Der Zustellmanager wartet das in der Eigenschaft für die Wartezeit pro Transport festgelegte Intervall von 3000 Millisekunden ab.
   e. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.

      Dies ist Transportwiederholung 2 von 2.
3. Wiederholung 2 von 3 des Konsolengateways.

   Der Zustellmanager wartet das festgelegte Konsolenintervall von 20 Sekunden ab, bevor er die Wiederholung 2 von 3 des Konsolengateways startet.

   a. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.
   b. Der Zustellmanager wartet das in der Eigenschaft für die Wartezeit pro Transport festgelegte Intervall von 3000 Millisekunden ab.
   c. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.

      Dies ist Transportwiederholung 1 von 2.
   d. Der Zustellmanager wartet das in der Eigenschaft für die Wartezeit pro Transport festgelegte Intervall von 3000 Millisekunden ab.
   e. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.

Dies ist Transportwiederholung 2 von 2.

4. Wiederholung 3 von 3 des Konsolengateways.

   Der Zustellmanager wartet das festgelegte Konsolenintervall von 20 Sekunden ab, bevor er die Wiederholung 3 von 3 des Konsolengateways startet.

   a. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.
   b. Der Zustellmanager wartet das in der Eigenschaft für die Wartezeit pro Transport festgelegte Intervall von 3000 Millisekunden ab.
   c. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.

      Dies ist Transportwiederholung 1 von 2.
   d. Der Zustellmanager wartet das in der Eigenschaft für die Wartezeit pro Transport festgelegte Intervall von 3000 Millisekunden ab.
   e. Der Absender des HTTP-Ziels sendet die Anforderung, erhält jedoch innerhalb des Verbindungszeitlimits von 120 Sekunden (festgelegt in **Verbindungszeitlimit**) keine Antwort.

      Dies ist Transportwiederholung 2 von 2.

Wenn das Dokument bis zu diesem Zeitpunkt nicht gesendet worden ist, wird es in das Verzeichnis für fehlgeschlagene Gatewayverbindungen verschoben.

Für obenstehendes Szenario treten die folgenden Zeitintervalle auf:

120 Sekunden (Punkt 1 auf Seite 54) – Verbindungszeitlimit des Konsolengateways.
Zwischensumme für Punkt 1 = 120 Sekunden.

 20 Sekunden (Punkt 2 auf Seite 54) – Intervall des Konsolengateways (Wiederholung 1 von 3 der Konsole).
120 Sekunden (Punkt 2a auf Seite 54) – Verbindungszeitlimit des Konsolengateways.
  3 Sekunden (Punkt 2b auf Seite 54) – Transportintervall (Transportwiederholung 1 von 2).
120 Sekunden (Punkt 2c auf Seite 54) – Verbindungszeitlimit des Konsolengateways.
  3 Sekunden (Punkt 2d auf Seite 54) – Transportintervall (Transportwiederholung 2 von 2).
120 Sekunden (Punkt 2e auf Seite 54) – Verbindungszeitlimit des Konsolengateways.
Zwischensumme für Punkt 2 = 386 Sekunden.

 20 Sekunden (Punkt 3 auf Seite 54) – Intervall des Konsolengateways (Wiederholung 2 von 3 der Konsole).
120 Sekunden (Punkt 3a auf Seite 54) – Verbindungszeitlimit des Konsolengateways.
  3 Sekunden (Punkt 3b auf Seite 54) – Transportintervall (Transportwiederholung 1 von 2).
120 Sekunden (Punkt 3c auf Seite 54) – Verbindungszeitlimit des Konsolengateways.
  3 Sekunden (Punkt 3d auf Seite 54) – Transportintervall (Transportwiederholung 2 von 2).
120 Sekunden (Punkt 3e auf Seite 54) – Verbindungszeitlimit des Konsolengateways.
Zwischensumme für Punkt 3 = 386 Sekunden.

 20 Sekunden (Punkt 4) – Intervall des Konsolengateways (Wiederholung 3 von 3 der Konsole).
120 Sekunden (Punkt 4a) – Verbindungszeitlimit des Konsolengateways.
  3 Sekunden (Punkt 4b) – Transportintervall (Transportwiederholung 1 von 2).
120 Sekunden (Punkt 4c) – Verbindungszeitlimit des Konsolengateways.
  3 Sekunden (Punkt 4d) – Transportintervall (Transportwiederholung 2 von 2).
120 Sekunden (Punkt 4e) – Verbindungszeitlimit des Konsolengateways.
Zwischensumme für Punkt 4 = 386 Sekunden.

Gesamtzeitintervall für alle Punkte = 1278 Sekunden (ungefähr 21 Minuten).

In der Instanz, in der für die Verbindung keine Zeitlimitüberschreitung sondern eine zurückgewiesene Verbindung auftritt, wird das obenstehende Szenario trotz-

dem gestartet, jedoch findet die 120 Sekunden dauernde Verbindungszeitlimitüberschreitung nicht statt, da die Verbindung sofort zurückgewiesen wird.

Forward Proxy-Unterstützung

Beim HTTP- und beim HTTPS-Transport können Sie die Forward Proxy-Unterstützung definieren, sodass Dokumente über einen konfigurierten Proxy-Server gesendet werden. Bei WebSphere Partner Gateway können die folgenden Unterstützungstypen konfiguriert werden:

- Proxy-Unterstützung über HTTP
- Proxy-Unterstützung über HTTPS
- Proxy-Unterstützung über HTTPS mit Authentifizierung
- Proxy-Unterstützung über SOCKS

Nachdem Sie eine Forward Proxy-Einheit definiert haben, können Sie diese global für den Transport angeben, indem Sie die Einheit als Standardziel für den Forward Proxy definieren. (In diesem Fall wird die Forward Proxy-Einheit beispielsweise von allen HTTP-Zielen verwendet.) Sie können für jedes Ziel separat angeben, ob der Forward Proxy-Standardserver verwendet werden soll, oder einen anderen Forward Proxy-Server auswählen. Weitere Informationen zur Forward Proxy-Unterstützung finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Zertifikate verwalten

Ein digitales Zertifikat ist ein Online-Identitätsnachweis, ähnlich einem Reisepass oder Ausweis. Mit einem digitalen Zertifikat können Sie eine Einzelperson oder eine Organisation identifizieren. Ein digitales Zertifikat enthält die Informationen für die Identifizierung eines Benutzers sowie den öffentlichen Schlüssel des Benutzers. Es verknüpft den Schlüssel mit dem Benutzernamen und ist entweder selbst unterzeichnet oder wurde von einer Zertifizierungsstelle unterzeichnet.

Digitale Signaturen sind Berechnungen auf der Basis eines elektronischen Dokuments, das für die Verschlüsselung einen öffentlichen Schlüssel verwendet. Durch diesen Prozess ist die digitale Signatur an das unterzeichnete Dokument und an den Unterzeichner gebunden und kann nicht reproduziert werden. Mittlerweile haben digital unterschriebene elektronische Transaktionen juristisch gesehen dasselbe Gewicht wie unterzeichnete Papierdokumente.

WebSphere Partner Gateway verwendet digitale Zertifikate, um die Authentizität von Geschäftsdokumenttransaktionen zwischen den internen Partnern und den externen Partnern zu überprüfen. Sie werden außerdem für Verschlüsselung und Entschlüsselung verwendet.

Sie können ein primäres und ein sekundäres Zertifikat angeben, um sicherzustellen, dass der Dokumentaustausch nicht unterbrochen wird. Das primäre Zertifikat wird für alle Transaktionen verwendet. Das sekundäre Zertifikat wird verwendet, falls das primäre Zertifikat abgelaufen ist.

Digitale Zertifikate werden während des Konfigurationsprozesses hochgeladen und identifiziert.

Wenn ein Zertifikat abgelaufen ist oder widerrufen wurde, wird es inaktiviert und in der Community Console als inaktiviert ausgewiesen. Dies gilt jedoch nicht für Zertifikate, die als Root- oder Intermediate-Zertifikat hochgeladen werden. Wenn das primäre Zertifikat abgelaufen ist, wird es inaktiviert, und das sekundäre Zerti-

fikat wird als primäres Zertifikat eingesetzt. Wenn festgestellt wird, dass ein Zertifikat abgelaufen ist, wird ein Ereignis generiert.

Die Option **Zertifikatverwendung** ist je nach ausgewähltem Zertifikatstyp verfügbar. Im Profil **Hub-Operator** kann die Zertifikatverwendung auf die Zertifikatstypen **Digitale Signatur** oder **SSL-Client** festgelegt werden. Andere Typen können nicht ausgewählt werden. Im Profil für den internen Partner kann die Zertifikatverwendung auf die Zertifikatstypen **Digitale Signatur** oder **SSL-Client**, aber nicht auf **Verschlüsselung** festgelegt werden. Im Profil für den externen Partner kann die Zertifikatverwendung auf den Typ **Verschlüsselung**, aber nicht auf **Digitale Signatur**, **SSL-Client** oder **Server** festgelegt werden. Wenn dasselbe Zertifikat für unterschiedliche Zwecke verwendet werden soll, z. B. im Hub-Operator-Profil für die digitale Signatur und die Verschlüsselung, muss es zweimal geladen werden, einmal für die digitale Signatur und einmal für das Verschlüsselungszertifikat. Wird das Zertifikat allerdings für digitale Signaturen und für den SSL-Client verwendet, können die entsprechenden Kontrollkästchen im selben Zertifikatseintrag definiert werden. Wenn das Zertifikat als FTP-Server-Zertifikat und/oder SFTP-Server-Zertifikat verwendet werden soll, muss der Zertifikatstyp **SSL Server** sein und eines oder beide der Kontrollkästchen **FTP-Server-Authentifizierung** oder **SFTP-Server-Authentifizierung** muss ausgewählt werden.

Sekundäre Zertifikate können auch zweimal geladen werden, wobei ein Ladevorgang für die digitale Signatur und der andere für den SSL-Client ausgeführt wird. In diesem Fall muss beim sekundären Zertifikat dieselbe Vorgehensweise verwendet werden. Wenn die primären Zertifikate z. B. als separate Zertifikate für digitale Signaturen und für den SSL-Client geladen wurden, dann müssen auch die sekundären Zertifikate als separate Zertifikatseinträge geladen werden. (Dies gilt auch bei identischen Zertifikaten.)

Für die vollständige Zertifikatspfaderstellung und Validierung ist es erforderlich, dass Sie alle Zertifikate in der Zertifikatkette hochladen. Wenn z. B. die Zertifikatkette die Zertifikate A -> B -> C -> D enthält, in der A -> B bedeutet, dass A der Aussteller von B ist, sollten die Zertifikate A, B und C als Root-Zertifikate hochgeladen werden. Wenn eines der Zertifikate nicht verfügbar ist, wird der Zertifikatspfad nicht erstellt und die Transaktion schlägt fehl. Die CA-Zertifikate können von Zertifikatrepositorys beschafft werden, die von der Zertifizierungsstelle verwaltet werden. Root- und Intermediate-Zertifikate können nur im Hub-Operator-Profil hochgeladen werden.

Anmerkung: Bevor Sie die in den folgenden Abschnitten beschriebenen Prozeduren anwenden können, müssen die Zertifikate in das System geladen werden. Weitere Informationen zum Laden der Zertifikate finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

In der Sicht **Zertifikatsmanagement** können Sie Zertifikatgruppen modifizieren, die für eine bestimmte Partnerverbindung verwendet werden. Eine Option zum Filtern wird bereitgestellt. Modifizieren Sie die Zertifikatgruppen, die in einer Verbindung verwendet werden. Dieser Vorgang kann auch direkt über die Partnerverbindung ausgeführt werden. Führen Sie die folgenden Schritte aus, um Zertifikatgruppen zu verwalten:

1. Navigieren Sie in der Konsole zur Option **Profil** > **{Partner}** > **Zertifikat** > **Zertifikatsmanagement**.
2. Wenn Sie als Hubbetreiber angemeldet sind, können Sie einen internen Partner und einen externen Partner auswählen. Stellen Sie sicher, dass nicht für beide Werte "Alle" ausgewählt ist.

3. Klicken Sie auf **Suchen** um die Partner oder Untergruppen von Partnern zu suchen.

   Anmerkung: Die Pakete für den Absender und den Empfänger werden auf der Basis der ausgewählten Partner im Voraus ausgefüllt. Die Untergruppen werden basierend auf Ihrer Auswahl auch in der Tabelle angezeigt. Die Tabellenspalten geben den SSL-Client, die digitale Signatur (ist der Absenderpartner auf "Alle" gesetzt, ist diese Angabe inaktiviert) und die Verschlüsselung (ist der Empfängerpartner auf "Alle" gesetzt, ist diese Angabe inaktiviert) an. Die Zeilen geben den Operationstyp an.
4. Aktualisieren Sie die Zertifikatgruppen und klicken Sie auf **Speichern**. Die Änderungen werden auf der Verbindungsebene widergegeben.

Eigenschaften für Zertifikatspfad ('CertPath') konfigurieren

Die Zertifikatspfadeigenschaften können mit der Administrationskonsole von WebSphere Application Server und der WebSphere Partner Gateway-Konsole konfiguriert werden. Auf die Eigenschaften greifen Sie zu, indem Sie auf **Systemkonfiguration** > **DocMgr-Konfiguration** > **Sicherheit** klicken. Die Eigenschaften werden in schreibgeschützter Ansicht angezeigt. Wenn Sie sie bearbeiten möchten, klicken Sie auf das Symbol **Bearbeiten**. In den folgenden Beschreibungen wird der Konfigurationsprozess für die Zertifikatspfadeigenschaften kurz zusammengefasst.

bcg.CRLDir

Diese Eigenschaft enthält den Verzeichnisnamen, in dem die Zertifikatswiderrufslisten (CRLs) gespeichert sind. Der Standardwert ist:

`<WebSphere_Partner_Gateway_installationsverzeichnis>/common/security/crl`

bcg.checkRevocationStatus

Diese Eigenschaft legt fest, ob der Widerrufsstatus geprüft werden soll. Die für diese Eigenschaft gültigen Werte sind "wahr", "falsch" und "leer".

Der Widerrufstatus des digitalen Zertifikats wird geprüft, wenn der Wert entweder auf "wahr" oder auf "leer" gesetzt wurde. Wenn der Wert auf "falsch" gesetzt wurde, wird der Widerrufsstatus nicht geprüft.

Standardwert und empfohlene Einstellung für diese Eigenschaft ist "wahr".

bcg.build_complete_certpath

Diese Eigenschaft gibt an, ob der Zertifikatspfad ('CertPath') zum Root-Zertifikat oder zum Ausstellerzertifikat aufgebaut werden soll. Die für diese Eigenschaft gültigen Werte sind "wahr", "falsch" und "leer".

Der Zertifikatspfad wird zum Root-Zertifikat aufgebaut, wenn der Wert entweder auf "wahr" oder auf "leer" gesetzt wurde. Der Zertifikatspfad wird nur zum Ausstellerzertifikat aufgebaut, wenn der Wert auf "falsch" gesetzt wurde.

Standardwert und empfohlene Einstellung für diese Eigenschaft ist "wahr".

CRL-DP konfigurieren

Wenn Sie den CRL-DP (Certificate Revocation List Distribution Point - Verteilungspunkt der Zertifikatswiderrufsliste) konfigurieren wollen, müssen Sie die folgenden beiden Aktionen ausführen:

- Java Virtual Machine so konfigurieren, dass der CRL-DP aktiviert oder inaktiviert ist.
- Den HTTP-Proxy-Host und -Port festlegen.

Einstellungen von Java Virtual Machine für den CRL-DP ändern:

Wenn Sie die Konfiguration von Java Virtual Machine für einen Anwendungsserverprozess anzeigen und ändern möchten, verwenden Sie dazu in der Administrationskonsole die Seite **Java Virtual Machine**, oder verwenden Sie die Administrationskonsole von WebSphere Application Server, um die Konfiguration über eine Scripterstellung zu ändern.

1. Wählen Sie in der Administrationskonsole **Server** > **Anwendungsserver** > <*Server*> > **Java- und Prozessverwaltung** > **Prozessdefinition** > **Java Virtual Machine** aus.
2. Geben Sie wie unten angegeben die betreffenden Werte für die Java Virtual Machine-Einstellungen an und klicken Sie auf **OK**.
3. Wenn die nächste Seite angezeigt wird, klicken Sie in der Taskleiste der Konsole auf **Speichern**, damit die Änderungen in der Masterkonfiguration gespeichert werden.
4. Starten Sie den Anwendungsserver erneut.

Nähere Einzelheiten zur Konfiguration der Java Virtual Machine finden Sie in der Dokumentation zu WebSphere Application Server.

Wenn Sie die Verwendung des CRL-DP (Certificate Revocation List Distribution Point - Verteilungspunkt für Zertifikatswiderrufslisten) aktivieren möchten, setzen Sie die betreffende Eigenschaft von Java Virtual Machine `com.ibm.security.enableCRLDP` im Feld **Generic JVM Properties** wie folgt auf "true":

```
-Dcom.ibm.security.enableCRLDP=true
```

Wenn Sie die Verwendung des CRL-DP inaktivieren möchten, setzen Sie die Eigenschaft `com.ibm.security.enableCRLDP` von Java Virtual Machine im Feld **Generic JVM Properties** wie folgt auf "false":

```
-Dcom.ibm.security.enableCRLDP=false
```

HTTP-Proxyhost und -Port für den CRL-DP einrichten: Richten Sie die folgenden Java Virtual Machine-Eigenschaften im Feld **Generic JVM Properties** ein:

```
-D http.proxyHost=<proxyhostname_oder_ip-adresse>

-D http.proxyPort=<proxy-portnummer>
```

Wenn Sie den HTTP-Proxyhost und -Port entfernen möchten, entfernen Sie die folgenden Eigenschaften aus den Java Virtual Machine-Eigenschaften im Feld **Generic JVM Properties**:

```
-D http.proxyHost

-D http.proxyPort
```

Anmerkung: Immer wenn eine dieser Eigenschaften geändert wird, muss die Änderung für alle Server durchgeführt werden, auf denen WebSphere Partner Gateway-Anwendungen aktiv sind.

Digitale Zertifikate anzeigen und bearbeiten

Gehen Sie folgendermaßen vor, um die digitalen Zertifikate aufzulisten und zu bearbeiten, die unter dem (zuvor auf das System hochgeladenen) Hub-Operator-Profil gespeichert sind.

Anmerkung: Um die unter dem Profil eines Geschäftspartners gespeicherten Zertifikate anzuzeigen und zu bearbeiten, müssen Sie zuerst auf der Seite **Partnersuche** den gewünschten Geschäftspartner und anschließend die Registerkarte **Zertifikate** auswählen.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Zertifikate**. In der Community Console wird die Liste der digitalen Zertifikate angezeigt.

   Anmerkung: Durch rote Zertifikatsdaten wird angegeben, dass das digitale Zertifikat abgelaufen oder noch nicht gültig ist.
2. Klicken Sie neben einem Zertifikat auf das Symbol **Details anzeigen**. In der Community Console wird das Fenster **Zertifikatdetails** angezeigt.
3. Klicken Sie auf das Symbol **Bearbeiten**, um das digitale Zertifikat zu bearbeiten.
4. Aktualisieren Sie die folgenden Parameter im Fenster und klicken Sie dann auf **Speichern**.

Tabelle 6. Parameter für digitale Zertifikate

Parameter	Beschreibung
Zertifikatsname	Geben Sie den Namen des Zertifikats an.
Beschreibung	Geben Sie eine kurze Beschreibung des Zertifikats an.
Status	Wählen Sie **Aktiviert** aus, um den Status des Zertifikats ('Gültig' oder 'Ungültig') anzuzeigen. Wählen Sie **Inaktiviert** aus, um das Zertifikat zu inaktivieren.

Digitales Zertifikat inaktivieren

Wenn Sie kein digitales Zertifikat verwenden möchten, gehen Sie nach der folgenden Prozedur vor, um es zu inaktivieren.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **Zertifikate**. In der Community Console wird die Liste der digitalen Zertifikate angezeigt.
2. Klicken Sie neben dem Zertifikat, das Sie inaktivieren möchten, auf das Symbol **Details anzeigen**.
3. Klicken Sie auf das Symbol **Bearbeiten**, um die Zertifikatdetails zu bearbeiten.
4. Wählen Sie für **Status** die Option **Inaktiviert** aus.
5. Klicken Sie auf **Speichern**.

Anmerkung: Wenn ein primäres Zertifikat inaktiviert wird, dann legt das System das zugehörige sekundäre Zertifikat als primäres Zertifikat fest. Ist das sekundäre Zertifikat inaktiviert, gibt das System eine Warnung aus, in der Sie darüber informiert werden, dass kein sekundäres Zertifikat zur Verfügung steht.

B2B-Attributwerte ändern

Verwenden Sie die folgende Prozedur, um die Attributwerte in einer Dokumentdefinition zu ändern.

Anmerkung: Änderungen der Attributwerte für eine Dokumentdefinition der höheren Ebene werden von den Definitionen der unteren Ebene innerhalb desselben Knotens übernommen.

1. Klicken Sie auf **Kontenadmin** > **Profile** > **{Partner}** > **B2B-Funktionalität**. In der Community Console wird das Fenster **B2B-Funktionalität** geöffnet.

2. Klicken Sie auf die betreffende Dokumentdefinitionsebene, um einen Knoten einzeln einzublenden, oder wählen Sie eine Zahl von 0 bis 4 oder **Alle** aus, um alle angezeigten Dokumentdefinitionsknoten für die ausgewählte Ebene einzublenden.
3. Klicken Sie auf das Symbol **Bearbeiten**, um die betreffenden Attributwerte in der Spalte **Aktualisieren** zu ändern.
4. Klicken Sie auf **Speichern**.

Partnerverbindungen verwalten

Partnerverbindungen sind der Mechanismus, der das System in die Lage versetzt, Dokumente zu verarbeiten und zwischen dem internen Partner und seinen verschiedenen Partnern weiterzuleiten. Die Verbindungen enthalten die Informationen, die für den korrekten Austausch aller Dokumenttypen notwendig sind. Hierzu gehören die Attribute für die RosettaNet-Handelspartnervereinbarung, die Informationen zum Transportprotokoll, zur Dokumentverarbeitungsaktion, zum Betriebsmodus und zum Partnerziel. Ein Dokument kann nur weitergeleitet werden, wenn eine Verbindung zwischen dem internen Partner und einem seiner Partner besteht.

Das System erstellt auf der Basis der jeweiligen B2B-Funktionalitäten automatisch Verbindungen zwischen den internen Partnern und den externen Partnern. Die Daten, die in das Modul für die B2B-Funktionalitäten der Community Console eingegeben werden, legen die Funktionalität aller verfügbaren Verbindungen fest. Die Konfiguration jeder einzelnen Verbindung kann so geändert werden, dass sie den Bedürfnissen der Hub-Community entspricht.

Verbindungskomponenten

Die einzelnen Verbindungen bestehen aus den folgenden Komponenten:

- Attribute
- Aktion
- Ziel
- Betriebsmodus
- Zertifikate
- Verbindungsprofil

Nachdem das System eine Verbindung erstellt hat, können alle Komponenten geändert werden, um die Routing- und Verarbeitungsfunktionalität anzupassen. In Tabelle 7 werden die einzelnen Komponenten beschrieben.

Tabelle 7. Partnerkomponenten verwalten

Komponente	Beschreibung
Attribute	Attribute sind die Informationen, die die Verbindung für verschiedene Dokumentverarbeitungs- und Routingfunktionen verwendet, z. B. Validierung, Verschlüsselung und Wiederholungszahl. Zur Steigerung der Effizienz beim Erstellen von Verbindungen werden die Attribute für eine neue Verbindung von den B2B-Funktionalitäten der Partner automatisch übernommen.
Aktion	Eine Aktion ist eine Folge von Schritten, die das System zur Verarbeitung eines bestimmten Dokuments ausführt. Jede Verbindung besteht normalerweise aus mindestens einem Schritt, einschließlich Umsetzung, Duplikatprüfung, Validierung oder Pass-Through-Routing. Sie können für jede Verbindung die geeignete Aktion auswählen.

Tabelle 7. Partnerkomponenten verwalten (Forts.)

Komponente	Beschreibung
Ziel	Jede Verbindung enthält ein Quellen- und ein Rückkehrziel. Das Rückkehrziel enthält die URI und die Transportinformationen des Partners, der einen Dokumentenfluss einleitet. Geschäftssignale wie z. B. Empfangsbestätigungen und allgemeine Ausnahmebedingungen werden über das Rückkehrziel an den einleitenden Partner gesendet. Die Zielonsoptionen **Client-IP prüfen** und **Client-SSL-Zertifikat prüfen** gelten für das Rückkehrziel. Das Rückkehrziel enthält die URI und die Transportinformationen des Partners, der einen Dokumenttyp empfängt.
Betriebsmodus	Der Betriebsmodus gibt die Art des ausgetauschten Dokuments an. Eine Verbindung kann mehrere Betriebsmodi enthalten, um das Routing und die Verarbeitung desselben Dokuments an ein oder mehrere Systeme aufzunehmen. Die Verbindungseffizienz wird durch die mehrfache Verwendung einer einzigen Verbindung für Produktion, Test oder Routing zu mehreren Systemen innerhalb derselben Organisation gesteigert.
Zertifikate	Zertifikate werden für Verbindungen konfiguriert. Die konfigurierten Zertifikate werden bei der Verschlüsselung, beim Signieren und bei der SSL-Clientauthentifizierung verwendet. Zertifikate können für verschiedene Betriebsmodi konfiguriert werden.
Verbindungsprofil	Ein Verbindungsprofil enthält EDI-Attribute, die für eine bestimme Verbindung verwendet werden.

Verbindungsduplizierung

Das System verhindert das versehentliche Duplizieren von Verbindungen, indem jede Verbindung durch die folgenden Parameter eindeutig angegeben wird:

- Quellenpartner
- Quellenpaket und -version
- Quellenprotokoll und -version
- Quellendokumenttyp und -version
- Quellenaktivität (falss definiert)
- Quellenaktion (falls definiert)
- Zielpartner

Wenn es z. B. zwei Verbindungen mit demselben Quellenpartner, Quellendokument und Zielpartner gibt, können nicht beide Verbindungen aktiviert werden, selbst wenn das Zieldokument in den beiden Verbindungen jeweils ein anderes ist. In diesem Fall muss eine der beiden Verbindungen inaktiviert werden.

Anmerkung: EDI-Dokumente können mehrere Verbindungen wie beschrieben haben, wenn ihnen ein zusätzliches Verbindungsprofil zugeordnet ist. Die für ein Verbindungsprofil konfigurierten Werte werden verwendet, um zusätzliche Kriterien hinzuzufügen, sodass die Verbindung eindeutig identifiziert werden kann.

Verbindungen suchen

Um auf Verbindungen zuzugreifen, müssen Sie nach diesen suchen. Es gibt zwei Möglichkeiten, Verbindungen zu suchen:

- Verwenden Sie das Fenster **Verbindungen verwalten**, und wählen Sie die Quelle und den Empfänger aus, um Verbindungen zu suchen. Weitere Informationen hierzu finden Sie in „Allgemeine Suche nach Verbindungen ausführen" auf Seite 63.

- Verwenden Sie die erweiterte Suchfunktion des Systems, um zusätzliche Suchkriterien einzugeben. Hierzu gehören z. B. die Geschäfts-ID, einleitende und empfangende Pakete und Protokolle sowie einleitende und empfangende Dokumentenflüsse. Weitere Informationen hierzu finden Sie in „Erweiterte Suche nach Verbindungen ausführen" auf Seite 64.

Verwenden Sie die folgende Prozedur, um eine allgemeine Suche nach Verbindungen auszuführen. Beachten Sie die folgenden Richtlinien, wenn Sie eine Quelle und ein Ziel auswählen:

- Die Quelle und das Ziel müssen eindeutig sein.
- Verwenden Sie ein Produktionsziel nicht zusammen mit einem Testziel, wenn Sie Quelle und Empfänger auswählen; andernfalls tritt ein Fehler auf. Die Quelle und das Ziel müssen jeweils beide entweder Produktions- oder Testziele sein.

1. Klicken Sie auf **Kontenadmin** > **Verbindungen** > **Partnerverbindungen**. In der Community Console wird das Fenster **Verbindungen verwalten** angezeigt.
2. Wählen Sie unter **Quelle** eine Quelle aus.
3. Wählen Sie unter **Ziel** ein Ziel aus.

   Anmerkung: Zum Erstellen einer neuen Verbindung müssen die Quelle und das Ziel eindeutig sein.
4. Klicken Sie auf **Suchen**, um die Verbindungen zu suchen, die mit Ihren Kriterien übereinstimmen.
5. Klicken Sie nach Bedarf auf das jeweilige Element:
   - Klicken Sie auf das Symbol **Inaktivieren**, um die Verbindung zu inaktivieren.
   - Klicken Sie auf das Symbol **Aktivieren**, um die Verbindung zu aktivieren.
   - Klicken Sie auf **Attribute**, um das Fenster **Verbindungsattribute** zu öffnen, in dem Sie die Verbindungsattribute anzeigen und ändern können. Weitere Informationen finden Sie im Abschnitt „Partnerattributwerte ändern" auf Seite 65.
   - Klicken Sie auf **Aktionen**, um das Fenster **Verbindungsdetails** zu öffnen, in dem Sie die Aktion anzeigen und ändern können. Weitere Informationen finden Sie im Abschnitt „Neue Aktion auswählen" auf Seite 66.
   - Klicken Sie auf **Ziele**, um das Fenster **Ziele des Verbindungsmanagements** zu öffnen, in dem Sie die Rückkehrziele oder die Ziele anzeigen und ändern können. Weitere Informationen finden Sie im Abschnitt „Ziel oder Rückkehrziel ändern" auf Seite 66.
6. Klicken Sie auf **Aktivieren**, um eine Verbindung zu aktivieren. In der Community Console wird das Fenster **Verbindungen verwalten** angezeigt. Dieses Fenster zeigt das Paket, das Protokoll und den Dokumenttyp für die Quelle und den Empfänger an, ebenso die Optionen zum Anzeigen und Ändern des Partnerverbindungsstatus und der Parameter.

Allgemeine Suche nach Verbindungen ausführen

Verwenden Sie die folgende Prozedur, um eine allgemeine Suche nach Verbindungen auszuführen. Beachten Sie die folgenden Richtlinien, wenn Sie eine Quelle und ein Ziel auswählen:

- Die Quelle und das Ziel müssen eindeutig sein.

- Verwenden Sie ein Produktionsziel nicht zusammen mit einem Testziel, wenn Sie Quelle und Ziel auswählen; andernfalls tritt ein Fehler auf. Die Quelle und das Ziel müssen jeweils beide entweder Produktions- oder Testziele sein.
  1. Klicken Sie auf **Kontenadmin** > **Verbindungen** > **Partnerverbindungen**. In der Community Console wird das Fenster **Verbindungen verwalten** angezeigt.
  2. Wählen Sie unter **Quelle** eine Quelle aus.
  3. Wählen Sie unter **Ziel** ein Ziel aus.

     Anmerkung: Zum Erstellen einer neuen Verbindung müssen die Quelle und das Ziel eindeutig sein.
  4. Klicken Sie auf **Suchen**, um die Verbindungen zu suchen, die mit Ihren Kriterien übereinstimmen.
  5. Klicken Sie auf **Aktivieren**, um eine Verbindung zu aktivieren. In der Community Console wird das Fenster **Verbindungen verwalten** angezeigt. Dieses Fenster zeigt das Paket, das Protokoll und den Dokumenttyp für die Quelle und den Empfänger an, ebenso die Optionen zum Anzeigen und Ändern des Partnerverbindungsstatus und der Parameter.
  6. Klicken Sie nach Bedarf auf das jeweilige Element:
     - Wenn Sie auf das Symbol **Inaktivieren** klicken, wird die Verbindung inaktiviert.
     - Wenn Sie auf das Symbol **Aktivieren** klicken, wird die Verbindung aktiviert.
     - Wenn Sie auf **Attribute** klicken, wird das Fenster **Verbindungsattribute** geöffnet, in dem Sie die Verbindungsattribute anzeigen und ändern können. Weitere Informationen finden Sie im Abschnitt „Partnerattributwerte ändern" auf Seite 65.
     - Wenn Sie auf **Aktionen** klicken, wird das Fenster **Verbindungsdetails** geöffnet, in dem Sie die Aktion anzeigen und ändern können. Weitere Informationen finden Sie im Abschnitt „Neue Aktion auswählen" auf Seite 66.
     - Wenn Sie auf **Ziele** klicken, wird das Fenster **Ziele des Verbindungsmanagements** geöffnet, in dem Sie die Rückkehrziele oder die Ziele anzeigen und ändern können. Weitere Informationen finden Sie im Abschnitt „Ziel oder Rückkehrziel ändern" auf Seite 66.

Erweiterte Suche nach Verbindungen ausführen

Verwenden Sie die folgende Prozedur, um eine erweiterte Suche nach Verbindungen auszuführen. Beachten Sie die folgenden Richtlinien, wenn Sie eine Quelle und ein Ziel auswählen:

- Die Quelle und das Ziel müssen eindeutig sein.
- Verwenden Sie ein Produktionsziel nicht zusammen mit einem Testziel, wenn Sie Quelle und Ziel auswählen; andernfalls tritt ein Fehler auf. Die Quelle und das Ziel müssen jeweils beide entweder Produktions- oder Testziele sein.
  1. Klicken Sie auf **Kontenadmin** > **Verbindungen** > **Partnerverbindungen**. In der Community Console wird das Fenster **Verbindungen verwalten** angezeigt.
  2. Klicken Sie in der oberen rechten Ecke des Fensters auf **Erweiterte Suche**.
  3. Definieren Sie die folgenden Parameter gemäß den Informationen in Tabelle 8 auf Seite 65:

Tabelle 8. Fenster "Erweiterte Suche"

Parameter	Beschreibung
Nach Partnername suchen	Name der Quelle und des Ziels.
Nach Geschäfts-ID suchen	Geschäfts-ID der Quelle und des Ziels. Schließt DUNS, DUNS+4 und unformatierte ein.
Quellenpaket	Das von der Quelle verwendete Paket.
Zielpaket	Vom Ziel verwendetes Paket.
Quellenprotokoll	Das von der Quelle verwendete Protokoll.
Zielprotokoll	Das vom Ziel verwendete Protokoll.
Quellendokumenttyp	Der von der Quelle verwendete Dokumenttyp.
Zieldokumenttyp	Der vom Ziel verwendete Dokumenttyp.
Verbindungsstatus	Ermöglicht die Suche nach aktivierten und inaktivierten Verbindungen.

4. Klicken Sie auf **Suchen**. Das System sucht nach den Verbindungen, die mit Ihren Kriterien übereinstimmen.

Verbindungskonfigurationen ändern

Verwenden Sie die folgende Prozedur, um die Konfiguration einer Verbindung zu ändern.

1. Klicken Sie auf **Kontenadmin** > **Partnerverbindungen**. In der Community Console wird das Fenster **Verbindungen verwalten** angezeigt.
2. Führen Sie eine allgemeine Suche (siehe „Allgemeine Suche nach Verbindungen ausführen" auf Seite 63) oder eine erweiterte Suche nach Verbindungen aus („Erweiterte Suche nach Verbindungen ausführen" auf Seite 64).
3. Lesen Sie die betreffenden Abschnitte:
   - „Partnerattributwerte ändern"
   - „Neue Aktion auswählen" auf Seite 66
   - „Eine neue Transformationszuordnung auswählen" auf Seite 66
   - „Ziel oder Rückkehrziel ändern" auf Seite 66
   - „Verbindung sperren oder inaktivieren" auf Seite 66.

Partnerattributwerte ändern

Verwenden Sie die folgende Prozedur, um die Partnerattributwerte zu ändern.

1. Klicken Sie für den Quellen- oder Zielpartner auf **Attribute**.
2. Wählen Sie in der Liste **Bereich** die Option **Verbindung** aus, wenn die Attributänderungen auf alle Betriebsmodi angewendet werden sollen, die der Verbindung zugeordnet sind, oder wählen Sie einen einzelnen Betriebsmodus aus, auf den die Änderungen angewendet werden sollen.
3. Klicken Sie auf das Symbol **Erweitern** und erweitern Sie den Knoten bis zu der Dokumenttypdefinition, deren Attributwerte geändert werden sollen.
4. Aktualisieren Sie den Attributwert.
5. Klicken Sie auf **Speichern**.

Neue Aktion auswählen

Verwenden Sie zum Auswählen einer neuen Aktion die folgende Prozedur.

1. Klicken Sie auf **Aktionen**.
2. Wählen Sie die neue Aktion in der Liste aus.
3. Klicken Sie auf **Speichern**.

Eine neue Transformationszuordnung auswählen

Verwenden Sie die folgende Prozedur, um eine neue Transformationszuordnung auszuwählen:

1. Klicken Sie auf **Aktionen**.
2. Wählen Sie die neue Transformationszuordnung in der Liste aus.
3. Klicken Sie auf **Speichern**.

Ziel oder Rückkehrziel ändern

Gehen Sie wie folgt vor, um das Rückkehrziel oder das Ziel zu ändern:

1. Klicken Sie auf **Ziel**.
2. Wählen Sie das Ziel oder das Rückkehrziel in der Liste aus.
3. Klicken Sie auf **Speichern**.

Verbindung sperren oder inaktivieren

Klicken Sie in der Spalte **Aktiviert** auf das Symbol **Inaktivieren**, um eine Verbindung zu inaktivieren. Die Verbindung wird grau dargestellt, wodurch angegeben wird, dass die Verbindung inaktiviert wurde. Klicken Sie auf **Aktivieren**, um die Verbindung wieder zu aktivieren.

Für EDI-Dokumente kann es verschiedene Verbindungen geben, die für dieselben Partner gelten. Zwischen den verschiedenen Verbindungen wird anhand von Verbindungsprofilen unterschieden. Wenn Sie eine Verbindung mit einem zugeordneten Verbindungsprofilnamen löschen, wird die Verbindung im System gelöscht. Nur eine Verbindung auf Basisebene ohne zugeordnetes Verbindungsprofil kann inaktiviert werden. Weitere Informationen zu Verbindungsprofilen finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Ausschlusslisten verwalten

Mit einer Ausschlussliste kann der Hubadministrator Document Manager so konfigurieren, dass das Senden von RosettaNet-Benachrichtigungen der Geschäftspartner an den internen Partner eingeschränkt wird. Die Geschäftspartner werden nach Namen und Geschäfts-ID identifiziert.

Die folgenden Benachrichtigungen können für Routing-Einschränkungen ausgewählt werden:

- 0A1 - Fehlerhinweis

  Wird von einem Partner, der einen bestimmten Dokumenttyp nicht abschließen kann, an den internen Partner gesendet.
- Back-End-Ereignis

  Eine von System generierte XML-Datei, die an den internen Partner gesendet wird, um diesen darüber zu informieren, dass sein Partner ein Geschäftsdokument erfolgreich empfangen hat.

Partner zur Ausschlussliste hinzufügen

Verwenden Sie die folgende Prozedur, um einen Partner zur Ausschlussliste hinzuzufügen.

1. Klicken Sie auf **Kontenadmin** > **Ausschlussliste**. In der Community Console wird das Fenster **Ausschlussliste** geöffnet.
2. Wählen Sie in der Liste **Partnername** einen Partner aus. In der Community Console wird eine Liste aller Partner einschließlich der zugehörigen Geschäfts-IDs und ihres Ausschluss-Status angezeigt. Standardmäßig ist **Alle Benachrichtigungen senden** ausgewählt.

Ausschlussliste bearbeiten

Manchmal müssen Sie die Ausschlussliste bearbeiten. Möglicherweise möchten Sie das Weiterleiten einer Benachrichtigung an den internen Partner einschränken.

1. Klicken Sie auf **Kontenadmin** > **Ausschlussliste**. In der Community Console wird das Fenster **Ausschlussliste** geöffnet.
2. Wählen Sie in der Liste **Partnername** einen Partner aus. In der Community Console wird eine Liste aller Partner einschließlich der zugehörigen Geschäfts-IDs und ihres Ausschluss-Status angezeigt.
3. Klicken Sie auf das Symbol **Bearbeiten** neben der Benachrichtigung, die Sie bearbeiten möchten.
4. Wählen Sie das Kontrollkästchen unter der Benachrichtigung aus, um das Weiterleiten einer Benachrichtigung an den internen Partner einzuschränken. Wählen Sie **Alle Benachrichtigungen senden** aus, um alle Routingeinschränkungen zu entfernen.

Kapitel 6. Partnermigration verwalten

Das Migrationsdienstprogramm für die Konfiguration unterstützt Sie beim selektivem Export und Import der Konfigurationsdaten von WebSphere Partner Gateway. Zu diesen Konfigurationsdaten gehören beispielsweise die Benutzervorgaben, die Features, die Verbindungsdetails und die B2B-Funktionalität. Hierin liegt ein Unterschied zu anderen Optionen für das Versetzen von Daten, wie etwa Datenbanksicherung und -Wiederherstellung (Restore), da die Daten während des Exports mit dem Dienstprogramm selektiv extrahiert werden, während eine Datenbanksicherung normalerweise nicht selektiv ausgeführt wird.

Das Migrationsdienstprogramm für die Konfiguration exportiert ausgewählte Partner- und Systemdefinitionen in eine XML-Datei und in eine Gruppe von Unterstützungsdateien. Sie können diese Dateien anschließend in ein anderes System importieren und die Konfiguration zwischen verschiedenen Systemen übertragen.

Anmerkung: Bei der Übertragung von Daten zwischen den Systemen müssen beide Systeme dieselbe Version von WebSphere Partner Gateway verwenden.

Das Migrationsdienstprogramm wird hauptsächlich verwendet, um Konfigurationsdaten aus einem Entwicklungs- und Testsystem in ein Produktionssystem zu übertragen, Sie können jedoch die Konfigurationsdaten auch aus einer XML-Datei laden, die Sie auf Basis des bereitgestellten XML-Schemas erstellen.

Für die Ausführung des Migrationsdienstprogramms stehen zwei Optionen zur Verfügung:

1. Über eine Befehlszeilenschnittstelle, sodass das Migrationsdienstprogramm unter Verwendung eines Scripts gestartet werden kann.
2. Über eine API, sodass benutzerdefinierte Java-Programme das Migrationsdienstprogramm aufrufen können. Weitere Informationen zur Verwendung der API finden Sie im Handbuch *WebSphere Partner Gateway Programming Guide*.

Das Migrationsdienstprogramm wird als eigenständige Java-Anwendung implementiert, die WebSphere Partner Gateway über Remotezugriff aufruft. Es ist in eine komprimierte Datei mit dem Namen `BCGMigrationUtil.zip` gepackt. Diese Datei wird vom Hub-Installationsprogramm in folgendem Verzeichnis installiert: *`hub_installation`* `/console/support`.

Migrationsdienstprogramm über Befehlszeile verwenden

Bevor Sie das Migrationsdienstprogramm verwenden können, müssen Sie die Datei `BCGMigrationUtil.zip` auf der Workstation extrahieren, auf der Sie das Dienstprogramm ausführen möchten. Führen Sie nach dem Extrahieren der Dateien des Dienstprogramms in Ihr lokales Dateisystem die folgenden erforderlichen Schritte aus:

1. Die Konsolenkomponente des WebSphere Partner Gateway-Systems, aus dem Sie exportieren bzw. in das Sie importieren möchten, muss aktiv sein. Beachten Sie, dass das Dienstprogramm auf einer anderen als der Workstation ausgeführt werden kann, auf der die Konsolenkomponente installiert ist. Dies liegt daran, dass das Dienstprogramm auf die Konsole zugreift, indem das Protokoll IIOP (EJB) über ein Netz verwendet wird. Zwischen den Workstations muss Konnek-

tivität bestehen, und der IIOP-Port der Konsole (normalerweise 58809) muss über die Workstation verfügbar sein, auf der das Dienstprogramm ausgeführt wird.

2. Sie benötigen Java 5 auf der Workstation, auf der das Dienstprogramm ausgeführt werden soll. Installieren Sie JDK 1.5 auf Ihrem System.

   Wenn Sie das Befehlszeilenscript zur Ausführung des Dienstprogramms starten, ruft es für diese Position die Systemumgebungsvariable JAVA_HOME ab. Wenn JAVA_HOME nicht definiert ist, fordert das Script Sie dazu auf, die Basisposition für Java 5 anzugeben. Sie können z. B. die Kopie von Java 5 benutzen, die für die Verwendung durch WebSphere Application Server installiert ist. Verwenden Sie dafür den Wert *<WebSphere_installationsverzeichnis>*\java.

   Außerdem kann eine andere Systemumgebungsvariable mit dem Namen MIGRATION_PATH so definiert werden, dass sie auf die Position zeigt, an die BCGMigrationUtil.zip extrahiert wurde. Wenn MIGRATION_PATH nicht definiert ist, fordert das Script Sie auf, einen Pfad zu diesem Verzeichnis einzugeben. Das Verzeichnis, auf das MIGRATION_PATH verweist, ist das Verzeichnis mit dem Namen bcgmigrate unter dem Verzeichnis, in das die komprimierte Datei extrahiert wurde. Beispiel: Wenn Sie die Dateien in das Verzeichnis c:\IBM\migration extrahieren möchten, sollten Sie MIGRATION_PATH auf c:\IBM\migration\bcgmigrate setzen.

   Anmerkung: Stellen Sie sicher, dass Sie über die Dateiberechtigung **Ausführen** für "bcgmigrate.bat" bzw. "bcgmigrate.sh" verfügen, wenn Sie den Befehl "bcgmigrate" ausführen. Dies gilt für die UNIX-Plattform.

3. Wenn Sie Daten exportieren, ist eine Exportoptionsdatei erforderlich. Die Exportoptionsdatei gibt an, welche Datentypen vom Dienstprogramm extrahiert werden sollen. Die Konfigurationsdaten können für folgende Elemente in ein System exportiert werden:
   - Zeitpläne für das Programm zur Umschlagsgenerierung
   - Ereigniscodes
   - Transport- und Betriebsmodi
   - Handlerdefinitionen (nur Metadaten, benutzerdefinierte JAR-Dateien mit ausführbarem Code werden manuell übertragen).
   - Definitionen für feste Arbeitsabläufe (nur Metadaten, benutzerdefinierte JAR-Dateien mit ausführbarem Code werden manuell übertragen)
   - Definitionen für variable Arbeitsabläufe (nur Metadaten, benutzerdefinierte JAR-Dateien mit ausführbarem Code werden manuell übertragen)
   - Proxykonfigurationen und Umschlagsprofile
   - Verbindungsprofile, Validierungszuordnungen und Transformationszuordnungen
   - FA-Zuordnungen und Empfängerinstanzdaten
   - XML-Dokumentfamilien und -formate
   - Routingdefinitionen (Pakete, Protokolle und Dokumenttypen)
   - Partnerprofildaten (einschließlich Kontakten, Adressen, EDI-Kontrollnummerdaten sowie Zieldaten)
   - B2B-Funktionalität für Partner
   - Partnerverbindungen
   - Alertbenachrichtigungen
   - Gruppenkonfiguration
   - Benutzerkonfiguration

- FTP-Benutzerkonfiguration
- Zertifikate
- Fehlerdatenflusskonfiguration
- Eigenschaften der Systemverwaltung
- Konfiguration der Archivierungsfunktion

Eine Beispielexportoptionsdatei mit dem Namen `export.zip` ist im Verzeichnis *root_des_migrationsdienstprogramms*`/samples/export` verfügbar. Diese Datei exportiert alle unterstützten Konfigurationsdatentypen aus einem System. Bei der Optionsdatei kann es sich um eine XML-Datei handeln oder um eine komprimierte Datei (.zip), die eine XML-Datei enthält. Die XML-Datei muss dem XML-Schema `bcgMigrationExport.xsd` entsprechen, das sich im Verzeichnis *root_des_migrationsdienstprogramms*`/schemas` befindet.

Anmerkung: Stellen Sie sicher, dass die Abhängigkeitsanforderungen zwischen Exporttypen erfüllt werden.
Diese Abhängigkeiten werden näher im Abschnitt *Konfigurationstypabhängigkeiten migrieren* beschrieben.

4. Wenn Sie Daten importieren, müssen Sie über zu importierende Daten verfügen. Die Importdatei kann durch das Exportieren von Daten erstellt werden, oder Sie können Ihre eigene Datei schreiben, die die Definitionen enthält, welche Sie in ein System laden möchten. Nach dem Export sind die exportierten Daten in einer .zip-Datei enthalten. Die .zip-Datei enthält eine XML-Datei, die dem XML-Schema `bcgMigrationImport.xsd` entspricht, das sich im Verzeichnis *root_des_migrationsdienstprogramms*`/schemas` befindet. Die XML-Datei enthält Daten, die vom Importcode verwendet werden können, um die exportierten Konfigurationstypen zu reproduzieren.

   Die .zip-Datei enthält außerdem die folgenden Dateien:

   - Die exportierten Validierungs-, Transformations- und FA-Zuordnungen.
   - Die Datei `RoutingObjects.zip`, die die internen Darstellungen der exportierten Routing-Objekte enthält (Pakete, Protokolle und Dokumenttypen).

   Führen Sie die folgenden Schritte aus, um Ihre eigene Importdatei zu schreiben:

   - Erstellen Sie eine XML-Datei, die `bcgMigrationImport.xsd` entspricht.

     Stellen Sie sicher, dass die Abhängigkeitsanforderungen zwischen Importtypen erfüllt werden. Weitere Informationen im Hinblick auf Abhängigkeiten finden Sie im Abschnitt zu den Konfigurationstypabhängigkeiten.
   - Wenn in der XML-Importdatei etwaige Zuordnungen oder Routing-Objekte beschrieben sind, erstellen Sie eine .zip-Datei, bei der die XML-Datei sich im Stammverzeichnis der .zip-Datei befindet.

     Die Verzeichnisse lauten wie folgt:

     – Die Routing-Objekte befinden sich in einer Datei mit dem Namen `RoutingObjects.zip` im Verzeichnis `RoutingObjects` des Stammverzeichnisses.
     – Die Transformationszuordnungen befinden sich im Verzeichnis `TransformationMaps` im Stammverzeichnis.
     – Die Validierungszuordnungen befinden sich im Verzeichnis `ValidationMaps` im Stammverzeichnis.
     – Die FA-Zuordnungen befinden sich im Verzeichnis `FAMaps` im Stammverzeichnis.

Anmerkung: Wenn Sie Dateiverzeichnisempfänger importieren, darf das Empfängersystem das Dateiverzeichnis, das vom Empfänger verwendet wird, nicht bereits in seinem Dateisystem haben. Stellen Sie sicher, solche Verzeichnisse vor dem Import zu löschen.

5. Das Migrationsdienstprogramm muss sich an der von Ihnen verwendeten Konsole anmelden. Der WebSphere Partner Gateway-Benutzeraccount muss über die Berechtigung verfügen, Konfigurationen zu exportieren oder zu importieren. Der Benutzer "hubadmin" verfügt über diese Berechtigung. Wenn Sie einen anderen Account als "Hubadmin" oder einen Benutzer verwenden möchten, der Mitglied der Gruppe "Hubadmin" ist, müssen Sie zunächst für den Benutzer die Berechtigung zum Verwenden des Migrationsmoduls aktivieren. Die Berechtigung ist standardmäßig inaktiviert.

   Der Hubadministrator gibt die Eingabedatei an, aus der die Daten importiert werden. Außerdem gibt er an, ob die vorhandenen Informationen überschrieben werden sollen. Mit dem Migrationsdienstprogramm für die Konfiguration können Sie dann Konfigurationsdaten importieren, die bereits auf dem System vorhanden sind, sofern Ihr Profil Sie für das Überschreiben der Konfiguration berechtigt.

   Neue Informationen, die noch nicht vorhanden sind, werden zur Datenbank hinzugefügt. Ist die Option zum Überschreiben aktiviert, werden die Informationen in der Datenbank durch die Eingabedaten überschrieben. Ist diese Option inaktiviert, werden die Informationen in der Datenbank nicht durch die Eingabedaten überschrieben. Wenn eine Ausnahmebedingung auftritt, wird die Importoperation gestoppt und ein Fehlerereignis wird in die Protokolldatei geschrieben.

Aufruf über Befehlszeile

Sie können Konfigurationsdaten von einer WebSphere Partner Gateway-Instanz zu einer anderen WebSphere Partner Gateway-Instanz migrieren, indem Sie das Befehlszeilendienstprogramm verwenden. Nach der Beendigung der vorausgesetzten Schritte für die Verwendung des Dienstprogramms können Sie das Dienstprogramm aufrufen, indem Sie die Stapeldatei `bcgmigrate.bat` oder die Shellprozedur `bcgmigrate.sh` aufrufen. Diese Dateien befinden sich in folgenden Verzeichnissen:

- **Unter Windows:** `\<stammverzeichnis_des_migrationsdienstprogramms>\bcgmigrate\bin\`
- **Unter Linux/UNIX:** `/<stammverzeichnis_des_migrationsdienstprogramms>/bcgmigrate/bin/`

Anmerkung: Der Benutzer sollte entweder zur Gruppe "Hubadmin" oder zu einer anderen Betreibergruppe gehören, für die die Berechtigung für das Migrationsmodul aktiviert ist.

Wenn Sie das Script ohne Argumente ausgeben, wird eine Bedienerführungshilfe mit den erforderlichen Argumenten und der Syntax angezeigt.

Die Syntax für den Befehlszeilenaufruf unter Windows lautet wie folgt:

```
bcgmigrate [-h hostname:bootstrap_port] [-a import|export] -f dateiname_mit_pfad
-u benutzer-id -p kennwort [-r rootpfad [-o] [-d 1..5] ]
```

Auf UNIX-Systemen ist der Aufruf ähnlich, außer dass Sie `bcgmigrate.sh` anstelle von `bcgmigrate` verwenden müssen.

Legende:

- `-h` ist der Port hostname:bootstrap, in dem die Konsolenkomponente ausgeführt wird.
- `-a` bezeichnet die Aktivität ('import' oder 'export'). Standardmäßig wird 'export' verwendet.
- `-f` ist der vollständig qualifizierte Dateiname der Exportoptionsdatei oder der Importkonfigurationsdatei.
- `-u` ist die WebSphere Partner Gateway-Benutzer-ID mit Migrationsberechtigung.
- `-p` ist das WebSphere Partner Gateway-Benutzerkennwort.
- `-o` ist die Option zum Überschreiben.

  Anmerkung: Die Option zum Überschreiben wird nur von der Importaktivität verwendet. Wenn Sie `-o` nicht miteinbeziehen, werden nur neue Konfigurationen erstellt, und vorhandene Konfigurationsdaten werden nicht geändert. Das Einbeziehen von `-o` bedeutet, dass die vorhandene Konfiguration möglicherweise überschrieben wird, wenn sie in den importierten Daten anders ist.
- `-d` ist eine Debugstufe zwischen 1 und 5, wobei 5 die umfangreichste Debug-Ausgabe bietet. Das Argument `-d` ist optional und kann ausgelassen werden. Wenn es ausgelassen wird, werden nur Fehler protokolliert.
- `-r` ist der Stammverzeichnispfad, in dem exportierte Daten gespeichert und die Protokolldatei geschrieben wird. Das Argument `-r` ist optional und kann ausgelassen werden. Wenn es ausgelassen wird, können exportierte Daten in das Verzeichnis geschrieben werden, das von der Option `-f` festgelegt wird.

Beispielbefehl für Export

Im Folgenden sehen Sie einen Beispielbefehl für den Export unter Windows:

```
bcgmigrate -h localhost:58809 -a export -f D:\partnerMigration\export.xml
-u hubadmin -p admin123 -r d:\partnermigration\output -d 5
```

Auf UNIX-Systemen ist der Aufruf ähnlich, außer dass Sie `bcgmigrate.sh` anstelle von `bcgmigrate.bat` und im Verzeichnispfad Schrägstriche anstelle der Backslashes verwenden müssen.

Die Ausgabe für das Beispiel wird im Stammverzeichnis gespeichert, das durch die Option `-r` festgelegt wird.

Die Ausgabe wird in eine komprimierte Datei (.zip) mit dem Namen `BCGMigration_<ip_oder_hostname_aus_option_-h>.zip` geschrieben. Protokolle werden in die Datei `BCGMigration.log` geschrieben. Wenn die Option `-r` für einen Export nicht angegeben ist, wird die Ausgabe in das Verzeichnis gestellt, welches in der Option `-f` konfiguriert wird.

Beispielbefehl für Import

Im Folgenden sehen Sie einen Beispielbefehl für den Import unter Windows:

```
bcgmigrate.bat -h localhost:58809 -a import
-f D:\partnerMigration\BCGMigration_localhost.zip -u hubadmin -p admin123
-r d:\partnermigration\output -d 5
```

Auf UNIX-Systemen ist der Aufruf ähnlich, außer dass Sie `bcgmigrate.sh` anstelle von `bcgmigrate.bat` verwenden müssen. Nach Abschluss der Importoperation werden die Protokolle in die Datei `BCGMigration.log` geschrieben. Wenn die Option `-r` für einen Import nicht angegeben ist, wird die Ausgabe in das Verzeichnis gestellt, das in der Option `-f` konfiguriert wird.

Zuordnung der XML-Elemente zu den Elementen in der Konsole

Die exportierte Datei oder die zu importierende Datei liegt im XML-Format vor. Die XML-Elemente weisen nicht den gleichen Namen auf wie die entsprechenden Elemente in der Konsole. In der folgenden Tabelle wird die Zuordnung zwischen der Anzeige auf der Konsole und dem jeweiligen Stammelement in der XML-Datei dargestellt. Die Tabelle enthält nur die Sichten und Elementnamen und nicht die einzelnen Felder in der Anzeige. Ist der Elementname ein Link in der Sicht, wird er in Kursivschrift dargestellt.

Tabelle 9. Zuordnung der XML-Elemente zur Konsole

Elementname in XML	Sicht in der Konsole
EnveloperSchedulingInfo	Hubadmin > Hubkonfiguration > EDI > Programm zur Umschlagsgenerierung.
TransportTypeInfo	Hubadmin > Hubkonfiguration > Empfänger> *Transporttypen verwalten* und: Kontenadmin > Partner > Ziele > *Transporttypen verwalten*.
DestinationTypeInfo	Kontenadmin > Partner > Ziele > *Ziel erstellen*. Der Betriebsmodus wird durch "DestinationTypeInfo" dargestellt.
HandlerInfo	Hubadmin > Hubkonfiguration > Handler. Diese Anzeige enthält vier weitere Untermenüs: Aktion, Fester Arbeitsablauf, Ziel und Empfänger.
FixedWorkflowStepInfo	Hubadmin > Hubkonfiguration > Fester Arbeitsablauf > Eingehend und Hubadmin > Hubkonfiguration > Fester Arbeitsablauf > Ausgehend. Jeder Schritt wird als "FixedWorkflowStepInfo" dargestellt.
WorkflowInfo	Hubadmin > Hubkonfiguration > Handler. Jede Aktion auf der Listenseite wird als "WorkflowInfo" dargestellt.
EnvelopeProfileInfo	Hubadmin > Hubkonfiguration > EDI > Umschlagsprofil. Jedes Umschlagsprofil auf der Listenseite wird als "EnvelopeProfileInfo" dargestellt.
MapInfo	Hubadmin > Hubkonfiguration > Zuordnungen > Validierungszuordnungen. Jede Zuordnung auf der Listenseite wird als "MapInfo" dargestellt. Darüber hinaus ist der innere Tag "routingNameList" vorhanden. Dieser Tag steht für die Namen der Routing-Objekte, mit denen die Validierungszuordnung verknüpft ist.
TransformMapInfo	Hubadmin > Hubkonfiguration > Zuordnungen > Transformationszuordnungen. Jede Zuordnung auf der Listenseite wird als "TransformMapInfo" dargestellt.
FAMapInfo	Hubadmin > Hubkonfiguration > Zuordnungen > FA-Zuordnungen. Jede Zuordnung auf der Listenseite wird als "FAMapInfo" dargestellt. Darüber hinaus ist der innere Tag "routingNameList" vorhanden. Dieser Tag steht für die Namen der Routing-Objekte, mit denen die FA-Zuordnung verknüpft ist.

Tabelle 9. Zuordnung der XML-Elemente zur Konsole (Forts.)

Elementname in XML	Sicht in der Konsole
ReceiverInfo	Hubadmin > Hubkonfiguration > Empfänger. Jeder Empfänger auf der Listenseite wird als "ReceiverInfo" dargestellt.
ProtocolFamilyInfo	Hubadmin > Hubkonfiguration > XML-Formate. Jede Dokumentfamilie wird durch "ProtocolFamilyInfo" dargestellt.
RoutingObjectPkgInfo	Hubadmin > Hubkonfiguration > Dokumentdefinitionen. "RoutingObjectPkgInfo" ist nur ein Platzhalter. Unterhalb dieses Platzhalters befinden sich der Ordner "RoutingObject" und die ZIP-Datei "RoutingObjects.zip". Dies ist die ZIP-Datei, die die gesamten Informationen zum Paket im XML-Format enthält. Die XML-Datei ist identisch mit der Datei in dem über Hubadministrator > Hubkonfiguration > Dokumentdefinitionen > *Pakete hoch-/herunterladen* heruntergeladenen Paket.
ValidObjInteractInfo	Hubadmin > Hubkonfiguration > Dokumentdefinitionen > *Interaktionen verwalten* > *Suchen*. Jede Interaktion in der Liste wird als "ValidObjInteractInfo" dargestellt.
PartnerInfo	Kontenadmin > Partner. "PartnerInfo" steht für jeden Partner in der Liste.
ContactInfo	Kontenadmin > Partner > Kontakte. "ContactInfo" steht für jeden Kontakt in der Liste.
PartnerAddressInfo	Kontenadmin > Partner > Adressen. "PartnerAddressInfo" steht für jede Adresse in der Liste.
ParticipantControlInfo	Hubadmin > Hubkonfiguration > EDI > Initialisierung der Kontrollnummer> *Suchen*. "ParticipantControlInfo" steht für die anfänglichen Kontrollnummern für jeden Partner.
ConnectionProfileInfo	Hubadmin > Hubkonfiguration > EDI > Verbindungsprofil. Jedes Verbindungsprofil auf der Listenseite wird als "ConnectionProfileInfo" dargestellt.
GatewayInfo	Kontenadmin > Partner > Ziele. "GatewayInfo" steht für die Details jedes aufgelisteten Ziels.
DefaultGatewayInfo	Kontenadmin > Partner > Ziele > *Standardziel anzeigen*. Jede Zeile in der Sicht steht für "DefaultGatewayInfo".
CapabilityInfo	Kontenadmin > Partner > B2B-Funktionalität. Die hellen Zeilen in der Baumstruktur mit dem Status "Aktiviert" oder "Inaktiviert" werden durch "CapabilityInfo" dargestellt. Ein Symbol "Attribut bearbeiten" ist enthalten, das die Attribute annehmen kann. Diese Attribute sind in Form von "ROAttrValueInfo" auch Teil von "CapabilityInfo".

Tabelle 9. Zuordnung der XML-Elemente zur Konsole (Forts.)

Elementname in XML	Sicht in der Konsole
ChannelInfo	Kontenadmin > Partnerverbindungen > *Suchen*. Jede aktive Zeile kann aktiviert oder inaktiviert werden. Anfänglich sind alle Verbindungen inaktiviert und zum Erstellen von Verbindungen verfügbar. Nachdem eine Verbindung aktiviert wurde, kann die eigentliche Verbindung erstellt werden. Auch wenn die Verbindung inaktiviert ist, ist sie weiterhin vorhanden. Verbindungen die nicht mindestens ein Mal aktiviert wurden sind keine tatsächlichen Verbindungen.
ProxyConfigInfo	Kontenadmin > Ziele > Forward Proxy-Unterstützung. Jede Zeile auf der Listenseite wird als "ProxyConfigInfo" dargestellt.
EventCodeInfo	Hubadmin > Hubkonfiguration > Ereigniscodes.
AlertInfo	Kontenadmin > Alerts.
CertificateInfo	Kontenadmin > Partner > Zertifikate. "CertificateInfo" stellt die Details der einzelnen Zertifikate dar.
SetMgmtInfo	Kontenadmin > Partner > Zertifikatsgruppen. "SetMgmtInfo" stellt die Details der einzelnen Gruppen dar. Kontenadmin > Partner > Zertifikatsmanagement enthält die Details der Konfigurationen des Zertifikatsmanagements für Pakete und Partner.
SetDestTypeInfo	Kontenadmin > Verbindungen > Partnerverbindungen > Zertifikate. "SetDestTypeInfo" stellt die Details der in den Verbindungen verwendeten Zertifikatsgruppen dar.
GroupInfo	Kontenadmin > Partner > Gruppen. "GroupInfo" steht für jede Gruppe in der Liste.
UserInfo	Kontenadmin > Partner > Benutzer. "UserInfo" steht für jeden Benutzer in der Liste.
FTPUserInfo	Kontenadmin > Profile > Benutzer > FTP-Benutzer. Für den Zugriff auf "FTPUserInfo" können Sie auch zu Kontenadmin > FTP-Benutzerverwaltung navigieren. "FTPUserInfo" steht für jeden FTP-Benutzer in der Liste.
ErrorFlowInfo	Kontenadmin > Fehlerdatenflüsse. "ErrorFlowInfo" steht für jeden Fehlerdatenfluss in der Liste.
SystemAdminInfo	Systemverwaltung
ArchiverInfo	Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Konfigurieren.

Partnermigration exportieren

Das Befehlszeilendienstprogramm ruft die Position der Optionsdatei ab. Die Optionsdatei sollte im XML- oder ZIP-Format vorliegen und muss sich auf demselben System befinden. Die Optionsdatei für den Export verfügt nicht über Attribute für Tags. Liegt die Optionsdatei im ZIP-Format vor, sollte die ZIP-Datei eine XML-Datei enthalten.

Die Eingabe eines POJO (Plain Old Java Object) kann ein Eingabedatenstrom (InputStream) anstelle einer Datei sein. Das Ergebnis wird in einer anderen XML-Datei im selben Ordner unter dem Namen "BCGMigration_HostName.xml" gespeichert. Da dieselben Dateien als Eingabe für die Importfunktion verwendet werden können, wird der allgemeine Name "BCGMigration_HostName.xml" verwendet. Ein POJO kann auch das Dienstprogramm für die Partnermigration aufrufen, um die Konfiguration zu exportieren. Die Optionsdatei oder der Eingabedatenstrom stellt eine der Eingaben dar. Interne Kennungen, wie beispielsweise die ID, rowTS oder Zeitmarke, werden bei der Exportoperation nicht exportiert. Nur die logischen Kennungen, wie beispielsweise der Name oder die Beschreibung werden exportiert. Konfigurationen, wie beispielsweise Handlertypen, die nicht über eine benutzerdefinierte Konfiguration verfügen, werden nicht exportiert. Die Exportoptionsdatei enthält die folgenden Optionen:

1. Partner – Jeder Partner wird durch den Tag identifiziert. Mit dieser Option werden Informationen des Partnerprofils, wie beispielsweise Partnerinformationen, die IP-Adresse, die Geschäfts-IDs, Kontakte und Adressen, exportiert. Wenn die Option für Partner bereitgestellt wird, können auch die folgenden Informationen in inneren Tags bereitgestellt werden:
   a. Gateways – "Alle" oder "Kein(e)". Wenn Gateways exportiert werden, wird auch "Default" exportiert.
   b. B2B-Funktionalität – "Alle" oder "Kein(e)".
   c. Verbindungen – "Alle" oder "Kein(e)".
   d. Anfängliche Kontrollnummern – "Alle" oder "Kein(e)".
   e. Gruppenkonfiguration – "Alle" oder "Kein(e)".
   f. Benutzerkonfiguration – "Alle" oder "Kein(e)".
   g. FTP-Benutzerkonfiguration – "Alle" oder "Kein(e)".
   h. Zertifikate – "Alle" oder "Kein(e)".
   i. Fehlerdatenflusskonfiguration - "Alle" oder "Kein(e)".
   j. Konfiguration der Archivierungsfunktion – "Alle" oder "Kein(e)".
2. Globale Konfiguration
   a. Ziele – "Alle" oder "Kein(e)".
   b. Programm zur Umschlagsgenerierung
   c. Transporttypen
   d. Zieltypen
   e. Handler – "Alle" oder "Kein(e)".
   f. Handlerattribute – "Alle" oder "Kein(e)" für einen Handler.
   g. Aktionen – "Alle" oder "Kein(e)".
   h. Fester Arbeitsablauf – "Alle" oder "Kein(e)".
   i. Umschlagsprofile – "Alle" oder "Kein(e)".
   j. Validierungszuordnungen – "Alle" oder "Kein(e)".
   k. Transformationszuordnungen – "Alle" oder "Kein(e)".
   l. EDI FA-Zuordnungen – "Alle" oder "Kein(e)".
   m. EDI FA-Zuordnungen – "Alle" oder "Kein(e)".
   n. Globale DFDs (Dokumentenflussdefinitionen) – "Alle" oder "Kein(e)".
   o. Interaktionen – "Alle" oder "Kein(e)".
   p. XML-Formatfamilie – "Alle" oder "Kein(e)".
   q. Verbindungsprofil - "Alle" oder "Kein(e)".
   r. Proxykonfiguration – "Alle" oder "Kein(e)".

s. Ereigniscodes – "Alle" oder "Kein(e)".
t. Alertbenachrichtigungen – Alle Alertbenachrichtigungen oder ausgewählte Alertbenachrichtigungen oder Keine Alertbenachrichtigungen.
u. Eigenschaften der Systemverwaltung - "Alle" oder "Kein(e)".

Zu berücksichtigende Aspekte beim Erstellen eigener Importdaten

Wenn Sie beschließen, Ihre eigene Importdatei zu erstellen oder eine Importdatei zu bearbeiten, die vom Exportdienstprogramm erstellt wurde, müssen Sie verschiedene Aspekte berücksichtigen. Ihre XML-Datei muss dem XML-Schema einer Importdatei entsprechen, und es sind Regeln zum Inhalt der Datei zu beachten, die vom XML-Schema nicht gesteuert werden.

Importdatei manuell validieren

Wenn Sie das Migrationsdienstprogramm über die Befehlszeile mithilfe des Partnermigrationsscripts aufrufen, werden Ihre Daten nicht validiert, da die Konsole nicht verwendet wird. Es ist z. B. möglich, eine falsche Partner-ID unter Verwendung eines Migrationsscripts zu erstellen, wohingegen dies unter Verwendung der Konsole nicht möglich ist. Daten, die in die Konsole eingegeben werden, werden von der Konsole validiert. Sie können z. B. eine DUNS-ID, die alphabetische Zeichen enthält, über die Befehlszeile eingeben, dies ist jedoch nicht über die Konsole möglich, da eine DUNS-ID nur numerische Zeichen enthalten darf.

Beachten Sie: Es ist wichtig, sämtliche Daten manuell zu validieren, bevor Sie sie über die Befehlszeile eingeben.

Migration von Konfigurationstypabhängigkeiten

Konfigurierbare Elemente können basierend auf ihren Abhängigkeiten generell in drei Bereiche untergliedert werden, und zwar unabhängige Elemente, abhängige Elemente der ersten Ebene und komplexe abhängige Elemente. Einige Konfigurationstypen haben keine Abhängigkeiten. Beispiel: eine Partnerdefinition kann erstellt werden, ohne auf eine andere konfigurierte Entität im System zu verweisen. Unabhängige Elemente sind konfigurierbare Elemente, die keine Abhängigkeiten haben, bevor sie ins Zielsystem importiert werden.

Andere Konfigurationstypen können nicht eigenständig existieren, da sie von anderen Entitäten im System abhängig sind. Beispiel: Ein Ziel ist mit einem Partner assoziiert; deswegen kann es nur vorhanden sein, wenn auch der Partner vorhanden ist.

Es muss sichergestellt werden, dass Abhängigkeitselemente immer verfügbar sind; daher sind Inhalt und Reihenfolge der Elemente in Export- und Importdateien wichtig. Wenn ein Export ausgeführt wird, muss jedes Element, das über Abhängigkeiten verfügt, nach den Abhängigkeitselementen exportiert werden. In der XML-Datei ist diese Reihenfolge abgebildet. Analog gilt die Logik, dass beim Import die Abhängigkeitselemente vor den abhängigen Elementen importiert werden.

Wenn Sie Konfigurationstypen selektiv exportieren, müssen Sie sicherstellen, dass Sie Abhängigkeitstypen für alle abhängigen Typen angeben. Dies ist auch wichtig, wenn Sie eine Importdatei unter Verwendung der Schemadefinition erstellen. Das Schema erzwingt die Reihenfolge, nicht aber den Inhalt. Wenn Sie also eine Importdatei nicht ordnungsgemäß definieren, z. B. vergessen, ein Abhängigkeitselement bereitzustellen oder ein Abhängigkeitselement nicht ordnungsgemäß definieren, schlägt dieses Element fehl, wenn Sie versuchen, es zu importieren.

Unabhängige Konfigurationselemente

Die folgenden konfigurierbaren Typen sind unabhängig. Andere Konfigurationstypen hängen von diesen Elementen ab, aber die Elemente hängen nicht direkt von anderen Systemelementen ab.

- Zeitplanung für das Programm zur Umschlagsgenerierung.
- Ereigniscodes
- Transporttypen
- Zieltypen
- Umschlagsprofile
- Verbindungsprofile
- Proxy-Konfigurationen
- Validierungszuordnungen
- FA-Zuordnungen
- Partner
- Eigenschaften der Systemverwaltung

Beachten Sie, dass Validierungszuordnungen und FA-Zuordnungen jeweils unabhängige Elemente sind, wenn sie einzeln betrachtet werden. Um von Nutzen zu sein, müssen sie jedoch mit Routing-Objektdefinitionen im System verknüpft werden. Wenn die Routing-Objekte nicht importiert werden, sind die Zuordnungen möglicherweise ohne die Verknüpfungen im System vorhanden. Da es sich hierbei um eine indirekte Abhängigkeit handelt, kann das Migrationsdienstprogramm Zuordnungstypen ohne die Routing-Objekte exportieren und importieren, die auf sie verweisen.

Abhängige Konfigurationselemente

Abhängige Elemente der ersten Ebene sind konfigurierbare Elemente, die von unabhängigen Elementen oder einem abhängigen Element der ersten Ebene abhängig sind. Werden die abhängigen Elemente nicht importiert, schlägt die Importoperation fehl oder sie generiert zur Laufzeit unerwartetes Verhalten. Die folgenden Konfigurationstypen sind abhängige Elemente der ersten Ebene:

- Routing-Objekte

  Routing-Objekte sind vom Import des Umschlagsprofils und der FA-Zuordnung abhängig. Die Validierungszuordnung wird als Teil von Routing-Objekten importiert. Verfügen die Routing-Objekte des Quellensystems über Assoziationen zu einem der Profile oder einer der Zuordnungen, ist das Laufzeitverhalten möglicherweise nicht wie erwartet. Verfügen die Routing-Objekte des Quellensystems nicht über Assoziationen zu Umschlagsprofilen oder FA-Zuordnungen, ist das Laufzeitverhalten wie erwartet, auch wenn die Umschlagsprofile und FA-Zuordnungen nicht importiert werden.
- Handler

  Transporttypen
- FA-Zuordnungsverknüpfungen

  Für FA-Zuordnungsverknüpfungen müssen FA-Zuordnungen und Routing-Objekte importiert werden. Wenn die Routing-Objekte nicht importiert werden, werden die Verknüpfungen mit den vorhandenen Routing-Objekten erstellt. Ist das Routing-Objekt nicht vorhanden, wird keine Verknüpfung erstellt.
- Validierungszuordnungsverknüpfungen

  Für Validierungszuordnungsverknüpfungen müssen Validierungszuordnungen und Routing-Objekte importiert werden. Wenn die Routing-Objekte nicht importiert werden, werden die Verknüpfungen mit den vorhandenen Routing-Objekten erstellt. Ist das Routing-Objekt nicht vorhanden, wird keine Verknüpfung erstellt.
- Fester Arbeitsablauf

Handler
- Variabler Arbeitsablauf (Aktionen)
  Handler
- Kontakte
  Partner
- Adressen
  Partner
- Initialisierung der Kontrollnummer
  Partner
- XML-Familien und -Formate
  Routing-Objekte
- Ziele
  Transporttypen, Zieltypen und Handler
- Transformationszuordnungen
  Routing-Objekte
- Benutzerkonfiguration
  Partner und Gruppenkonfiguration
- FTP-Benutzerkonfiguration
  Benutzerkonfiguration, Gruppenkonfiguration und Partner
- Gruppenkonfiguration
  Partner
- Zertifikate
  Partner, Zertifikatgruppen, Zieltypen und Routing-Objekte

Komplexe abhängige Elemente sind konfigurierbare Elemente, die von unabhängigen Elementen abhängig sind und die komplexer sind als abhängige Elemente der ersten Ebene. Die folgenden Konfigurationstypen sind komplexe abhängige Elemente:

1. Interaktionen – Sind von Routing-Objekten, Aktionen und der Transformationszuordnung abhängig. Wird das Routing-Objekt oder die Aktion nicht importiert, wird die Interaktion ebenfalls nicht importiert.
2. Empfänger – Sind vom Import des Transporttyps, des Zieltyps und des Handlers abhängig. Wird eines der genannten Elemente nicht importiert, wird der Empfänger ebenfalls nicht importiert. Wird der Empfänger ohne die genannten konfigurierbaren Elemente importiert, wird möglicherweise die Importaktivität beendet.
3. Gateways – Sind vom Import des Transporttyps, des Zieltyps und des Handlers abhängig. Wird eines der genannten Elemente nicht importiert, wird das Gateway ebenfalls nicht importiert. Wird das Gateway ohne die genannten konfigurierbaren Elemente importiert, wird möglicherweise die Importaktivität beendet.
4. B2B-Funktionalität – Die B2B-Funktionalität ist eines der komplexesten abhängigen Elemente. Die B2B-Funktionalität ist vom Import des Routing-Objekts, der FA-Zuordnung, des Umschlagprofils und des Partners abhängig. Wird der Partner oder das Routing-Objekt nicht importiert, wird auch die B2B-Funktionalität nicht importiert.
5. Verbindung – Die Verbindung ist das komplexeste abhängige Element. Der Import der Verbindung ist vom Import des Routing-Objekts, der Interaktion, des Partners, der B2B-Funktionalität, des Gateways, der Aktionen und des Verbin-

dungsprofils abhängig. Wird eines der aufgelisteten konfigurierbaren Elemente nicht importiert, führt das Importieren der Verbindungen möglicherweise zur Beendigung der Importaktivität.

6. Alertbenachrichtigungen – Sind von Routing-Objekten, Partnern Ereigniscodes und Kontakten abhängig.
7. Fehlerdatenflusskonfiguration – Ist von Routing-Objekten, Partnern und Ereigniscodes abhängig.
8. Konfiguration der Archivierungsfunktion – Ist von Routing-Objekten und Partnern abhängig.

Bei der Validierungszuordnung und der FA-Zuordnung handelt es sich um Attribute von Routing-Objekten. Die Transformationszuordnung ist ein Attribut einer Interaktion. Die Transformationszuordnung wird in der Detailanzeige der Transformationszuordnung mit einer “ID des Absenderroutingobjekts” und einer “ID des Empfängerroutingobjekts” verknüpft. Die Validierungszuordnung und die FA-Zuordnung können in der jeweiligen Detailanzeige einer bestimmten ID eines Routing-Objekts verknüpft werden. Wird eine Zuordnung verknüpft, kann sie als Option für eine Assoziation verwendet werden. Im folgenden Beispiel wird angenommen, dass das Attribut der Validierungszuordnung für das Routing-Objekt "AS-Binary" konfiguriert ist. "MapA" und "MapB" sind mit "AS-Binary" verknüpft. Enthält die Sicht zum Bearbeiten des Attributs "AS-Binary" (in den Dokumentenflussdefinitionen) eine Validierungszuordnung, ist ihr Wert “Wählen Sie eine Zuordnung in der Liste aus”, und die Dropdown-Liste enthält "MapA" und "MapB". Eine der Zuordnungen kann ausgewählt und als Attribut assoziiert werden.

Das Verknüpfen ermöglicht es also, dass die Zuordnung eine der Optionen sein kann, und das Assoziieren ermöglicht es, dass die Zuordnung zur Laufzeit ausgeführt werden kann. Das Gleiche gilt auch für FA-Zuordnungen und Transformationszuordnungen. Transformationszuordnungen unterscheiden sich geringfügig, da sie anstelle des Routing-Objekts bei der Interaktion verwendet wird. Das Konzept der Verknüpfung und Assoziation ist jedoch identisch.

Reihenfolge von Export und Import

Die generierte XML-Datei beim Export und die Eingabe-XML-Datei beim Import sollten die folgende Reihenfolge befolgen. Die Reihenfolge ist so aufgebaut, dass unabhängige Elemente zuerst importiert werden, gefolgt von Partnern und von Partnern abhängigen Elementen.

1. Programm zur Umschlagsgenerierung (Enveloper)
2. Ereigniscodes (Event Codes)
3. Transporttypen (Transport Types)
4. Zieltypen (Destination Types)
5. Handlerinformationen (Handler Info)
6. Handlerattribute (Handler Attributes)
7. Fester Arbeitsablauf (Fixed Workflow)
8. Aktionen (Actions)
9. Proxykonfiguration (Proxy Configuration)
10. Umschlagsprofile (Envelope Profiles)
11. Verbindungsprofile (Connection Profiles)
12. Validierungszuordnungen (Validation Maps)
13. Transformationszuordnungen (Transform Maps)
14. EDI-Funktionsbestätigungszuordnungen (EDI FA Maps)

15. Ziele (Targets)
16. XML-Formatfamilie (XML format family)
17. Routing-Objekte (Routing Objects)
18. FA-Zuordnungsverknüpfungen (FA Map links)
19. Validierungszuordnungsverknüpfungen (Validation Map links)
20. Transformationszuordnungsverknüpfungen (Transform Map links)
21. Interaktionen (Interactions)
22. Partner (Partners)
23. Gruppenkonfiguration (Group Configuration)
24. Kontakte (Contacts)
25. Adressen (Addresses)
26. Initialisierung der Kontrollnummer (Control Number Initialization)
27. Alertbenachrichtigungen (Alert Notifications)
28. B2B-Funktionalität (B2B Capabilities)
29. Verbindungen (Connections)
30. Gateways (Gateways)
31. Zertifikate (Certificates)
32. Benutzerkonfiguration (User Configuration)
33. FTP-Benutzer (FTP Users)
34. Fehlerdatenflusskonfiguration (Error Flow Configuration)
35. Konfiguration der Archivierungsfunktion (Archiver Configuration)
36. Eigenschaften der Systemverwaltung (System Admin Properties)

BCG- und DIS-Import

Das Migrationsdienstprogramm BCG migriert auch Zuordnungen und Routing-Objekte. Werden für das Produktionssystem Zuordnungen und Routing-Objekte über das DIS-Tool (DIS - Document Information System) importiert, werden diese vom Migrationsdienstprogramm BCG überschrieben, wenn die Option zum Überschreiben aktiviert ist. Wenn Sie die Laufzeitumgebung (Zuordnungen und Routing-Objekte) über den DIS-Client importieren, muss der DIS-Import nach dem BCG-Import ausgeführt werden, damit das Zielproduktionssystem über die zur Ausführungszeit erforderliche Konfiguration verfügt.

Nicht migrierbare Konfigurationen

Die folgenden Konfigurationsdaten werden nicht migriert:

- CPA

  Das CPA (Community Partner Agreement) ist nur für das Produktionssystem gedacht. Es ist nicht im Testsystem vorhanden.
- Berichte und Protokolle werden nicht migriert. Dies sind keine Konfigurationselemente.
- Auch Daten von EDI-Zuordnungen und zugehörige Informationen werden nicht migriert.

Einschränkungen bei Migrationsdienstprogrammen

- Falls Fehler während der Migration auftreten, werden die Transaktionen nicht zurückgesetzt. Beim Import können Fehler aufgrund der folgenden Ursachen auftreten:

- Die exportierte Datei wurde manuell bearbeitet, und erforderliche Informationen wurden entfernt.
- Die manuell erstellte Importdatei enthält nicht alle erforderlichen Informationen für alle Objekte.
- Ein neues konfigurierbares Element wird erstellt, während das Dienstprogramm ausgeführt wird.
- Ein vorhandenes konfigurierbares Element wird aktualisiert, während das Dienstprogramm ausgeführt wird.

- Nur Partnermigrationen und -verbindungen können selektiv migriert werden. Alle anderen Migrationen müssen im Ganzen durchgeführt werden.
- Wenn ein Export von einem Quellensystem ausgeführt wird, das einen anderen Dateisystemtyp als das Empfängersystem verwendet, erfordert das in der exportierten Ausgabe enthaltene XML-Dokument manuelle Aktualisierungen, um etwaige dateisystemspezifische <*targetURL*>-Elemente zu korrigieren. Diese Elemente müssen korrigiert werden, damit sie der Dateisystemumgebung des Empfängers entsprechen, bevor der Import ausgeführt wird.

Forward Proxy-Migration

Forward Proxys werden von HTTP/S-Zielen als Platzhalter während des Importprozesses verwendet. Die Produktionsumgebung (das Empfängersystem) hat möglicherweise nicht die gleichen Proxys wie die Testumgebung (das Quellensystem). Nach dem Import muss der Administrator möglicherweise die zum Proxy gehörenden Informationen ändern, um die Informationen der Produktionsumgebung abzubilden. Wenn die Testumgebung mit der Produktionsumgebung übereinstimmt, muss der Administrator keine Änderungen durchführen.

Anmerkung: Die Option zum Überschreiben ist für Forward Proxys inaktiviert. Wenn also ein Forward Proxy auf dem Empfängersystem vorhanden ist, wird er vom Importdienstprogramm nicht geändert.

Kapitel 7. LDAP-Unterstützung für Authentifizierung der Anmeldung

Zusätzlich zur Verwendung der WebSphere Partner Gateway-Partnerregistry für die Konsolenauthentifizierung unterstützt WebSphere Partner Gateway LDAP (Lightweight Directory Access Protocol) für containerbasierte Authentifizierung, die wiederum das Authentifizierungsverfahren von WebSphere Application Server benutzt. WebSphere Application Server unterstützt drei Authentifizierungstypen:

1. LDAP-Registry.
2. Lokale Betriebssystemregistry.
3. Angepasste Registry.

WebSphere Partner Gateway verwendet den Authentifizierungstyp "LDAP-Registry" von WebSphere Application Server. Durch die Aktivierung der containerverwalteten Authentifizierung in Anwendungen wie WebSphere Partner Gateway, die in WebSphere Application Server implementiert sind, kann der Administrator die Benutzerauthentifizierung an einer zentralen Position außerhalb der WebSphere Partner Gateway-Anwendung verwalten.

LDAP verwenden

Verwenden Sie LDAP, wenn die containerbasierte Authentifizierung ausgewählt ist, in folgenden Fällen:

- Während der Installation.
- Indem Sie das Attribut `bcg.ldap.containerauth`, das sich in **Konsolensystemverwaltung** > **Gemeinsame Merkmale** befindet, auf TRUE (wahr) setzen.

Containerverwaltetes Authentifizierungsverfahren aktivieren

Wenn Sie das containerverwaltete Authentifizierungsverfahren aktivieren möchten, setzen Sie in der Konsole von WebSphere Partner Gateway den Eigenschaftswert `bcg.ldap.containerauth` auf `TRUE` und konfigurieren Sie anschließend die WebSphere Application Server-Einstellung **Globale Sicherheit** so, dass LDAP verwendet wird. Nachdem Sie die Authentifizierung aktiviert haben, werden die Benutzer am LDAP-Server authentifiziert, wenn sie sich bei WebSphere Partner Gateway anmelden.

Anmerkung: Wenn LDAP während des Installationsprozesses aktiviert ist, muss der Administrator sicherstellen, dass der konfigurierte LDAP-Server einen Benutzer mit dem Namen "Hubadmin" erhält; dies ist unabhängig vom gewählten Anmeldetyp ein gültiger Anmeldebenutzername für die LDAP-Authentifizierung.

J2EE-Sicherheit aktivieren

Wenn Sie die J2EE-Sicherheit zusätzlich zur globalen Sicherheit von WebSphere Application Server aktivieren, sollten Sie für Java Runtime Environment (JRE) eine Richtliniendatei erstellen (Beispiel: `wpg.policy`), die die notwendigen Sicherheitsberechtigungen erteilt. Führen Sie die folgenden Schritte aus, um diese Datei zu Java Runtime Environment hinzuzufügen:

1. Erstellen Sie in der Datei `java.security`, die sich im Ordner *WASND_ROOT*`/java/jre/lib/security` befindet, einen Eintrag.

Die Syntax für den neuen Eintrag in der Datei `java.security` lautet:
`policy.url.3=file:///`*`vollständig_qualifizierter_pfad`*`/wpg.policy`.

2. Starten Sie sämtliche Java-Prozesse erneut.

Benutzernamen und -gruppen

Gruppen geben allen Benutzern, die Mitglieder der Gruppe "Hubadmin" sind, Berechtigungen als Superuser. Durch die Gruppen können mehrere Benutzer Hubadministrationszuständigkeiten haben, während gleichzeitig der Kennwortschutz gewährleistet bleibt.

Da für einen LDAP-Server eindeutige Benutzernamen erforderlich sind, müssen die Benutzernamen für WebSphere Partner Gateway ebenfalls eindeutig sein. Wenn Sie einen neuen Benutzer erstellen und der Benutzername bereits im selben oder in einem anderen Partner vorhanden ist, wird die folgende Fehlernachricht angezeigt: `Ein Benutzer mit diesem Namen ist bereits vorhanden.` Geben Sie in diesem Fall einen anderen Benutzernamen in der Konsole ein und fahren Sie fort. Wenn Sie zu einer neueren Version von WebSphere Partner Gateway migrieren, in der die Benutzernamen nicht eingeschränkt sind, werden neben etwaigen doppelt vorhandenen Benutzernamen zwei Sterne (**) angezeigt, um darauf hinzuweisen, dass der betreffende Name bereits im selben oder in einem anderen Partner vorhanden ist. Ändern Sie einen der Benutzernamen, sodass beide eindeutig sind.

Anmerkung: Neue Benutzer und Gruppen, die zum LDAP-Server und zur WAS-Verwaltungskonsole hjinzugefügt werden, müssen auch in der WebSphere Partner Gateway-Konsole hinzugefügt werden, damit sie aktiv werden können.

Verwendung der LDAP-Authentifizierung stoppen

Unter folgenden Umständen müssen Sie die LDAP-Authentifizierung möglicherweise stoppen:

- Der LDAP-Server stoppt oder fällt dauerhaft aus.
- Die containerbasierte Authentifizierung wurde bei der Installation von WebSphere Partner Gateway ausgewählt, der LDAP-Server ist jedoch nicht bereit.

Hinweise für UNIX-Benutzer:

1. UNIX-Benutzer, die DB2 verwenden, müssen sich als Benutzer "db2instance" anmelden und den Benutzernamen "db2instance" und das zugehörige Kennwort verwenden, um das Script auszuführen.
2. UNIX-Benutzer, die Oracle verwenden, müssen sich als Benutzer "Oracle" anmelden und den zum Zeitpunkt der Installation vergebenen Benutzernamen und das zugehörige Kennwort verwenden, um das Script auszuführen.

Führen Sie die folgenden Scripts aus, damit WebSphere Partner Gateway für den Zugriff auf Kennwörter nicht mehr LDAP verwendet, sondern zum Speichern von Kennwörtern stattdessen die WebSphere Partner Gateway-Datenbank benutzt:

- `bcgResetAuthentication.bat` unter Windows.
- `bcgResetAuthentication.sh` unter UNIX.

Das Script erfordert die folgenden Eingabeparameter:

- Benutzer-ID des Datenbankschemaeigners
- Kennwort des Datenbankschemaeigners

Das Script erfordert diese Parameter, um eine Verbindung zur WebSphere Partner Gateway-Datenbank herzustellen.

Anmerkung: Wenn Sie eine DB2-Datenbank verwenden, starten Sie das Script über eine DB2-Befehlszeile.

Das Script befindet sich im Verzeichnis {*dbloader install location*}/scripts/{*database type*}.

Das Script hat folgende Aufgaben:

- Es setzt das Attribut `bcg.ldap.containerauth`, das sich in **Konsolensystemverwaltung** > **Konsolenmerkmale** > **Gemeinsame Attribute** befindet, auf FALSE (falsch).
- Setzt das Kennwort für die Benutzer-ID "Hubadmin" auf den Installationsstandard zurück, wodurch die Datenbank jetzt zum Speichern von Kennwörtern verwendet wird.

Anmerkung: Nachdem die Scripts ausgeführt wurden, müssen alle Kennwörter, die in LDAP konfiguriert wurden, für jeden definierten Benutzer, der die Konsole von WebSphere Partner Gateway verwendet, erneut eingegeben werden.

Beispiel für LDAP-Konfiguration

Im folgenden Abschnitt finden Sie Anleitungen, wie WebSphere Application Server zu konfigurieren ist, damit er eine Verbindung zu den LDAP-Servern herstellen kann, um die implementierte Anwendung zu authentifizieren. In diesem Abschnitt wird die Verwaltung des LDAP-Servers jedoch nicht behandelt, da diese für die Site, auf der er installiert ist, spezifisch ist. Ausführlichere Informationen zur Konfiguration von LDAP-Servern oder der Verwaltung des LDAP-Servers finden Sie in der Dokumentation zu WebSphere Application Server.

WebSphere Application Server für eigenständigen IBM Tivoli Directory Server konfigurieren

Wenn Sie einen eigenständigen LDAP-Server für WebSphere Partner Gateway konfigurieren möchten, können Sie IBM Tivoli Directory Server installieren und WebSphere Application Server so konfigurieren, dass Benutzer im LDAP-Server authentifiziert werden.

1. Installieren Sie IBM Tivoli Directory Server. Befolgen Sie die Anleitungen im Installationshandbuch für IBM Tivoli Directory Server.

   Installationstipps:

   - Der für die Installation des Produkts verwendete Benutzername sollte derselbe sein wie der DB2-Instanzname, und es muss sich um ein Mitglied der Administrator- und DB2Admin-Gruppen handeln.
   - Der Verzeichnisservername sollte derselbe sein wie der DB2-Name.
   - Erstellen Sie einen Benutzer mit dem Namen DB2 und nehmen Sie diesen Benutzernamen in die Administrator- und DB2Admin-Gruppen auf.
   - Melden Sie sich als Benutzer "DB2" an und führen Sie die Installation durch.

   Nachdem Sie IBM Tivoli Directory Server installiert haben, fahren Sie mit dem nächsten Schritt fort und erstellen Sie Benutzer für die LDAP-Server.

2. Starten Sie mit folgendem Befehl den LDAP-Verzeichnisserver:
   ```
   idsslapd -I db2
   ```
3. Starten Sie den mit LDAP gelieferten WebSphere Application Server.
4. Greifen Sie über folgende Adresse auf die Verwaltungsseite für LDAP von WebSphere Application Server zu:
   `http://<ip-adresse>:12000/IDSWebApp/IDSjsp/Login.jsp`
5. Melden Sie sich mit der folgenden Konsolenadministrations-ID an:

   Benutzername: superadmin
   Kennwort: secret
6. Wechseln Sie zu **Console Administrator** > **Manage console server** und fügen Sie Ihren LDAP-Server aus der Liste hinzu.
7. Melden Sie die Konsolenadministrations-ID ab.
8. Wählen Sie Ihren LDAP-Server aus und melden Sie sich mit dem Benutzernamen und Kennwort für den Administrator an.
9. Gehen Sie zu **Server Administration** > **Manage server properties** > **Suffices** und fügen Sie ein Suffix hinzu (z. B. o=ibm, c=us).
10. Klicken Sie auf **Apply**.
11. Gehen Sie zu **Directory Management-Add an entry** und wählen Sie unter **Structural object classes** den Eintrag **Organization** aus.
12. Klicken Sie auf **Next**.
13. Wählen Sie in diesem Bildschirm die Standardwerte (aixAuxAccount) aus und klicken Sie auf **Next**.
14. Legen Sie die folgenden Einstellungen fest:
    ```
    Relative DN='o=ibm'
    Reqd attributes= o='ibm'
    Parent DN= 'c=us'
    ```

    Anmerkung: Die für die Einstellungen angegebenen Werte dienen nur als Beispiele.
15. Klicken Sie auf **Finish**.
16. Erstellen Sie einen Benutzer und fügen Sie einen Verzeichniseintrag unter `'o=ibm,c=us'` hinzu.

    Beispiel: Hinzufügen des Benutzers `'cn=user1,o=ibm,c=us'`:

    a. Wählen Sie die strukturelle Objektklasse `'Person'` aus, sodass Sie `'password'` (Kennwort) als optionales Attribut erhalten.
    b. Geben Sie `sn='user1',cn='user1'` an.
    c. Geben Sie in den optionalen Attributen `password=<kennwort>` an.

    Nachdem Sie den LDAP-Server installiert und einen Benutzer erstellt haben, konfigurieren Sie mit den folgenden Schritten WebSphere Application Server mit dem betreffenden LDAP-Server:
17. Klicken Sie auf **Sicherheit** > **Sichere Verwaltung, Anwendungen und Infrastuktur**.
18. Klicken Sie im rechten Fensterbereich auf der Seite auf **Konfigurationsassistent für Sicherheit**. Der Assistent wird für den ersten von vier Konfigurationsschritten geöffnet.
19. Wählen Sie für Schritt 1 **Anwendungssicherheit aktivieren** aus und klicken Sie auf **Weiter**, um zu Schritt 2 des Konfigurationsassistenten zu gelangen.
20. Wählen Sie für Schritt 2 **Eigenständige LDAP-Registry** aus und klicken Sie auf **Weiter**, um zu Schritt 3 des Konfigurationsassistenten zu gelangen.

21. Geben Sie für Schritt 3 im Assistenten die folgenden Informationen über den LDAP-Server an, der ausgeführt wird, und klicken Sie auf **Weiter**.
    a. Name des primären Benutzers mit Verwaltungsaufgaben: In LDAP erstellter Benutzer (z. B. cn=user1,o=ibm,c=us).
    b. Typ des LDAP-Servers: `IBM_Tivoli Directory_Server`.
    c. Host: *<ip-adresse_des_ldap-servers>*
    d. Port: *<port_ihres_ldap-servers>* (z. B. 389)
    e. Basis-DN: `o=ibm,c=us`
    f. Eindeutiger Name für Bindung: *<ldap-adminname>* (z. B.: cn=root).
    g. Kennwort für Bindung: *<ldap-adminkennwort>*
22. Für Schritt 4 wird eine Zusammenfassung der auf den vorherigen Seiten angegebenen Konfigurationsdaten angezeigt. Überprüfen Sie die Angaben und klicken Sie für die Konfiguration auf **Fertig stellen** und **Speichern**.
23. Starten Sie WebSphere Application Server erneut.

    Stoppen Sie mit folgendem Befehl den Server:

    ```
    startserver <servername> -username <ldap-benutzername>
    -password <ldap-kennwort>
    ```

    Starten Sie den Server mit folgendem Befehl erneut:

    ```
    startserver <servername> -username <ldap-benutzername> -password <ldap-kennwort>
    ```

    Jetzt kann sich der Benutzer mit jedem in IBM Tivoli Directory Server erstellten Benutzernamen anmelden.

LDAP-Benutzer für Verwendung der WebSphere Partner Gateway-Konsole festlegen

Nach der Authentifizierung im LDAP-Server müssen Sie den LDAP-Benutzer der Berechtigungsklasse "Hubuser" zuordnen. Nur Benutzer, die Mitglieder dieser Berechtigungsklasse sind, können nach der Authentifizierung auf die Anwendung zugreifen. Gehen Sie wie folgt vor, um LDAP-Benutzer als Mitglieder dieser Berechtigungsklasse zu definieren:

1. Starten Sie den WebSphere Application Server, für den die Konsolenanwendung implementieren ist.
2. Wählen Sie **Anwendungen** > **Unternehmensanwendungen** aus und klicken Sie dann auf **BCGConsole**.
3. Klicken Sie rechts auf der Seite im Teilfenster **Weitere Merkmale** auf **Sicherheitsaufgabenbereiche zu Benutzern oder Gruppen zuordnen**.
4. Sie können entweder angeben, dass alle erfolgreich authentifizierten Benutzer zu Mitgliedern der Berechtigungsklasse "Hubuser" werden sollen, oder dass nur bestimmte Benutzer aufgenommen werden sollen.
   - Wählen Sie zur Aufnahme aller authentifizierten Benutzer die Option **Alle Authentifizierten** unter der Berechtigungsklasse mit dem Namen **Hubuser** aus.
   - Wenn Sie nur bestimmte Benutzer aufnehmen wollen, klicken Sie auf **Benutzer suchen** und nehmen Sie nur ausgewählte Benutzer als Mitglieder der Berechtigungsklasse **Hubuser** auf.

Kapitel 8. Unterstützung für Internet Protocol Version 6 (IPv6)

Internet Protocol Version 6 (IPv6) ist eine Erweiterung des aktuellen Internet Protocol Version 4 (IPv4). Anders als die Unterstützung von 32-Bit-Adressen durch IPv4 bietet IPv6 Unterstützung von 128-Bit-Adressen. Außer der Änderung des Adressformats sind in der Community Console keine sonstigen Konfigurationsänderungen für IPv6 erforderlich.

Der Unterschied zwischen der Konfiguration von IPv4 und IPv6 ist die geänderte IP-Adresse oder das URL-Format.

- Wenn Sie das Protokoll IPv4 verwenden, schreiben Sie die Adresse wie folgt: `9.183.12.12`.
- Wenn Sie das Protokoll IPv6 verwenden, schreiben Sie die IP-Adresse wie im folgenden Beispiel dargestellt in eckigen Klammern ('[' und ']'): `[0::9.183.12.12]`.
- Wenn Sie das Protokoll IPv6 und eine HTTP-Adresse verwenden, schreiben Sie die IP-Adresse wie im folgenden Beispiel dargestellt in eckigen Klammern ('[' und ']'): `http://[::FFFF:129.144.52.38]:80/index.htm`.
- Wenn Sie das Protokoll IPv6 und eine FTP-Adresse verwenden, schreiben Sie die IP-Adresse wie im folgenden Beispiel dargestellt in eckigen Klammern ('[' und ']'): `ftp://[::FFFF:129.144.52.38]:80/index.htm`.

Tunnelung von IPv6 über IPv4 aktivieren

Das Protokoll IPv6 kann derzeit nicht im gesamten Internet verwendet werden; daher müssen Sie IPv6-Pakete in IPv4 einkapseln und durch Netze, in denen nur IPv4 verfügbar ist, im Tunnelungsverfahren übertragen.

RHEL Linux 3

Gehen Sie wie folgt vor, um auf einer RHEL Linux 3-Plattform die Tunnelung zu aktivieren:

1. Melden Sie sich als Benutzer "Root" an.
2. Fügen Sie die Zeile `add - NETWORKING_IPV6=yes` in der Datei `etc/sysconfig/network` hinzu.
3. Speichern Sie die Datei und schließen Sie sie.
4. Fügen Sie die folgenden Zeilen zur Datei `etc/sysconfig/network-scripts/ifcfg-eth0` hinzu.
   a. `add - IPV6INIT=yes`
   b. `add - IPV6TO4INIT=yes`
5. Speichern Sie die Datei und schließen Sie sie.
6. Setzen Sie den Befehl `ifconfig` über die Eingabeaufforderung ab.

Das System generiert automatisch eine IPv6-Adresse. Verwenden Sie diese Adresse für die Konfiguration von Empfängern und Zielen in WebSphere Partner Gateway.

Windows 2003, Windows XP

Wenn Sie IPv6 auf einem Windows 2003- oder Windows XP-System konfigurieren möchten, befolgen Sie die Richtlinien von Microsoft unter http://www.microsoft.com/windowsserver2003/techinfo/overview/ipv6faq.mspx. Wenn Ihre Windows-Plattform IPv6 unterstützt, wenden Sie sich an Ihren Systemadministrator, um die Tunnelungsfunktion zu aktivieren.

HP-UX 11i

Gehen Sie wie folgt vor, um auf einer HP-UX 11i-Plattform die Tunnelung zu aktivieren:

1. Melden Sie sich als Benutzer "Root" an.
2. Fügen Sie zum Aktivieren der Tunnelung die Zeile `IPV6_TUNNEL="1"` der Datei `/etc/rc.config.d/netconf-ipv6` hinzu.
3. Weisen Sie in der Datei `/etc/rc.config.d/netconf-ipv6` die folgenden Parameter zu:

   ```
   IPV6_DESTINATION[0]=
   IPV6_GATEWAY[0]=" " (wenn auf 1 gesetzt, ist das Gateway remote angebunden,
   wenn auf 0 gesetzt ist das Gateway lokal angebunden)
   IPV6_ROUTE_COUNT[0]=
   IPV6_ROUTE_ARGS[0]=
   ```

   Weitere Informationen finden Sie im Begleittext in der Datei `netconf-ipv6` und auf der Man-Page `route(1m) man`.
4. Speichern Sie die Datei und schließen Sie sie.
5. Sie haben die folgenden beiden Möglichkeiten, damit die Änderungen wirksam werden:
   - Starten Sie das System erneut.
   - Setzen Sie die Befehle `ifconfig` und `route` ab, um die funktional entsprechenden Konfigurationseinstellungen festzulegen.

IPv6 aktivieren

Ändern Sie zur Konfiguration von IPv6 in der WebSphere Application Server-Konsole die Java Virtual Machine-Parameter für die Laufzeitunterstützung. Gehen Sie wie folgt vor, um die Parameter von Java Virtual Machine zu ändern:

1. Melden Sie sich an der Admininistrationskonsole von WebSphere Application Server an.
2. Wechseln Sie zu **Server** > **Anwendungsserver** und wählen Sie **Server** aus.
3. Wählen Sie alle Server aus und ändern Sie mit dem folgendem Prozess die Eigenschaft `java.net.preferIPv4Stack`:
   a. Wählen Sie den Server aus (bcgdocmgr, bcgreceiver oder bcgconsole).
   b. Erweitern Sie auf der Konfigurationsseite im Bereich für die Serverinfrastruktur die Option **Java- und Prozessverwaltung** und wählen Sie **Prozessdefinition** aus.
   c. Wählen Sie auf der Seite für die Konfiguration der Prozessdefinition im Abschnitt mit den weiteren Merkmalen die Option **Java Virtual Machine** aus.
   d. Wählen Sie **Benutzerdefinierte Merkmale** aus.
   e. Ändern Sie die Eigenschaft **java.net.preferIPv4Stack** in *False* (falsch).
   f. Klicken Sie zum Abschluss der Konfiguration auf **Anwenden** und danach auf **Speichern**.

g. Wiederholen Sie diesen Prozess für sämtliche Server.

4. Nachdem Sie die Eigenschaft **java.net.preferIPv4Stack** für alle Server geändert haben, ist eine vollständige Neusynchronisation des Knotens für den vollständig verteilten Modus erforderlich. Wechseln Sie zur Neusynchronisation des Knotens zu **Systemverwaltung** > **Knoten** und wählen Sie **bcgnode** aus. Klicken Sie auf **Vollständige Neusynchronisation**.

   Anmerkung: Die Synchronisation kann ca. 5 bis 10 Minuten beanspruchen.

5. Starten Sie alle Server erneut.

Attribute konfigurieren

Wenn die Workstation, auf der Document Manager installiert ist, mit IPv6 konfiguriert wurde und die Dokumente über ein Ziel gesendet werden, das auf der Internetprotokollversion 6 (IPv6) basiert, muss die IPv6-Adresse der Workstation konfiguriert werden. Gehen Sie wie folgt vor, um die Workstationadresse zu konfigurieren:

1. Melden Sie sich an der WebSphere Partner Gateway-Konsole an.
2. Wechseln Sie zu **Systemverwaltung** > **DocMgr-Verwaltung** > **Attribute des Zustellmanagers**.
3. Klicken Sie auf das Symbol **Eigenschaften der Veröffentlichungsinformationen bearbeiten**.
4. Geben Sie die IPv6-Adresse der lokalen Workstation, auf der der Hub ausgeführt wird, in der Eigenschaft "bcg.router.ipv6.address" an.

   Anmerkung: Wenn mehr als eine Instanz von Document Manager vorhanden ist, lassen Sie die Eigenschaft "bcg.router.ipv6.address" frei.

5. Klicken Sie auf **Speichern**.
6. Wechseln Sie für den Empfänger zu **Systemverwaltung** > **Empfängerverwaltung** > **Andere**.
7. Geben Sie die IPv6-Adresse der lokalen Workstation, auf der der Hub ausgeführt wird, in der Eigenschaft "bcg.receiver.ipv6" an.

   Anmerkung: Wenn mehr als eine Instanz des Empfängers vorhanden ist, lassen Sie die Eigenschaft "bcg.receiver.ipv6" frei.

8. Klicken Sie auf **Speichern**.

Kapitel 9. Zielwarteschlange verwalten

In der Zielwarteschlange können Dokumente angezeigt werden, die in der Warteschlange stehen, um von einem beliebigen Ziel im System übermittelt zu werden. Außerdem haben Sie folgende Möglichkeiten:

- Alle Partnerziele anzeigen, für die sich Dokumente in der Warteschlange für die Zustellung befinden.
- Dokumente in einer Warteschlange anzeigen.
- Ziele aktivieren oder inaktivieren.

Die Zielwarteschlange enthält Nachrichten, die darauf warten, von WebSphere Partner Gateway an Partnerziele gesendet zu werden.

Die Zielwarteschlange kann verwendet werden, um sicherzustellen, dass eilige Dokumente nicht in der Warteschlange aufgehalten werden. Außerdem können Sie sie nutzen, um sicherzustellen, dass die maximale Anzahl an Dokumenten, die in die Warteschlange gestellt werden können, nicht überschritten wird. Mit der Zielwarteschlange haben Sie die folgenden Möglichkeiten:

- Eine Liste aller Ziele anzeigen, die Dokumente enthalten, welche sich für die Zustellung in einer Warteschlange befinden.
- Ein Dokument anzeigen, das sich zu lange in einer Zielwarteschlange befunden hat (30 Sekunden oder länger). Darüber hinaus können Sie die Dokumentdetails anzeigen, um Dokumente in der Warteschlange zu berichtigen.

  Anmerkung: Wenn Sie ein FTP-Scriptingziel mit einem Intervall- oder Kalenderzeitplan implementieren, verbleiben Dokumente über einen längeren Zeitraum in dieser Warteschlange und werden erst dann entfernt, wenn das für sie definierte Intervall abgelaufen ist bzw. das definierte Datum und die entsprechende Uhrzeit erreicht sind. Diese Funktionsweise ist beabsichtigt und die Dokumente sollten nicht vorzeitig aus der Warteschlange entfernt werden.
- Zieldetails anzeigen, um die ordnungsgemäße Verarbeitung sicherzustellen. Dokumente, die sich in einer Zielwarteschlange stauen, können ein Hinweis auf Fehler im Zustellmanager oder im Ziel sein.
- Zielstatus bestätigen. Ein Ziel im Offlinestatus bewirkt, dass Dokumente in der Warteschlange erfasst werden, bis das Ziel in den Onlinestatus versetzt wird. Der Zielstatus wirkt sich nicht auf die Verbindungsfunktionalität aus, und die Dokumente werden weiter verarbeitet und für die Zustellung in die Warteschlange gestellt.
- Über die Felder **Partnername** und **Ziel** können Sie die Größe der Zielwarteschlangenliste begrenzen.

Zielwarteschlange anzeigen

Verwenden Sie das folgende Verfahren, um eine Liste der Dokumente anzuzeigen, die sich in der Zielwarteschlange befinden:

1. Wählen Sie **Anzeigen** > **Zielwarteschlange** aus. In der Community Console wird das Fenster **Zielwarteschlange** geöffnet.
2. Geben Sie die Parameter wie in Tabelle 10 auf Seite 96 gezeigt ein.

Tabelle 10. Fenster "Zielwarteschlange"

Kriterien	Beschreibung
Partnername	Wenn Sie dieses Feld ausfüllen, haben Sie die folgenden Möglichkeiten: 1. Den Partnernamen angeben. 2. Geben Sie in diesem Feld einen Teil des Partnernamens an und klicken Sie auf **Partner anzeigen**. Wählen Sie den Partner in der Partnerliste aus. 3. Geben Sie das Platzhalterzeichen * an und klicken Sie auf **Partner anzeigen**. Wählen Sie den Partner in der Partnerliste aus. Wenn Sie auf **Partner anzeigen** klicken, wird auf der Seite das Feld **Partner** angezeigt. Im Feld **Partner** werden alle verfügbaren Partner in alphabetischer Reihenfolge angezeigt.
Ziel	Das erste Element in dieser Liste ist `Alle`, welches standardmäßig ausgewählt wird. Der verbleibende Teil der Liste ist eine sortierte Liste der Zieltransporte. In dieser Liste können Sie nur ein einziges Ziel auswählen. Der Standardwert ist `Alle`. **Anmerkung:** Die Zieladressenliste wird automatisch mit den ausgewählten Partnerzielen gefüllt, und die Liste wird in alphabetischer Reihenfolge dargestellt.
In Warteschlange mindestens	Mindestanzahl an Minuten, die ein Dokument bereits in der Zielwarteschlange steht. Wenn z. B. "sechs Minuten" ausgewählt wurde, werden alle Ziele angezeigt, die Dokumente enthalten, welche sechs Minuten oder länger auf die Zustellung gewartet haben. Der Standardwert ist `0`.
Sortieren nach	Sortiert die Suchergebnisse nach Partner- (Standard) oder Zielname.
Aktualisieren	Schalten Sie die Aktualisierung ein oder aus (Standard).
Minimum in Warteschlange	Mindestanzahl an Dokumenten in einer Zielwarteschlange. Der Standardwert ist `1`.
Richtung	Klicken Sie auf **Aufsteigend**, um Dokumente beginnend mit der ältesten Zeitmarke oder dem Ende des Alphabets anzuzeigen, oder klicken Sie auf **Absteigend**, um Dokumente anzuzeigen, die mit der jüngsten Zeitmarke oder dem Anfang des Alphabets beginnen.
Aktualisierungsrate	Anzahl der Sekunden, die die Community Console wartet, bis sie die angezeigten Daten aktualisiert.

3. Klicken Sie auf **Suchen**. Das System sucht nach allen Dokumenten im Ziel, die mit Ihren Suchkriterien übereinstimmen. In **Tabelle 11** werden die nach der Suche zurückgegebenen Informationen aufgelistet.

Tabelle 11. Ergebnisse nach der Zielwarteschlangensuche

Kriterien	Beschreibung
Partner	Geschäftspartner, der dem Ziel zugeordnet ist.
Ziel	Name des Ziels.
In Warteschlange	Anzahl der Dokumente, die in der Zielwarteschlange auf die Zustellung warten. Link zu Zieldetails.
Status	Gibt an, ob das Ziel sich im Onlinestatus oder Offlinestatus befindet.

Anmerkung: Die Community Console zeigt ein Ziel nur dann an, wenn das Ziel alle Anforderungen in den Suchkriterien erfüllt.

Dokumente in Warteschlange anzeigen

Gehen Sie wie folgt vor, um für einen bestimmten Partner die Dokumente in der Warteschlange anzuzeigen:

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Klicken Sie im Fenster **Zielwarteschlange - Suche** auf **Dokumentensuche**.
3. Geben Sie im Fenster **Dokumente in Warteschlange - Suche** die Suchkriterien an (siehe Tabelle 12).

Tabelle 12. Fenster "Dokumente in Warteschlange - Suche"

Kriterien	Beschreibung
Partnername	Wenn Sie dieses Feld ausfüllen, haben Sie die folgenden Möglichkeiten: 1. Den Partnernamen im Feld angeben. 2. Geben Sie in diesem Feld einen Teil des Partnernamens an und klicken Sie auf **Partner anzeigen**. Wählen Sie den Partner in der Liste aus. 3. Geben Sie das Platzhalterzeichen * an und klicken Sie auf **Partner anzeigen**. Wählen Sie den Partner in der Partnerliste aus. **Anmerkung:** Wenn Sie auf **Partner anzeigen** klicken, wird auf der Seite das Feld **Partner** angezeigt. Im Feld **Partner** werden alle verfügbaren Partner in alphabetischer Reihenfolge angezeigt.
Ziel	Das erste Element in dieser Liste ist `Alle`, welches standardmäßig ausgewählt wird. Der verbleibende Teil der Liste ist eine sortierte Liste der Zieltransporte. In dieser Liste können Sie nur ein einziges Ziel auswählen. Der Standardwert ist `Alle`. **Anmerkung:** Die Zieladressenliste wird automatisch mit den ausgewählten Partnerzielen gefüllt und die Liste wird in einer alphabetisch geordneten Liste dargestellt.
Sortieren nach	Wählen Sie aus, ob die Liste nach Partnern (Standard), nach Zielen, Referenz-ID oder nach der Zeitmarke für das Einreihen in die Warteschlange (d. h. dem Zeitpunkt, zu dem das Dokument das letzte Mal gesendet wurde) sortiert werden soll.
Referenz-ID	Geben Sie die eindeutige Identifikationsnummer an, die dem Dokument vom System zugeordnet wird.
Richtung	Klicken Sie auf **Aufsteigend**, um Dokumente beginnend mit der ältesten Zeitmarke oder dem Anfang des Alphabets anzuzeigen, oder klicken Sie auf **Absteigend**, um Dokumente anzuzeigen, die mit der jüngsten Zeitmarke oder dem Ende des Alphabets beginnen.
Dokument-ID	Geben Sie die eindeutige Identifikationsnummer an, die dem Dokument vom Quellenpartner zugeordnet wird.
Ergebnisse pro Seite	Gibt die Anzahl der angezeigten Dokumente auf einer Seite an.
Maximal zulässige Anzahl an Dokumenten	Gibt die Anzahl der anzuzeigenden Datensätze an.

4. Klicken Sie auf **Suchen**. Die Ergebnisse der Warteschlangensuche werden angezeigt.

Verarbeitung von Dokumenten aus Zielwarteschlange stoppen

Mit der Zielwarteschlange können Sie eine Anforderung an WebSphere Partner Gateway senden, die Verarbeitung von Dokumenten zu stoppen. Wenn Sie auf das Symbol **Prozess stoppen** klicken, wird Ihre Anforderung übergeben, die Verarbeitung des Dokuments zu stoppen, und der neue angezeigte Status des Dokuments

lautet **Stopp übergeben**. Dieser Status bedeutet, dass die Anforderung zum Stoppen der Verarbeitung des Dokuments übergeben wurde.

In der folgenden Prozedur wird beschrieben, wie die Verarbeitung der Dokumente gestoppt werden kann.

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Klicken Sie im Fenster **Zielwarteschlange** auf **Dokumentensuche**.
3. Geben Sie in dem Fenster die Parameter ein (siehe Tabelle 12 auf Seite 97).
4. Klicken Sie auf **Suchen**. Die Ergebnisse der Warteschlangensuche werden angezeigt.
5. Klicken Sie auf das Symbol **Prozess stoppen**, um die Verarbeitung des Dokuments zu stoppen.

Anmerkung: Wenn das Dokument bereits von Document Manager verarbeitet wurde, wenn Sie auf das Symbol **Prozess stoppen** klicken, hat die Aktion zum Stoppen des Prozesses keinerlei Auswirkung.

Zieldetails anzeigen

Wenn Sie Informationen zu einem bestimmten Ziel einschließlich einer Liste der Dokumente in der Warteschlange anzeigen möchten, verwenden Sie die folgende Prozedur:

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Geben Sie über das Fenster **Zielwarteschlange** die Suchkriterien ein (siehe Tabelle 10 auf Seite 96).
3. Klicken Sie auf **Suchen**.
4. Klicken Sie in der Liste der Ziele auf den Link für die Dokumentenzahl in der Spalte **In Warteschlange**, um das Fenster **Dokumente in Warteschlange - Suche** zu öffnen.
5. Klicken Sie im Fenster **Dokumente in Warteschlange - Suche** auf **Suchen**. Die Details des Ziels und eine Liste der Dokumente in der Warteschlange werden angezeigt.

Zielstatus ändern

Verwenden Sie die folgende Prozedur, um ein Ziel in den Onlinestatus oder den Offlinestatus zu versetzen:

1. Klicken Sie auf **Anzeigen** > **Zielwarteschlange**.
2. Geben Sie über das Fenster **Zielwarteschlange** die Suchkriterien ein (siehe Tabelle 10 auf Seite 96).
3. Klicken Sie auf **Suchen**.
4. Klicken Sie in der Liste der Ziele auf den Link für die Dokumentenzahl in der Spalte **In Warteschlange**. Es werden die Zieldetails und eine Liste der Dokumente in der Warteschlange angezeigt.
5. Klicken Sie in **Zielinformationen** auf **Online**, damit das Ziel in den Offlinestatus gesetzt wird, oder auf **Offline**, damit das Ziel in den Onlinestatus gesetzt wird (Sie müssen als Hubadmin angemeldet sein, um den Zielstatus zu ändern).

Kapitel 10. Dokumentenflüsse analysieren

Mit dem Dokumentanalysetool erhalten Sie einen detaillierten Überblick über die Anzahl der Dokumente im System, sortiert nach deren Status:

- Empfangen
- Wird ausgeführt
- Fehlgeschlagen
- Erfolgreich

Sie können die Suche anhand folgender Kriterien eingrenzen:

- Datum
- Zeit
- Prozesstyp (Empfänger- oder Absenderprozess)
- Betriebsmodus
- Protokoll
- Dokumenttyp
- Prozessversion

Der Dokumentvolumenbericht unterstützt Sie dabei, den Fluss Ihrer Geschäftsdokumente zu verwalte, zu verfolen und zu berichtigen, indem die fehlgeschlagenen Dokumente gesucht und angezeigt werden und die Ursache für ihr Fehlschlagen untersucht wird. Der Bericht zeigt das Volumen der vom System innerhalb eines bestimmten Zeitraums verarbeiteten Dokumente an und kann angezeigt, gedruckt, gespeichert (exportiert) und an Mitarbeiter gesendet werden. Sie können den Bericht so anpassen, dass Informationen auf der Basis bestimmter Suchkriterien angezeigt werden.

Das Tool "Partnerverbindung testen" wird verwendet, um die Verbindung zum Ziel zu testen.

In diesem Kapitel werden die folgenden Produktmerkmale behandelt:

- „Tool 'Dokumentanalyse'"
- „Dokumentvolumenbericht" auf Seite 101
- „Partnerverbindung testen" auf Seite 103
- „EDI-Berichte" auf Seite 107
- „FTP-Berichte" auf Seite 110

Tool 'Dokumentanalyse'

Mit dem Dokumentanalysetool erhalten Sie einen detaillierten Überblick über die Anzahl der Dokumente im System nach deren Status und innerhalb eines bestimmten Zeitraums.

Verwenden Sie die Suchkriterien, um fehlgeschlagene Dokumente zu suchen und die Fehlerursache zu untersuchen.

Dokumentstatus im System anzeigen

Die folgende Tabelle beschreibt die unterschiedlichen Dokumentstatus.

Tabelle 13. Dokumentstatus

Status	Beschreibung
Empfangen	Das Dokument wurde vom System empfangen und wartet auf die Verarbeitung.
Wird ausgeführt	Das Dokument befindet sich derzeit in einem der folgenden Verarbeitungsschritte: • **Unvollständig**. Beispiel: Das System wartet auf weitere Dokumente. • **Datenvalidierung**. Beispiel: Das System prüft den Dokumentinhalt. • **Konvertierung**. Beispiel: Das System konvertiert das Dokument in ein anderes Protokoll. • **Warteschlange**. Beispiel: Das Dokument wartet darauf, an den externen Partner oder internen Partner weitergeleitet zu werden.
Fehlgeschlagen	Die Dokumentverarbeitung wurde aufgrund von Fehlern im System, in der Datenvalidierung oder aufgrund von Duplikaten unterbrochen.
Erfolgreich	Die abschließende Nachricht, mit der die Dokumentverarbeitung abgeschlossen wird, wurde vom System an den Empfängerpartner übertragen.

Dokumente im System anzeigen

Die folgende Prozedur beschreibt, wie Sie Dokumente im System anzeigen:

1. Klicken Sie auf **Tools** > **Dokumentanalyse**.
2. Wählen Sie im Fenster **Dokumentanalyse - Suche** die Suchkriterien in den Listen aus.

   In Tabelle 14 werden die Werte beschrieben, die Sie angeben können, um festzulegen, welche Dokumente angezeigt werden sollen.

Tabelle 14. Dokumentsuchkriterien

Wert	Beschreibung
Startdatum und Zeit	Datum und Uhrzeit des Prozessbeginns.
Enddatum und Zeit	Datum und Uhrzeit des Prozessendes.
Quellenpartner	Der Partner, der den Geschäftsprozess eingeleitet hat (nur für internen Partner).
Empfängerpartner	Der Partner, der den Geschäftsprozess empfangen hat (nur für internen Partner).
Suchen in	Suche im Dokumenttyp des Absenders oder Dokumenttyp des Empfängers.
Betriebsmodus	Zum Beispiel "Alle", "Produktion", "Test", "CPS-Partner" oder "CPS-Manager". Der Typ "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen.
Paket	Beschreibt Dokumentformat, Paket, Verschlüsselung und Inhaltstypkennung.
Protokoll	Verfügbares Protokoll des Dokuments für die Partner.
Dokumenttyp	Bestimmter Geschäftsprozess.
Sortieren nach	Sortiert die Ergebnisse nach dem Namen des absendenden oder des empfangenden Partners.

Tabelle 14. Dokumentsuchkriterien (Forts.)

Wert	Beschreibung
Aktualisieren	Steuert, ob die Suchergebnisse regelmäßig aktualisiert werden sollen (nur für internen Partner).
Aktualisierungsrate	Steuert, wie oft die Suchergebnisse aktualisiert werden sollen (wird nur vom internen Partner verwendet).

3. Klicken Sie auf **Suchen**. Das System öffnet die Anzeige **Dokumentanalyse - Zusammenfassung**.

Prozess- und Ereignisdetails anzeigen

Die folgende Prozedur beschreibt, wie Sie Prozesse und Ereignisdetails anzeigen:

1. Klicken Sie auf **Tools** > **Dokumentanalyse**. Das System öffnet das Fenster **Dokumentanalyse - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System öffnet die Anzeige **Dokumentanalyse - Zusammenfassung**.
4. Klicken Sie neben den Quellen- und Empfängerpartnern, die Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt für die ausgewählten Partner eine Liste aller Dokumente an. Der Dokumentbestand wird in Spalten nach Dokumentverarbeitungsstatus angeordnet.
5. Wählen Sie unter den verschiedenen Dokumentenflüssen, die unter **Dokumentanalyse - Zusammenfassung** aufgelistet werden, aus der Spalte **Empfangen**, **Wird ausgeführt**, **Fehlgeschlagen** oder **Erfolgreich** den Link für die Menge aus. Das System stellt die Dokumentverarbeitungsdetails im Dokumentanalysebericht dar. Wenn Sie **Fehlgeschlagen** ausgewählt haben, umfasst der Bericht auch eine Zusammenfassung der Dokumentereignisse.

Dokumentvolumenbericht

Der Dokumentvolumenbericht ist ein wertvolles Tool zum Verwalten, Verfolgen und Beheben von Fehlern im Fluss Ihrer Geschäftsdokumente. Der Bericht zeigt das Volumen verarbeiteter Dokumente durch das System innerhalb eines bestimmten Zeitraums an. Dieser Bericht kann angezeigt, gedruckt, gespeichert (exportiert) und an Mitarbeiter gesendet werden.

Sie können den Bericht so anpassen, dass Informationen auf der Basis bestimmter Suchkriterien angezeigt werden.

Der Dokumentvolumenbericht zeigt die Anzahl der Dokumente, die derzeit verarbeitet werden, nach ihrem Status an:

Tabelle 15. Dokumentstatus

Wert	Beschreibung
Insgesamt empfangen	Gesamtzahl der vom System empfangenen Dokumente.
Wird ausgeführt	Dokumente, die ausgeführt werden, werden getestet und geprüft. Es wurde kein Fehler festgestellt, aber der Prozess ist noch nicht abgeschlossen.
Fehlgeschlagen	Die Dokumentverarbeitung wurde aufgrund eines Fehlers unterbrochen.

Tabelle 15. Dokumentstatus (Forts.)

Wert	Beschreibung
Erfolgreich	Die abschließende Nachricht, mit der die Dokumentverarbeitung abgeschlossen wird, wurde vom System an den Empfängerpartner übertragen.

Verwenden Sie diesen Bericht, um die folgenden Tasks auszuführen:

- Feststellen, ob Schlüsselgeschäftsprozesse abgeschlossen wurden.
- Trends im Verarbeitungsvolumen zwecks Kostenkontrolle verfolgen.
- Prozessqualität verwalten, Erfolge und Fehler.
- Prozesseffektivität überwachen.

Dokumentvolumenbericht erstellen

Die folgende Prozedur beschreibt, wie Sie einen Dokumentvolumenbericht erstellen:

1. Klicken Sie auf **Tools** > **Dokumentvolumenbericht**. Das System öffnet das Fenster **Dokumentvolumenbericht - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.

Tabelle 16. Dokumentvolumenbericht - Suchkriterien

Wert	Beschreibung
Startdatum und Zeit	Datum und Uhrzeit des Prozessbeginns.
Enddatum und Zeit	Datum und Uhrzeit des Prozessendes.
Quellenpartner	Der Partner, der den Geschäftsprozess eingeleitet hat (nur für internen Partner).
Empfängerpartner	Der Partner, der den Geschäftsprozess empfangen hat (nur für internen Partner).
Suchen in	Suche im Dokumenttyp des Absenders oder Dokumenttyp des Empfängers.
Betriebsmodus	Produktion oder Test. Der Typ "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen.
Paket	Beschreibt Dokumentformat, Paket, Verschlüsselung und Inhaltstypkennung.
Protokoll	Typ des Prozessprotokolls, z. B. XML, EDI, Flachdatei.
Dokumenttyp	Bestimmter Geschäftsprozess.
Sortieren nach	Suchergebnisse nach diesem Kriterium sortieren (Dokumenttyp oder Empfängerdokumenttyp).
Ergebnisse pro Seite	Anzahl der angezeigten Datensätze pro Seite.

3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.

Dokumentvolumenbericht exportieren

1. Klicken Sie auf **Tools** > **Dokumentvolumenbericht**. Das System öffnet das Fenster **Dokumentvolumenbericht - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.
4. Klicken Sie auf das Symbol **Bericht exportieren**, um den Bericht zu exportieren. Navigieren Sie zu der Speicherposition, an der Sie die Datei speichern möchten.

Anmerkung: Berichte werden als Dateien mit durch Kommata getrennte Werte gespeichert (CSV - Comma-Separated Value).

Berichte drucken

1. Klicken Sie auf **Tools** > **Dokumentvolumenbericht**. Das System öffnet das Fenster **Dokumentvolumenbericht - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt den Bericht an.
4. Klicken Sie auf das Symbol **Drucken**, um den Bericht zu drucken.

Partnerverbindung testen

Die Funktion **Partnerverbindung testen** wird verwendet, um das Ziel oder den Web-Server zu testen. Falls Sie der interne Partner sind, können Sie außerdem einen bestimmten Partner auswählen. Der Test besteht darin, eine leere POST-Anforderung an ein Ziel oder eine URL zu senden. Beispiel: Bei der Anforderung wird ähnlich vorgegangen wie bei der Eingabe der Webadresse von Yahoo (www.yahoo.com) in das Adressfeld Ihres Browsers. Es wird nichts gesendet, es handelt sich um eine leere Anforderung. Die vom Ziel oder dem Web-Server empfangene Antwort gibt deren Status an:

- Wenn eine Antwort zurückgegeben wird, ist der Server aktiv.
- Wenn nichts zurückgegeben wird, ist der Server inaktiv.

Wichtig: Die Funktion **Partnerverbindung testen** arbeitet mit HTTP, sodass keine Verbindungsparameter erforderlich sind.

Gehen Sie wie folgt vor, um eine Partnerverbindung zu testen:

1. Klicken Sie auf **Tools** > **Partnerverbindung testen**.
2. Wählen Sie im Fenster **Partnerverbindung testen** die Testkriterien in den Listen aus.

Tabelle 17. Werte für 'Partnerverbindung testen'

Wert	Beschreibung
Empfängerpartner	Der Name eines bestimmten zu testenden Empfängerpartners (nur für internen Partner).
Absenderpartner	Der Name eines bestimmten zu testenden Absenderpartners (nur für internen Partner). Dieses Feld ist nur verfügbar, wenn im Befehlsfeld die Option **PING ebMS** ausgewählt wurde.
Ziel	Zeigt die verfügbaren Ziele für den ausgewählten Empfängerpartner an.
URL	Wird dynamisch auf der Basis des ausgewählten Ziels gefüllt.
Befehl	POST, GET oder PING ebMS. Weitere Informationen zu PING ebMS finden Sie im Abschnitt „ebMS-Partner mit Ping überprüfen".

3. Klicken Sie auf **Test**. Das System zeigt die Testergebnisse an. Informationen zu dem zurückgegebenen Statuscode finden Sie im Abschnitt „Ergebniscodes des Web-Servers" auf Seite 104.

ebMS-Partner mit Ping überprüfen

Über die Seite **Partnerverbindung testen** können Sie ebMS-Partner mit Ping überprüfen. Dies bedeutet, dass Sie eine Pingnachricht an einen Partner senden können,

und falls der Partner aktiv und empfangsbereit ist, antwortet er mit einer Pongnachricht. Sobald Sie ein CPA hochladen, wird die Verbindung für die Ping- und Pongnachrichten erstellt.

Die Überprüfung mit Ping funktioniert nur, wenn mit dem beteiligten Partner entsprechende Verbindungen definiert wurden. Nähere Einzelheiten finden Sie im Abschnitt zum Überprüfen von ebMS-Partnern mit Ping im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Führen Sie die folgenden Schritte aus, um einen ebMS-Partner mit Ping zu überprüfen:

1. Klicken Sie auf **Tools** > **Partnerverbindung testen**.
2. Wählen Sie als **Befehl PING ebMS** aus.
3. Wählen Sie einen **Absenderpartner** und einen **Zielpartner** aus.
4. Wählen Sie optional ein **Ziel** aus, oder geben Sie eine **URL** an.
5. Klicken Sie auf **Testen**, um eine Pingnachricht zu senden.

Wenn Sie den Status der Pingnachricht ermitteln möchten, klicken Sie auf **Ping-Status**. Anschließend wird der Status der letzten Pinganforderung unter **Ergebnisse** angezeigt.

Anmerkung: Die letzte Pinganforderung wurde möglicherweise durch das erneute Senden eines vorhandenen Pingdokuments über **Partnerverbindung testen** oder über eine Dokumentanzeige eingeleitet.

Ergebniscodes des Web-Servers

In den folgenden Abschnitten werden die Serverergebniscodes erläutert:

Codes von 200 - 299

- 200 - OK

  Übertragung erfolgreich. Dies ist kein Fehler.
- 201 - Created (Erstellt)

  Die Anforderung wurde erfüllt und hat die Erstellung einer neuen Ressource bewirkt. Auf die neu erstellte Ressource kann durch URLs verwiesen werden, die im URL-Headerfeld der Antwort zurückgegeben wurden. Die zutreffendste URL für die Ressource wird durch ein Location-Headerfeld angegeben.
- 202 - Accepted (Akzeptiert)

  Die Anforderung wurde zur Verarbeitung akzeptiert, die Verarbeitung ist jedoch noch nicht beendet.
- 203 - Non-Authoritative Information (Nicht autoritative Informationen)

  Die zurückgegebenen META-Informationen im Entity-Header sind nicht der endgültige Satz, der vom Quellenserver bereitgestellt wird, sondern stammen von einer lokalen Kopie oder einer Kopie eines Fremdanbieters.
- 204 - No Content (Kein Inhalt)

  Der Server hat die Anforderung erfüllt, es sind jedoch keine neuen Informationen zum Rücksenden vorhanden.
- 206 - Partial Content (Rückgabe eines Teilinhalts)

  Sie haben eine Anzahl an Byte in der Datei angefordert, die hier ausgegeben werden. Dies ist neu in HTTP 1.1.

Codes von 300 - 399

- 301 - Moved Permanently (Permanent verschoben)

  Der angeforderten Ressource wurde dauerhaft eine neue URL zugeordnet, und künftige Verweise auf diese Ressource sollten über eine der zurückgegebenen URLs erfolgen.

- 302 - Moved Temporarily (Temporär verschoben)

  Die angeforderte Ressource befindet sich momentan unter einer neuen URL. Umleitung an eine neue URL. Die ursprüngliche Seite wurde verschoben. Dies ist kein Fehler, da die meisten Browser die neue Seite im Hintergrund abrufen, sobald dieses Ergebnis ausgegeben wird.

Codes von 400 - 499

- 400 - Bad Request (Fehlerhafte Anforderung)

  Die Anforderung wurde möglicherweise vom Server nicht verstanden, da ihre Syntax fehlerhaft ist. Die ungültige Anforderung wurde vom Client ausgegeben.

- 401 - Unauthorized (Nicht berechtigt)

  Diese Anforderung erfordert eine Benutzerauthentifizierung. Die Antwort muss ein WWW-Authentifizierungs-Headerfeld enthalten sowie eine auf die angeforderte Quelle anwendbare Abfrage. Der Benutzer hat ein Dokument angefordert, aber keinen gültigen Benutzernamen bzw. kein gültiges Kennwort angegeben.

- 402 - Payment Required (Zahlung erforderlich)

  Dieser Code wird derzeit nicht unterstützt; er ist jedoch für künftige Zwecke reserviert.

- 403 - Forbidden (Verboten)

  Der Server hat die Anforderung verstanden, lehnt das Ausführen dieser Anforderung jedoch aus einem nicht näher angegebenen Grund ab. Zu diesem Dokument wird der Zugriff explizit verweigert. (Dies kann geschehen, weil der Web-Server eventuell keinen Lesezugriff auf die von Ihnen angeforderte Datei hat.) Der Server lehnt es ab, Ihnen diese Datei zu schicken. Möglicherweise wurde die Berechtigung explizit inaktiviert.

- 404 - Not Found (Nicht gefunden)

  Der Server hat keine Daten gefunden, die mit der angeforderten URL übereinstimmen. Diese Datei ist nicht vorhanden. Diese Nachricht erhalten Sie, wenn Sie eine fehlerhafte URL in Ihren Browser eingeben. Eventuell wird dieser Code auch gesendet, wenn der Server eingestellt wurde, das Dokument vor unberechtigten Benutzern zu schützen, indem er diesen mitteilt, dass Dokument sei nicht vorhanden. Fehler aus dem Codebereich 404 resultieren aus Anforderungen nach bestimmten Seiten, die nicht vorhanden sind, und entstehen u. a. aus folgenden Gründen:

  – Eine URL wurde falsch eingegeben.
  – Ein Lesezeichen zeigt auf eine nicht mehr vorhandene Datei.
  – Die Suchmaschinen suchen nach der Datei `robots.txt` (die zur Markierung von Seiten verwendet wird, welche jedoch nicht von Suchmaschinen indexiert werden dürfen).
  – Die Dateinamen werden vom Benutzer nur geraten.
  – Es sind fehlerhafte Links von Ihrer Site auf andere Sites vorhanden.

- 405 - Method Not Allowed (Methode nicht zulässig)

  Die in der Anforderungszeile angegebene Methode ist für die Ressource, die von der Anforderungs-URL angegeben wird, nicht zulässig.

- 406 - None Acceptable (Nicht akzeptabel)

Der Server hat eine Ressource gefunden, die der angeforderten URL entspricht, sie erfüllt jedoch nicht die Bedingungen der Anforderungsheader "Accept" und "Accept-Encoding".

- 407 - Proxy Authentication Required (Proxyauthentifizierung erforderlich)

  Dieser Code ist für künftige Zwecke reserviert. Er gleicht dem Code 401 (Unauthorized), gibt allerdings an, dass der Client sich zuerst bei einem Proxy authentifizieren muss. HTTP 1.0 bietet keine Möglichkeit zur Proxy-Authentifizierung.
- 408 - Request Time Out (Zeitlimitüberschreitung der Anforderung)

  Der Client hat seine Anforderung nicht innerhalb der Zeit gestellt, die der Server zu warten bereit war.
- 409 - Conflict (Konflikt)

  Die Anforderung konnte möglicherweise aufgrund eines Konflikts mit dem derzeitigen Status der Ressource nicht abgeschlossen werden.
- 410 - Gone (Nicht mehr vorhanden)

  Die angeforderte Ressource ist nicht mehr auf dem Server verfügbar, und es ist keine Weiterleitungsadresse bekannt.
- 411 - Authorization Refused (Berechtigung abgelehnt)

  Der vom Client angegebene Berechtigungsnachweis für die Anforderung wurde vom Server zurückgewiesen oder reicht für eine Zugriffsberechtigung auf die Ressource nicht aus.
- 412 - Precondition Failed (Bedingung fehlgeschlagen)
- 413 - Request Entity Too Large (Angeforderte Entität zu groß)
- 414 - Request URI Too Large (Angeforderte URI zu groß)
- 415 - Unsupported Media Type (Nicht unterstützter Medientyp)

Codes von 500 - 599

- 500 - Internal Server Error (Interner Serverfehler)

  Der Server hat einen unerwarteten Zustand vorgefunden, sodass er die Anforderung nicht erfüllen konnte. Beim Web-Server ist ein Fehler aufgetreten, sodass keine aussagekräftige Antwort möglich ist. Normalerweise kann von der Browserseite her nichts getan werden, um diesen Fehler zu beheben; der Serveradministrator überprüft das Fehlerprotokoll des Servers, um festzustellen, welches Problem vorlag. Oftmals ist dies die Fehlernachricht, die für ein nicht ordnungsgemäß codiertes CGI-Script ausgegeben wird.
- 501 - Method Not Implemented (Methode nicht implementiert)

  Der Server unterstützt die Funktionalität nicht, die zur Erfüllung der Anforderung notwendig ist. Die Anwendungsmethode (GET oder POST) ist nicht implementiert.
- 502 - Bad Destination (Fehlerhaftes Ziel)

  Der Server hat eine nicht verwendbare Antwort vom Zielserver oder übergeordneten Server empfangen, auf den er zur Erfüllung der Anforderung zugreifen wollte.
- 503 - Service Temporarily Unavailable (Service temporär nicht verfügbar)

  Der Server kann die Anforderung derzeit nicht bearbeiten, da er temporär überlastet ist oder gewartet wird. Der Server hat keine Ressourcen mehr.
- 504 - Destination Time Out (Zeitlimitüberschreitung des Ziels)

  Der Server hat nicht rechtzeitig eine Antwort vom Zielserver oder übergeordneten Server erhalten, auf den er zum Ausführen der Anforderung zugegriffen hat.
- 505 - HTTP Version Not Supported (HTTP-Version nicht unterstützt)

EDI-Berichte

Verwenden Sie EDI-Berichte, um überfällige funktionale Bestätigungen (Functional Acknowledgement - FA) für Electronic Data Interchange (EDI) zu suchen. Darüber hinaus können Sie auch zurückgewiesene EDI-Transaktionen suchen. In den folgenden Abschnitten wird die Vorgehensweise für die Verwendung der EDI-Berichte beschrieben.

Suche nach überfälligen EDI-FAs

Auf der Seite **Suche nach überfälligen EDI-FAs** werden Suchkriterien für die Suche nach überfälligen funktionalen EDI-Bestätigungen (EDI-FAs) bereitgestellt.

Anmerkung: Alle Sätze, die aus vorherigen Suchoperationen nach überfälligen funktionalen EDI-Bestätigungen entfernt wurden, werden auch von späteren Suchoperationen ignoriert. Daher werden entfernte Sätze in späteren Berichten nicht angezeigt. Sätze können aus einem Bericht entfernt werden, indem auf der Seite **Bericht für überfällige funktionale EDI-Bestätigungen** die Option **Ausgewählte Sätze ignorieren** ausgewählt wird. Nur der Hubadministrator kann Sätze aus einem Bericht löschen.

Gehen Sie wie folgt vor, um nach überfälligen EDI-FA-Sätzen zu suchen:

1. Klicken Sie auf **Tools > EDI-Berichte**. Die Seite **Suche nach überfälligen EDI-FAs** wird angezeigt.
2. Wählen Sie in der Dropdown-Liste eines oder mehrere der folgenden Suchkriterien aus:

Tabelle 18. Suchkriterien für überfällige EDI-FAs

Wert	Beschreibung
Startdatum und Zeit	Das Datum und die Zeit für den Beginn der Transaktion.
Enddatum und Zeit	Das Datum und die Zeit für das Ende der Transaktion.
Quellenpartner	Der Partner, der die Transaktion eingeleitet hat.
Zielpartner	Der Partner, der die Transaktion empfangen hat.
Suchen in	Gibt an, ob im Quellendokumenttyp oder im Zieldokumenttyp gesucht werden soll.
Paket	Beschreibt Dokumentformat, Paket, Verschlüsselung und Inhaltstypkennung.
Protokoll	Typ des Prozessprotokolls, z. B. XML, EDI, Flachdatei. Die angezeigten Protokolle variieren abhängig von dem im Feld **Paket** ausgewählten Wert.
Dokumenttyp	Der jeweilige Dokumenttyp. Die angezeigten Typen variieren abhängig von dem im Feld **Protokoll** ausgewählten Wert.
Referenz-ID	Gibt eine Transaktions-ID an.
Sortieren nach	Gibt die Kriterien zum Sortieren der Suchergebnisse an. Die Standardwerte sind **Überfällig seit** und **Absteigend**. Verwenden Sie **Absteigend**, um die FAs zuerst anzuzeigen, die am längsten überfällig sind. Wählen Sie **Aufsteigend** aus, um die FAs zuerst anzuzeigen, die am wenigsten überfällig sind.
Ergebnisse pro Seite	Gibt an, wie viele Ergebnisse einer Transaktionssuche auf jeder einzelnen Seite angezeigt werden sollen.

3. Klicken Sie auf **Suchen**, um den Bericht über die Suche nach überfälligen EDI-FAs anzuzeigen.

Berichte zu überfälligen EDI-FAs anzeigen

Das Suchergebnis wird abhängig von den auf der Seite **Suche nach überfälligen EDI-FAs** ausgewählten Suchkriterien auf der Seite **Bericht für überfällige EDI-FAs** angezeigt.

Der Bericht für überfällige EDI-FAs (funktionale EDI-Bestätigungen) enthält die folgenden Daten (falls anwendbar):

Tabelle 19. Bericht für überfällige EDI-FAs

Wert	Beschreibung
Datum	Das Datum, an dem die EDI-Transaktion vom Quellenpartner an den Zielpartner gesendet wurde.
Zeit	Die Uhrzeit (Greenwich Mean Time), zu der die EDI-Transaktion vom Quellenpartner an den Zielpartner gesendet wurde.
Aktivitäts-ID	Die eindeutige ID (UID) der Transaktion.
Quellenhandelspartner	Der Partner, der die Transaktion gesendet hat.
Quellenpaket	Das Quellenpaket der Transaktion.
Quellenprotokoll	Das Quellenprotokoll der Transaktion.
Quellendokumenttyp	Der Quellendokumenttyp der Transaktion.
Zielhandelspartner	Der Partner, der die Transaktion gesendet hat.
Zielpaket	Das Zielpaket der Transaktion.
Zielprotokoll	Das Zielprotokoll der Transaktion.
Zieldokumenttyp	Der Zieldokumenttyp der Transaktion.
Austauschnummer	Die Austauschnummer der Transaktion.
Gruppennummer	Die Gruppennummer der Transaktion.
Transaktionsnummer	Die Kenn-Nummer der Transaktion.
FA fällig am	Das Datum, an dem die FA für die Transaktion fällig war.
Überfällig seit	Die Zeitdauer, seit der die FA bereits überfällig ist.
Ausgewählte Sätze ignorieren	Wenn Sie diese Option für einen Satz auswählen, wird dieser Satz aus dem Bericht entfernt. Wenn ein Satz aus einem Bericht entfernt wurde, wird dieser Satz auch von späteren Suchen nach überfälligen EDI-FAs ignoriert und wird daher auch in diesen Berichten nicht angezeigt. Nur der Hubadministrator kann Sätze aus einem Bericht löschen.

Suche nach zurückgewiesenen EDI-Transaktionen

Auf der Seite **Suche nach zurückgewiesenen EDI-Transaktionen** werden Kriterien angezeigt, mit deren Hilfe Sie EDI-Transaktionen (EDI, Electronic Data Interchange - elektronischer Datenaustausch) suchen können, deren funktionale Bestätigung (FA) einen Fehlercode enthält. Transaktionsdatensätze ohne FAs werden von der Suche nach zurückgewiesenen EDI-Transaktionen nicht zurückgegeben.

Gehen Sie wie folgt vor, um nach zurückgewiesenen EDI-Sätzen zu suchen:

1. Klicken Sie auf **Tools > EDI-Berichte > Bericht zu zurückgewiesenen EDI-Transaktionen**.
2. Wählen Sie in der Dropdown-Liste eines oder mehrere der folgenden Suchkriterien aus:

Tabelle 20. Suchkriterien für zurückgewiesene EDI-Transaktionen

Wert	Beschreibung
Startdatum und Zeit	Das Datum und die Zeit für den Beginn der Transaktion.
Enddatum und Zeit	Das Datum und die Zeit für das Ende der Transaktion.
Quellenpartner	Der Partner, der die Transaktion eingeleitet hat.

Tabelle 20. Suchkriterien für zurückgewiesene EDI-Transaktionen (Forts.)

Wert	Beschreibung
Zielpartner	Der Partner, der die Transaktion empfangen hat.
Suchen in	Gibt an, ob im Quellendokumenttyp oder im Zieldokumenttyp gesucht werden soll.
Paket	Beschreibt Dokumentformat, Paket, Verschlüsselung und Inhaltstypkennung.
Protokoll	Typ des Prozessprotokolls, z. B. XML, EDI, Flachdatei. Die angezeigten Protokolle variieren abhängig von dem im Feld **Paket** ausgewählten Wert.
Dokumenttyp	Der jeweilige Dokumenttyp. Die angezeigten Typen variieren abhängig von dem im Feld **Protokoll** ausgewählten Wert.
Referenz-ID	Gibt eine Transaktions-ID an.
Sortieren nach	Gibt die Kriterien zum Sortieren der Suchergebnisse an. Die Standardwerte sind **Überfällig seit** und **Absteigend**. Verwenden Sie **Absteigend**, um die FAs zuerst anzuzeigen, die am längsten überfällig sind. Wählen Sie **Aufsteigend** aus, um die FAs zuerst anzuzeigen, die am wenigsten überfällig sind.
Ergebnisse pro Seite	Gibt an, wie viele Ergebnisse einer Transaktionssuche auf jeder einzelnen Seite angezeigt werden sollen.

3. Klicken Sie auf **Suchen**, um die zurückgewiesenen EDI-Transaktionen anzuzeigen.

Berichte zu zurückgewiesenen EDI-Transaktionen anzeigen

Das Suchergebnis wird abhängig von den auf der Seite **Suche nach zurückgewiesenen EDI-Transaktionen** ausgewählten Suchkriterien auf der Seite **Bericht für zurückgewiesene EDI-Transaktionen** angezeigt.

Der Bericht für zurückgewiesene EDI-Transaktionen enthält die folgenden Daten (falls anwendbar):

Tabelle 21. Bericht für zurückgewiesene EDI-Transaktionen

Wert	Beschreibung
Datum	Das Datum, an dem die EDI-Transaktion empfangen wurde.
Zeit	Die Uhrzeit (Greenwich Mean Time), zu der die EDI-Transaktion vom Quellenpartner an den Zielpartner gesendet wurde.
Aktivitäts-ID	Die eindeutige ID (UID) der Transaktion.
Quellenhandelspartner	Der Partner, der die Transaktion gesendet hat.
Quellenpaket	Das Quellenpaket der Transaktion.
Quellenprotokoll	Das Quellenprotokoll der Transaktion.
Quellendokumenttyp	Der Quellendokumenttyp der Transaktion.
Zielhandelspartner	Der Partner, der die Transaktion empfangen hat.
Zielpaket	Das Zielpaket der Transaktion.
Zielprotokoll	Das Zielprotokoll der Transaktion.
Zieldokumenttyp	Der Zieldokumenttyp der Transaktion.
Austauschnummer	Die Austauschnummer der Transaktion.
Gruppennummer	Die Gruppennummer der Transaktion.
Transaktionsnummer	Die Kenn-Nummer der Transaktion.
Statuscode	Der Statuscode der funktionalen Bestätigung (FA).
Statustext	Der Statustext der funktionalen Bestätigung (FA).

FTP-Berichte

FTP-Berichte enthalten Details zu den Statistiken und Verbindungen von FTP- und SFTP-Servern.

Statistiken

Auf der Seite **Statistiken** wird der Status des FTP- und des SFTP-Servers im schreibgeschützten Modus angezeigt.

Anmerkung: Die Statistik wird nicht angezeigt, wenn der FTP- bzw. der SFTP-Server oder der FTP- bzw. SFTP-Management-Server nicht verfügbar ist.

Gehen Sie wie folgt vor, um den Status des FTP- bzw. des SFTP-Servers anzuzeigen:

1. Klicken Sie auf **Tools** > **FTP-Berichte** > **Statistik**. Die Seite **FTP-Statistiken** wird angezeigt.
2. Wählen Sie für die Option **Servertyp** den Eintrag *FTP-Server* oder *SFTP-Server* aus.
3. Die folgenden Informationen zum Serverstatus werden angezeigt:

Tabelle 22. FTP- und SFTP-Statistiken

Wert	Beschreibung
Startzeit des Servers	Die Zeit, zu der der FTP- bzw. SFTP-Server gestartet wurde.
Anzahl erstellter Verzeichnisse	Die Anzahl der Verzeichnisse, die von Benutzern mithilfe des Befehls "mkdir" erstellt wurden.
Anzahl entfernter Verzeichnisse	Die Anzahl der Verzeichnisse, die von Benutzern mithilfe des Befehls "rmdir" entfernt wurden.
Anzahl hochgeladener Dateien	Die Anzahl der von allen Benutzern hochgeladenen Dateien.
Anzahl heruntergeladener Dateien	Die Anzahl der von allen Benutzern heruntergeladenen Dateien.
Anzahl gelöschter Dateien	Die Anzahl der von allen Benutzern mithilfe des Befehls "delete" gelöschten Dateien.
Hochgeladene Byte	Die Summe der hochgeladenen Byte.
Heruntergeladene Byte	Die Summe der heruntergeladenen Byte.
Aktuelle Anmeldungen	Die Anzahl der momentan angemeldeten Benutzer.
Gesamtzahl Anmeldungen	Die Summe der Anmeldungen seit dem letzten Zurücksetzen.
Gesamtzahl fehlgeschlagene Anmeldungen	Die Summe der fehlgeschlagenen Anmeldungen.
Aktuelle Verbindungen	Die Anzahl der momentan aktiven Verbindungen.
Gesamtzahl Verbindungen	Die Summe der Verbindungen seit dem letzten Zurücksetzen.

4. Klicken Sie auf **Neu laden**, um die aktuelle Anmeldung zu aktualisieren.
5. Klicken Sie auf **Zurücksetzen**, um die Werte zurückzusetzen.

Verbindungen

Zeigen Sie die FTP-Verbindungen an, indem Sie die folgenden Schritte ausführen:

1. Klicken Sie auf **Tools > FTP-Berichte > Verbindungen**.

2. Wählen Sie für die Option **Servertyp** den Eintrag *FTP-Server* oder *SFTP-Server* aus. Abhängig von Ihrer Auswahl werden alle Verbindungen zu FTP- oder SFTP-Servern angezeigt.
3. Im Bericht werden die folgenden Verbindungsinformationen angezeigt:

Tabelle 23. FTP-Verbindungen

Wert	Beschreibung
Anmeldename	Die Anmeldebenutzer-ID für diese Verbindung. Ist dieses Feld leer, bedeutet dies, dass der Benutzer nur eine Verbindung hergestellt, sich aber noch nicht angemeldet hat.
Zeit der Anmeldung	Der Zeitpunkt, zu dem sich der Benutzer angemeldet hat. Ist dieses Feld leer, bedeutet dies, dass der Benutzer nur eine Verbindung hergestellt hat.
Zeit des letzten Zugriffs	Der Zeitpunkt, zu dem der Benutzer das letzte Mal zuvor auf diese Verbindung zugegriffen hat. Ist dieses Feld leer, bedeutet dies, dass der Benutzer sich zwar angemeldet hat, aber noch keinen Befehl ausgegeben hat.
Clientadresse	Die IP-Adresse des Clients, von der aus der Benutzer sich angemeldet hat.

Anmerkung: Um die Verbindung zu einem bestimmten Server zu trennen, können Sie auf das Symbol **Löschen** für den gewünschten Server klicken.

Kapitel 11. Ereignisse und Dokumente anzeigen

Die folgenden Funktionen ermöglichen Ihnen einen Überblick über den allgemeinen Systemzustand. Sie stellen außerdem Tools zur Fehlerbehebung bei Fehlerereignissen dar.

- „Ereignisanzeige"
- „AS-Anzeige" auf Seite 116
- „RosettaNet-Anzeige" auf Seite 120
- „Dokumentanzeige" auf Seite 122
- „ebMS-Anzeige" auf Seite 131
- „Zielwarteschlange" auf Seite 134

Anmerkung: Die Datenübertragungszeit wird im System mit dem Wert der Greenwich Mean Time (GMT) gespeichert, jedoch gemäß der Zeitzoneneinstellung des Benutzers angezeigt.

Die RosettaNet- und die AS-Anzeigen enthalten zusätzliche Suchkriterien für den Hubadministrator. Weitere Informationen finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Ereignisanzeige

Mit der Ereignisanzeige können Sie Ereignisse anzeigen und ihrer Ursache auf den Grund gehen.

Ein Ereignis informiert Sie über ein wichtiges Vorkommnis im System. Ereignisse des Typs "Fehler" und "Schwerwiegend" geben an, dass im System etwas Ungewöhnliches passiert ist. Ein Ereignis kann Sie darüber informieren, dass eine Systemoperation oder eine Systemfunktion (z. B. das Hinzufügen eines Teilnehmers zum System) erfolgreich war. Ein Ereignis kann auch auf einen Fehler oder ein Problem hinweisen (Beispiel: das System kann ein Dokument nicht verarbeiten). Die meisten Dokumenttypen werden mehrere Male gesendet. Wenn also ein Dokument fehlschlägt und ein Ereignis generiert, können Sie anhand dieser Informationen dem Problem nachgehen und es beheben, um künftige Fehler zu vermeiden.

WebSphere Partner Gateway enthält vordefinierte Ereignisse.

Mit der Funktion **Alerts** im Modul "Kontenadmin" können Sie die folgenden Aufgaben ausführen:

- Ereignisbasierte Alerts erstellen
- Ereignisse identifizieren, die das System beeinträchtigen

Über die Funktion **Kontakte** im Modul "Kontenadmin" werden Mitarbeiter angegeben, die vom System benachrichtigt werden sollen, falls solche Ereignisse auftreten.

Anmerkung: Der Administrator muss den Ereignissen, die als wichtig und grundlegend gelten, Alerts zuordnen. Wenn diese Zuordnung nicht während der Konfiguration stattfindet, generiert WebSphere Partner Gateway keine Alertbenachrichtigungen.

Die Ereignisanzeige zeigt Ereignisse basierend auf bestimmten Suchkriterien an. Anhand dieser Suchkriterien können Sie ein bestimmtes Ereignis suchen und feststellen, warum es aufgetreten ist. Mit der Ereignisanzeige können Sie Ereignisse nach Zeit, Datum, Ereignistyp, ("Debugging", "Information", "Warnung", "Fehler" und "Kritisch"), Ereigniscode und Ereignisposition suchen.

Zu den in der Ereignisanzeige verfügbaren Daten gehören Ereignisname, Zeitmarke, Benutzer und die Partnerinformationen. Diese Daten helfen Ihnen bei der Identifizierung des Dokuments oder Prozesses, durch das bzw. den das Ereignis generiert wurde. Wenn das Ereignis zu einem Dokument gehört, können Sie außerdem das unformatierte Dokument anzeigen, welches das Feld, den Wert und die Fehlerursache angibt.

Ereignistypen

WebSphere Partner Gateway enthält die in Tabelle 24 aufgelisteten Ereignistypen.

Tabelle 24. Ereignistypen

Ereignistyp	Beschreibung
Debugging	Debugging-Ereignisse werden für den Systembetrieb auf der unteren Ebene und die Unterstützung verwendet. Ihre Sichtbarkeit und Verwendung hängt von der Berechtigungsebene des Benutzers ab. Nicht alle Benutzer haben Zugriff auf Debugging-Ereignisse.
Information	Informationsereignisse werden bei erfolgreichem Abschluss einer Systemoperation generiert. Diese Ereignisse werden auch verwendet, um den Status eines Dokuments anzugeben, das derzeit verarbeitet wird. Informationsereignisse erfordern keine Benutzeraktion.
Warnung	Warnereignisse treten aufgrund von nicht kritischen Unregelmäßigkeiten in der Dokumentverarbeitung oder in Systemfunktionen auf, bei denen die Operation jedoch weiter läuft.
Fehler	Fehlerereignisse treten bei Unregelmäßigkeiten in der Dokumentverarbeitung auf, durch die der Prozess vorzeitig beendet wird.
Kritisch	Kritische Ereignisse werden generiert, wenn ein Dienst aufgrund eines Systemausfalls vorzeitig beendet wird. Kritische Ereignisse erfordern das Eingreifen der Benutzerunterstützung.

Ereignisse suchen

1. Klicken Sie auf **Anzeigen** > **Ereignisanzeige**.

   Die Kontrollkästchen für den Schweregrad des Ereignisses werden von links nach rechts aufgelistet, wobei "Debugging" auf der linken Seite des Suchfensters in der Ereignisanzeige steht. Der ganz links stehende Ereignistyp ist der am wenigsten schwerwiegende; der Ereignistyp "Kritisch" ganz rechts ist der gravierendste. Für jedes ausgewählte Ereignis werden in der Ereignisanzeige das Ereignis selbst sowie alle Ereignisse angezeigt, deren Wertigkeit höher ist. Wenn z. B. der Ereignistyp "Warnung" in den Suchkriterien ausgewählt wurde, werden die Ereignisse "Warnung", "Fehler" und "Kritisch" angezeigt. Wenn Debugging-Ereignisse ausgewählt wurden, werden alle Ereignistypen angezeigt.

   Anmerkung: Debugging-Ereignisse können nicht von allen Benutzern angezeigt werden.
2. Wählen Sie die Suchkriterien in den Listen aus.

Tabelle 25. Kriterien für die Ereignissuche

Wert	Beschreibung
Startdatum und Zeit	Datum und Uhrzeit, zu dem bzw. der das erste Ereignis aufgetreten ist.
Enddatum und Zeit	Datum und Uhrzeit, zu dem bzw. der das letzte Ereignis aufgetreten ist.
Partner	Wählen Sie alle Partner oder einen bestimmten Partner aus.
Ereignistyp	Der Typ des Ereignisses: Debugging, Information, Warnung, Fehler oder Kritisch.
Ereigniscode	Durchsuchen Sie die verfügbaren Ereigniscodes basierend auf dem ausgewählten Ereignistyp.
Ereignisposition	Position, an der das Ereignis generiert wurde: Alle, Unbekannt, Quelle bzw. Absender, Ziel bzw. Empfänger.
Sortieren nach	Ergebnisse sortieren nach: • Ereignisname • Zeitmarke • Typ • Quellenpartner • Quellen-IP Der Standardwert ist "Zeitmarke".
Absteigend oder Aufsteigend	"Absteigend" zeigt zuerst die neuste Zeitmarke oder den Anfang des Alphabets an. "Aufsteigend" zeigt zuerst die älteste Zeitmarke oder das Ende des Alphabets an. Der Standardwert ist "Absteigend".
Ergebnisse pro Seite	Anzahl der angezeigten Datensätze pro Seite.
Aktualisieren	Die Standardeinstellung ist "Off". Wenn die Aktualisierung eingestellt ist ("On"), führt die Ereignisanzeige zunächst eine neue Abfrage aus und bleibt dann im Aktualisierungsmodus.
Aktualisierungsrate	Steuert, wie oft die Suchergebnisse aktualisiert werden sollen (nur für internen Partner).

3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Ereignisse an.

Tipp: Die Ereignisliste kann nach dem Ereignistyp neu gefiltert werden, der oben im Fenster **Ereignisanzeige** ausgewählt wurde. Bei der nächsten Fensteraktualisierung wird der neu ausgewählte Ereignistyp berücksichtigt.

Ereignisdetails anzeigen

1. Klicken Sie auf **Anzeigen** > **Ereignisanzeige**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**.
4. Klicken Sie in der angezeigten Ereignisliste neben dem Ereignis, dessen Details Sie anzeigen möchten, auf das Symbol **Details anzeigen** .
5. Klicken Sie in den angezeigten Ereignisdetails neben dem Dokument, das Sie anzeigen möchten (falls vorhanden), auf das Symbol **Details anzeigen**.
6. Klicken Sie auf das Symbol **Unformatiertes Dokument anzeigen**, um das unformatierte Dokument anzuzeigen, falls es vorhanden ist.
7. Klicken Sie auf das Symbol **Validierungsfehler anzeigen**, um eventuell vorhandene Validierungsfehler anzuzeigen.

Tipp: Wenn in der **Ereignisanzeige** unter **Details** das Ereignis **Doppeltes Dokument** angezeigt wird, können Sie das zuvor gesendete Originaldokument anzeigen, indem Sie in **Dokumentdetails** auf das Symbol zum Anzeigen des Originaldokuments klicken.

Fehlerereignisse

Zu jedem Fehler- oder Warnereignis, das auf der Anzeigeseite der Konsole angezeigt wird, können detaillierte Informationen abgerufen werden. Diese Informationen zur Selbsthilfe enthalten Angaben zu Ursache, Diagnose und Lösung des Problems.

Das folgende Beispiel liefert die erforderlichen Details im Falle eines Verbindungsparsingfehlers für eine XML-Nachricht:

BCG240065 - Verbindungsparsingfehler für XML-Nachricht. XML-Verbindungsparsing fehlgeschlagen: {0}

Fehlerursache: Der Fehler 'Verbindungsparsingfehler für XML-Nachricht' wird aus folgendem Grund generiert: Die Informationen aus dem eingehenden Dokument sind für das Parsing der Verbindung nicht ausreichend.

Erläuterung: Der Hub muss das eingehende Dokument parsen, um die erforderlichen Attribute zum Identifizieren der Verbindung für das eingehende XML-Dokument abzurufen. Die Verbindung ist entweder nicht konfiguriert oder das eingehende XML-Dokument enthält die entsprechenden Werte nicht.

Lösung: Gehen Sie wie folgt vor, um diesen Fehler zu beheben:

- Stellen Sie sicher, dass die Verbindung ordnungsgemäß konfiguriert ist.
- Stellen Sie sicher, dass das eingehende Dokument alle erforderlichen Attribute zum Identifizieren der Verbindung enthält.

Technische Unterstützung: Weitere Informationen zu diesem Fehlerereignis finden Sie auf der WebSphere Partner Gateway-Site für technische Unterstützung.

Detaillierte Informationen zu Ereignissen: Klicken Sie auf den bereitgestellten Ereigniscode, um die Details des Ereignisses anzuzeigen.

AS-Anzeige

Verwenden Sie die AS-Anzeige, um gepackte B2B-Transaktionen und B2B-Prozessdetails anzuzeigen, die das Kommunikationsprotokoll Applicability Statement 1, 2 oder 3 (AS1, AS2 oder AS3) verwenden. Sie können den Ablauf des B2B-Prozesses und der zugehörigen Geschäftsdokumente, der Empfangsbestätigungssignale, des Verarbeitungsstatus, der HTTP-Header und des Inhalts der übertragenen Dokumente anzeigen.

Wie der Vorgänger AS1, ein Standard zur Datenübertragung mit SMTP, ist auch AS2 ein solcher Standard zur Datenübertragung mit HTTP. AS3 ist der Standard für die Datenübertragung über FTP (File Transfer Protocol).

AS2 und AS3 geben an, wie Daten verbunden, zugestellt, geprüft und beantwortet werden. Sie interagieren jedoch nicht mit dem Inhalt des Dokuments, sondern nur mit dessen Transport. AS2 und AS3 erstellen einen Wrapper (eine Oberfläche) für ein Dokument, sodass es über das Internet mit HTTP oder HTTPS für AS2 bzw. FTP für AS3 transportiert werden kann. Zusammen werden Dokument und Wrap-

per als "Nachricht" bezeichnet. AS2 bietet Signierung und Verschlüsselung für die Daten, die in HTTP-Paketen übertragen werden. AS3 bietet das gleiche für Daten, die per FTP-Transport übertragen werden. AS2 und AS3 bieten eine Verschlüsselungsbasis mit garantierter Zustellung. AS1, AS2 und AS3 bieten die Funktionalität für die Signierung und Verschlüsselung. Darüber hinaus wird auch Funktionalität für die Komprimierung bereitgestellt.

Eine wichtige Komponente von AS2 und AS3 ist der Empfangsmechanismus, der als MDN (Message Disposition Notification - Benachrichtigung über die Nachrichtendisposition) bezeichnet wird. Mit MDN hat der Absender eines Dokuments die Gewissheit, dass der Empfänger das Dokument erfolgreich erhalten hat. Der Absender kann angeben, wie die MDN zurückgesendet werden soll (synchron oder asynchron, unterschrieben oder nicht unterschrieben).

Anmerkung: Wenn die Entschlüsselung für ein ankommendes verschlüsseltes AS2-Dokument fehlschlägt, wird kein MDN-Fehler über dieselbe Verbindung gesendet. Um dies zu korrigieren, muss zwischen den beiden Partnern eine Partnerverbindung aktiviert werden, unabhängig davon, ob die Verbindung verwendet wird. Bei der erstellten Verbindung muss es sich um eine Verbindung des Typs "AS zu None" handeln. Eine solche Verbindung wird erstellt und aktiviert, indem die B2B-Funktionalität "AS auf einem Partner und die B2B-Funktionalität "None" auf dem anderen Partner aktiviert wird. Stellen Sie sicher, dass das Quellengateway auf der AS-Seite ein SMTP-Gateway (für AS1), ein HTTP-Ziel (für AS2) oder ein FTP-Gateway (für AS3) ist. Dieses Gateway muss für die MDN-Adresse konfiguriert sein. Auf diese Weise wird die MDN bei einem Fehlschlag der Entschlüsselung über diese binäre Verbindung "AS zu None" zurückgesendet.

Nachrichten suchen

1. Klicken Sie auf **Anzeigen** > **AS-Anzeige**. Das System zeigt das Fenster **AS-Anzeige** an.
2. Wählen Sie die Suchkriterien in den Listen aus, wie in Tabelle 26 beschrieben.

Tabelle 26. Suchkriterien der AS-Anzeige

Wert	Beschreibung
Startdatum und Zeit	Datum und Uhrzeit des Prozessbeginns.
Enddatum und Zeit	Datum und Uhrzeit des Prozessendes.
Quellen- und Zielpartner	Gibt den Quellenpartner (einleitend) und den Zielpartner (empfangend) an (nur für internen Partner).
Partner	Gibt an, ob die Suche sämtliche Partner einbezieht oder nur den internen Partner (gilt nur für Partner).
Meine Rolle ist	Gibt an, ob Dokumente gesucht werden sollen, in denen der Partner das Ziel oder die Quelle ist (nur für Partner).
AS-Quellengeschäfts-ID	Geschäfts-ID des Quellenpartners, wie im AS-Header definiert.
Quellengeschäfts-ID der Nutzdaten	Geschäfts-ID des Quellenpartners, wie durch den Inhalt der Nutzdaten definiert.
Betriebsmodus	Produktion oder Test. Der Typ "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen.

Tabelle 26. Suchkriterien der AS-Anzeige (Forts.)

Wert	Beschreibung
Paket	Beschreibt Dokumentformat, Paket, Verschlüsselung und Inhaltstypkennung.
Protokoll	Für Partner verfügbares Dokumentformat, z. B. RosettaNet-XML.
Dokumenttyp	Der jeweilige Geschäftsprozess.
Nachrichten-ID	ID-Nummer, die dem mit AS gepackten Dokument zugeordnet wird. Suchkriterien können das Platzhalterzeichen Stern (*) einbeziehen. Die maximale Länge ist 255 Zeichen.
Dokument-ID	Gibt eine Dokument-ID an.
Synchron/Asynchron	"Alle", "Synchron" und "Asynchron". Suche nach Dokumenten, die im synchronen, asynchronen oder in beiden Modi empfangen wurden.
MDN-Status	Geben Sie einen oder mehrere MDN-Status über das Multiselektionsfenster **MDN-Status** an. Mögliche Optionen sind: **Alle** Zeigt alle Ergebnisse an, filtert nicht nach MDN-Status. **MDN nicht erforderlich** Zeigt alle AS-Transaktionen an, in denen MDN nicht vorhanden und nicht erforderlich ist. **MDN verarbeitet** Zeigt alle AS-Transaktionen mit erfolgreichen MDNs an. **Wartet auf MDN** Zeigt alle AS-Transaktionen an, die auf MDN warten, das zulässige Zeitlimit jedoch noch nicht überschritten haben und nicht als fehlend (= als nicht empfangen) betrachtet werden. **MDN nicht empfangen** Zeigt alle AS-Transaktionen an, die das zulässige Zeitlimit beim Warten auf MDN überschritten haben. **MDN-Dispositionsfehler** Zeigt alle AS-Transaktionen an, bei denen MDN mit einem Dispositionsfehler zurückgegeben wurde. **Unbekannt** Gibt an, dass die Datenbank nicht mit dem MDN-Status aktualisiert wurde.
Sortieren nach	Ergebnisse sortieren nach: • Zielzeitmarke • Quellendokumentdefinition • Zieldokumenttyp • Nachrichten-ID • MDN-Status • Dokument-ID Der Standardwert ist "Zielzeitmarke".

Tabelle 26. Suchkriterien der AS-Anzeige (Forts.)

Wert	Beschreibung
Absteigend oder Aufsteigend	"Absteigend" zeigt zuerst die neuste Zeitmarke oder den Anfang des Alphabets an. "Aufsteigend" zeigt zuerst die älteste Zeitmarke oder das Ende des Alphabets an. Der Standardwert ist "Absteigend".
Ergebnisse pro Seite	Wählen Sie hiermit die Anzahl der angezeigten Datensätze pro Seite aus.

3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Nachrichten an.

Nachrichtendetails anzeigen

1. Klicken Sie auf **Anzeigen** > **AS-Anzeige**. Das System öffnet das Fenster **AS-Anzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Nachrichten an.
4. Klicken Sie neben der Nachricht, die Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt die Nachricht und die zugehörigen Dokumentdetails an, wie in Tabelle 27 beschrieben.

Tabelle 27. Nachrichtendetails

Wert	Beschreibung
Nachrichten-ID	ID-Nummer, die dem mit AS gepackten Dokument zugeordnet wird. Diese Nummer gibt nur das Paket an. Das Dokument selbst hat eine separate Dokument-ID-Nummer, die zusammen mit den Dokumentdetails angezeigt wird. Die maximale Länge ist 255 Zeichen.
Quellenpartner	Partner, der einen Geschäftsprozess einleitet.
Zielpartner	Partner, der den Geschäftsprozess empfängt.
Quellenzeitmarke	Datum und Uhrzeit, zu dem bzw. der die Dokumentverarbeitung beginnt.
Betriebsmodus	Entweder Test oder Produktion. Der Typ "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen.
MDN-URI	Die Zieladresse für die MDN. Die Adresse kann als HTTP-URI oder als E-Mail-Adresse angegeben werden.
MDN-Dispositionstext	Dieser Text enthält den Status der ursprünglich empfangenen Nachricht (entweder "erfolgreich" oder "fehlgeschlagen"). Die Beispiele enthalten die folgenden Informationen: • Automatic-action/MDN-sent-automatically; processed. • Automatic-action/MDN-sent-automatically; processed/ Warning;duplicate-document. • Automatic-action/MDN-sent-automatically; processed/ Error;decryption-failed. • Automatic-action/MDN-sent-automatically;failed:unsupported MIC-algorithms.

5. (Optional) Klicken Sie auf das Symbol **Dokumentdetails**, um weitere Informationen zu dem Dokument anzuzeigen.

RosettaNet-Anzeige

RosettaNet ist eine Gruppe von Unternehmen, die einen Branchenstandard für e-business Transaktionen erstellt haben. PIPs (Partner Interface Processes - Partnerschnittstellenprozesse) definieren Geschäftsprozesse zwischen den Mitgliedern der Hub-Community. Jeder PIP steht für ein bestimmtes Geschäftsdokument und wie es zwischen den internen und externen Partnern verarbeitet wird.

Die RosettaNet-Anzeige listet die korrekte Reihenfolge der Subtransaktionen auf, wie sie für das erfolgreiche Beenden eines Dokumentenflusses erforderlich ist. Mit der RosettaNet-Anzeige können Sie Werte wie den Prozess-Status, Details, unformatierte Dokumente und zugehörige Prozessereignisse anzeigen.

Mit der RosettaNet-Anzeige können Sie einen bestimmten Prozess suchen, der ein Ereignis generiert hat. Wenn Sie den Zielprozess angeben, können Sie die Prozessdetails und das unformatierte Dokument anzeigen.

Die RosettaNet-Anzeige zeigt Prozesse basierend auf bestimmten Suchkriterien an.

RosettaNet-Prozesse suchen

1. Klicken Sie auf **Anzeigen** > **RosettaNet-Anzeige**.
2. Wählen Sie im Fenster **RosettaNet-Anzeige - Suche** die Suchkriterien in der Liste aus, wie in Tabelle 28 beschrieben.

Tabelle 28. RosettaNet-Suchkriterien

Wert	Beschreibung
Startdatum und Zeit	Datum und Uhrzeit des Prozessbeginns.
Enddatum und Zeit	Datum und Uhrzeit des Prozessendes.
Quellen- und Zielpartner	Gibt den Quellenpartner (einleitend) und den Zielpartner (empfangend) an (nur für internen Partner).
Partner	Gibt an, ob die Suche sämtliche Partner einbezieht oder nur den internen Partner (gilt nur für Partner).
Meine Rolle ist	Gibt an, ob Dokumente gesucht werden sollen, in denen der Partner das Ziel oder die Quelle ist (nur für Partner).
Quellengeschäfts-ID	Geschäfts-ID des einleitenden Partners, z. B. DUNS.
Betriebsmodus	Produktion oder Test. Der Typ "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen.
Protokoll	Für die Partner verfügbare Protokolle.
Dokumenttyp	Der jeweilige Geschäftsprozess.
Prozessinstanz-ID	Eindeutige Identifikationsnummer, die dem Prozess zugeordnet wird. Die Kriterien können das Platzhalterzeichen Stern (*) einbeziehen.
Sortieren nach	Ergebnisse sortieren nach: • Zielzeitmarke • Dokumenttyp Der Standardwert ist "Zielzeitmarke".
Absteigend oder Aufsteigend	"Absteigend" zeigt zuerst die neuste Zeitmarke oder den Anfang des Alphabets an. "Aufsteigend" zeigt zuerst die älteste Zeitmarke oder das Ende des Alphabets an. Der Standardwert ist "Absteigend".
Ergebnisse pro Seite	Gibt die Anzahl der angezeigten Ergebnisse pro Seite an.

3. Klicken Sie auf **Suchen**. Das System zeigt die RosettaNet-Prozesse an, die Ihren Suchkriterien entsprechen.

RosettaNet-Prozessdetails anzeigen

1. Klicken Sie auf **Anzeigen** > **RosettaNet-Anzeige**. Das System öffnet das Fenster **RosettaNet-Anzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt die Ergebnisse Ihrer Suche an, wie in Tabelle 29 beschrieben.

Tabelle 29. Dokumentverarbeitungsdetails

Wert	Beschreibung
Partner	Partner, die in den Geschäftsprozess eingebunden sind.
Zeitmarken	Datum und Uhrzeit, zu dem bzw. der das erste Dokument verarbeitet wird.
Dokumenttyp	Spezifischer Geschäftsprozess, z. B. RosettaNet (1.1): 3A7.
Betriebsmodus	Zeigt die Art des Dokuments an, das ausgetauscht wird.
Prozessinstanz-ID	Eindeutige Zahl, die dem Prozess durch den einleitenden Handelspartner zugeordnet wird.
Dokument-ID	Proprietäre Dokumentkennung, die vom absendenden Partner zugeordnet wird. Das Feld befindet sich nicht an einer festgelegten Position und variiert nach Dokumenttyp.
Quellenpartner	Einleitender Partner.
Zielpartner	Empfangender Partner.

4. Klicken Sie neben dem RosettaNet-Prozess, den Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt Details und zugehörige Dokumente für den ausgewählten Prozess an.
5. Klicken Sie neben dem Dokument, das Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt das Dokument und die zugehörigen Ereignisdetails an.

Unformatierte Dokumente anzeigen

Verwenden Sie diese Prozedur, um ein unformatiertes Dokument anzuzeigen, das einer RosettaNet-Transaktion zugeordnet ist.

1. Klicken Sie auf **Anzeigen** > **RosettaNet-Anzeige**. Das System öffnet das Fenster **RosettaNet-Anzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Prozesse an.
4. Klicken Sie neben dem Prozess, den Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt Prozessdetails und zugehörige Dokumente für den ausgewählten Prozess an.
5. Klicken Sie neben dem Dokumenttyp auf das Symbol **Unformatiertes Dokument anzeigen**, um das unformatierte Dokument anzuzeigen.

Einschränkungen:

1. Unformatierte Dokumente, die größer als 100 KB sind, werden abgeschnitten. Wenn sich die Signatur z. B. unten im unformatierten Dokument (Datei mit Erweiterung `.rno`) befindet und die Größe des unformatierten Dokuments 100 KB überschreitet oder wenn die Signatur nach den ersten 100 KB der `.rno`-Datei aufgeführt ist, wird die Signatur nicht in der Dokumentanzeige angezeigt.

Wenn Sie die vollständige Datei anzeigen wollen, können Sie sie mithilfe der Option zum Kopieren auf die lokale Platte herunterladen.

2. Die Anzeige für unformatierte Dokumente zeigt möglicherweise keine Dokumentanhänge an. Klicken Sie zum Anzeigen von Anhängen in der Anzeige für unformatierte Dokumente auf die Verknüpfung **Kopieren**, um die Datei einschließlich Anhängen auf Ihrem lokalen Datenträger zu speichern.

Tipps:

- Zur Fehlerbehebung von Dokumenten, deren Verarbeitung fehlgeschlagen ist, siehe auch „Datenvalidierungsfehler anzeigen" auf Seite 128.
- Die Anzeige für unformatierte Dokumente zeigt den HTTP-Header mit dem unformatierten Dokument an.

Dokumentanzeige

Verwenden Sie die Dokumentanzeige, um einzelne Dokumente anzuzeigen, aus denen ein Prozess besteht. Sie können Suchkriterien verwenden, um unformatierte Dokumente und zugehörige Dokumentverarbeitungsdetails und Ereignisse anzuzeigen. Über die Dokumentanzeige können Sie außerdem fehlgeschlagene oder erfolgreich gesendete Dokumente erneut senden.

Dokumente suchen

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus, wie in Tabelle 30 beschrieben.

Tabelle 30. Suchkriterien der Dokumentanzeige

Wert	Beschreibung
Startdatum	Datum, zu dem der Dokumenttypprozess eingeleitet wurde.
Startzeit	Zeit, zu der der Dokumenttypprozess eingeleitet wurde.
Enddatum	Datum, zu dem der Dokumenttypprozess beendet wurde.
Endzeit	Zeit, zu der der Dokumenttypprozess beendet wurde.
Quellenpartner	Steht für den Partner, der den Dokumenttyp eingeleitet hat. Der Standardwert ist "Alle".
Zielpartner	Steht für den Partner, der den Dokumenttyp empfangen hat. Der Standardwert ist "Alle".
Suchen in	Gibt an, ob im Quellendokumenttyp oder im Zieldokumenttyp gesucht werden soll. Der Standardwert ist "Quellendokumenttyp".
Betriebsmodus	Gibt die Art des Dokuments an, das ausgetauscht wird (z. B. ob es für Produktions- oder Testzwecke verwendet wird). Der Standardwert ist "Alle".
Dokumentstatus	Derzeitiger Dokumentstatus im System: "Wird ausgeführt", "Erfolgreich"oder "Fehlgeschlagen". Der Standardwert ist "Alle".
Paket	Beschreibt Dokumentformat, Paket, Verschlüsselung und Inhaltstypkennung. Begrenzt die Suche auf das aufgelistete Paket. Der Standardwert ist "Alle".
Protokoll	Typ des für die Partner verfügbaren Prozessprotokolls.
Dokumenttyp	Der genaue Dokumenttyp, für den das Dokument enthalten ist. Ein Dokumenttyp ist die dritte Ebene einer Dokumentdefinition und ist unter Paket und Protokoll angegeben.
Name der Originaldatei	Der ursprünglich der Datei zugewiesene Name.
Dokument-ID	Erstellt vom Quellenpartner. Die Kriterien können das Platzhalterzeichen Stern (*) einbeziehen.

Tabelle 30. Suchkriterien der Dokumentanzeige (Forts.)

Wert	Beschreibung
Referenz-ID	Die ID-Nummer, die vom System für die Verfolgung des Dokumentstatus erstellt wurde.
Quellen-IP-Adresse	Die IP-Adresse des Quellenpartners.
Filter	Dokumente suchen, die im synchronen Modus empfangen wurden. Dies bedeutet, dass die Verbindung zwischen dem Initiator und dem Hub geöffnet bleibt, einschließlich Anforderung und Bestätigung oder Anforderung und Antwort.
Sortieren nach	Ergebnisse sortieren nach: • Zielzeitmarke • Quellendokumenttyp • Zieldokumenttyp • Dokument-ID • Suchfelder 1 bis 10 Der Standardwert ist "Zielzeitmarke".
Ergebnisse pro Seite	Anzahl der angezeigten Datensätze pro Seite.
Absteigend oder Aufsteigend	"Absteigend" zeigt zuerst die neuste Zeitmarke oder den Anfang des Alphabets an. "Aufsteigend" zeigt zuerst die älteste Zeitmarke oder das Ende des Alphabets an. Der Standardwert ist "Absteigend".

3. Gehen Sie wie folgt vor, um über die benutzerdefinierten Suchfelder eine Suche auszuführen: Geben Sie in den Feldern mit der Bezeichnung **Suchfeld 1** bis **Suchfeld 10** die Suchkriterien an.

   Benutzerdefinierte Suchfelder können für das Dokument in Ihrem System beim Konfigurieren von XML-Formaten oder EDI-Transformationszuordnungen definiert werden oder in angepassten Benutzerexits. Weitere Informationen zum Konfigurieren von XML-Formaten finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*. Hilfe zum Erstellen von Benutzerexits finden Sie im Handbuch *WebSphere Partner Gateway Programmers Guide*.

   Wenn für die Dokumente in Ihrem System keine angepassten Suchfelder definiert wurden, lassen Sie die Suchfelder unausgefüllt.

   Anmerkung: Benutzerdefinierte Suchdaten werden nur für Dokumente gespeichert, die nach abgeschlossener Konfiguration ausgetauscht werden. Dokumente, die vor dieser Konfiguration ausgetauscht wurden, enthalten keine benutzerdefinierten Suchdaten.

4. Klicken Sie auf **Suchen**. Das System zeigt die Ergebnisse Ihrer Suche an, wie in Tabelle 31 beschrieben.

   Anmerkung: Der Terminus "Partner" wird in den Anzeigefenstern verwendet, um ein Mitglied der Hub-Community (einschließlich des internen Partners) zu bezeichnen.

Tabelle 31. Dokumentdetails

Wert	Beschreibung
Partner	Quellenpartner (Absender) und Zielpartner (Empfänger), die in den Geschäftsprozess eingebunden sind.
Zeitmarken	Datum und Uhrzeit, zu dem bzw. der die Dokumentverarbeitung jeweils beginnt und endet.
Dokumenttyp	Geschäftsprozess, der gerade ausgeführt wird.

Tabelle 31. Dokumentdetails (Forts.)

Wert	Beschreibung
Betriebsmodus	Test oder Produktion. Der Typ "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen.
Synchron	Gibt an, dass das Dokument im synchronen Modus empfangen wurde. Dies bedeutet, dass die Verbindung zwischen dem Initiator und dem Hub geöffnet bleibt, einschließlich Anforderung und Bestätigung oder Anforderung und Antwort.

Dokumentdetails, Ereignisse und unformatierte Dokumente anzeigen

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste von Dokumenten an.
4. Klicken Sie neben dem Dokument, das Sie anzeigen möchten, auf das Symbol **Details anzeigen**.
   - Verfügen EDI-Austauschdokumente über untergeordnete EDI-Transaktionen, die beim Entfernen des Umschlags bzw. beim Einfügen in den Umschlag generiert wurden, können Sie diese anzeigen. Wählen Sie hierzu das Optionsfeld **Untergeordnete Elemente des Dokuments** für die Quelle oder das Ziel aus. Detaillierte Informationen hierzu finden Sie unter „EDI-Dokumente anzeigen" auf Seite 126.
   - Wenn Sie das unformatierte Dokument einschließlich der vorhandenen Transportheader anzeigen möchten, klicken Sie neben dem gewünschten Dokument auf das Symbol **Unformatiertes Dokument anzeigen**. Das System zeigt den Inhalt des unformatierten Dokuments an.
   - Klicken Sie zum Anzeigen der benutzerdefinierten Suchfelder, die diesem Dokument zugeordnet wurden, im Bereich **Benutzerdefinierte Suchfelder** auf die Verknüpfung **Anzeigen**.
   - Klicken Sie zum Anzeigen der Felder mit doppelten IDs, die diesem Dokument zugeordnet wurden, im Bereich **Felder mit doppelten IDs** auf die Verknüpfung **Anzeigen**.

     Anmerkung: Wenn das betreffende Dokument als doppeltes Dokument zurückgegeben wurde, sind die Felder mit doppelten IDs leer. Wenn in diesen Feldern etwaige Daten vorhanden sind, müssen die Daten für alle Dokumente im System eindeutig sein.

Die Dokumentverarbeitungsinformationen werden angezeigt, wenn Sie Dokumentdetails anzeigen, wie in Tabelle 32 beschrieben.

Tabelle 32. Dokumentverarbeitungswerte, verfügbar über die Dokumentanzeige

Wert	Beschreibung
Referenz-ID	Eindeutige Identifikationsnummer, die dem Dokument vom System zugeordnet wird.
Dokument-ID	Eindeutige Identifikationsnummer, die dem Dokument vom Quellenpartner zugeordnet wird.
Dokumentzeitmarke	Datum und Uhrzeit, zu dem bzw. zu der das Dokument vom Partner erstellt wurde.
Betriebsmodus	Die Ziel, durch das das Dokument geleitet wird.

Tabelle 32. Dokumentverarbeitungswerte, verfügbar über die Dokumentanzeige (Forts.)

Wert	Beschreibung
Verbindungsdokument-definition	Aktionen, die das System für ein Dokument ausgeführt hat, um dessen Kompatibilität mit den Geschäftsanforderungen zwischen den Partnern sicherzustellen.
Quelle und Ziel	Quellen- und Zielpartner, die in den Geschäftsprozess eingebunden sind.
Eingangszeitmarke	Datum und Uhrzeit, zu dem bzw. der das System das Dokument vom Partner empfangen hat.
Zeitmarke für Endstatus	Datum und Uhrzeit, zu dem bzw. zu der das System das Dokument erfolgreich an den Zielpartner weitergeleitet hat.
Quellen- und Zielgeschäfts-ID	Geschäfts-ID des Quellen- und Zielpartners, z. B. DUNS.
Quellen- und Zieldokumenttyp	Der spezielle Geschäftsprozess, der zwischen Quellen- und Zielpartnern ausgeführt wird.

Einschränkungen:

1. Unformatierte Dokumente, die größer als 100 KB sind, werden abgeschnitten. Wenn sich die Signatur z. B. unten im unformatierten Dokument (Datei mit Erweiterung `.rno`) befindet und die Größe des unformatierten Dokuments 100 KB überschreitet oder wenn die Signatur nach den ersten 100 KB der `.rno`-Datei aufgeführt ist, wird die Signatur nicht in der Dokumentanzeige angezeigt. Wenn Sie die vollständige Datei anzeigen wollen, können Sie sie mithilfe der Option zum Kopieren auf die lokale Platte herunterladen.
2. Die Anzeige für unformatierte Dokumente zeigt möglicherweise keine Dokumentanhänge an. Klicken Sie zum Anzeigen von Anhängen in der Anzeige für unformatierte Dokumente auf die Verknüpfung **Kopieren**, um die Datei einschließlich Anhängen auf Ihrem lokalen Datenträger zu speichern.

Tipps:

1. Wenn im System das Ereignis **Doppeltes Dokument** angezeigt wird, zeigen Sie das zuvor gesendete Originaldokument an, indem Sie neben dem Ereignis **Doppeltes Dokument** auf das Symbol zum Anzeigen des zuvor gesendeten Originaldokuments klicken.
2. Informationen zur Fehlerbehebung in Dokumenten, deren Verarbeitung fehlgeschlagen ist, finden Sie im Abschnitt „Datenvalidierungsfehler anzeigen" auf Seite 128.

Mehrere Dokumente erneut versenden

Führen Sie die folgenden Schritte in der Anzeige der Suchergebnisse in der Dokumentanzeige aus, um mehrere Dokumente erneut zu versenden:

1. Führen Sie die Schritte im Abschnitt Dokumente suchen aus.
2. Wählen Sie in der daraufhin angezeigten Anzeige der Dokumentanzeige das Kontrollkästchen **Eingehend** oder **Ausgehend** aus, um alle Dokumente in der ausgewählten Kategorie erneut zu senden. Alternativ hierzu können Sie die Dokumente einzeln erneut senden, indem Sie die Kontrollkästchen für die entsprechenden Dokumente auswählen.

   Anmerkung: Es können nur jeweils eingehende oder ausgehende Dokumente, aber nicht beide Kategorien gleichzeitig erneut gesendet werden.
3. Klicken Sie auf **Erneut senden**.

EDI-Dokumente anzeigen

Zusätzlich zur Unterstützung der Pass-Through-Funktion für EDI-Austauschelemente unterstützt WebSphere Partner Gateway das Entfernen von EDI-Austauschelementen aus Umschlägen und das Einfügen dieser Elemente in Umschläge. Die EDI-Austauschdokumente werden aus ihrem Umschlag entfernt, wenn sie von einem externen Partner oder einem internen Partner empfangen werden. Transaktionsdokumente, die aus dem Umschlag für den eingehenden Austausch entfernt werden, können dann von WebSphere Partner Gateway in derselben Weise verarbeitet werden wie andere Geschäftsdokumente.

WebSphere Partner Gateway fügt EDI-Transaktionen in einen Umschlag ein und generiert EDI-Austauschelemente. Die EDI-Transaktionsdokumente werden generiert, indem XML-, EDI- und ROD-Dokumente in EDI-Transaktionen transformiert werden. EDI-Transaktionsdokumente, die aus dem Umschlag mit EDI-Austauschelementen entfernt wurden, die von WebSphere Partner Gateway empfangen wurden, können in andere EDI-Transaktionsdokumenttypen umgewandelt werden. WebSphere Partner Gateway fügt EDI-Transaktionsdokumente in ein EDI-Austauschdokument ein und sendet dieses anschließend an den gewünschten Empfänger.

Die folgenden Szenarios helfen Ihnen beim Auffinden dieser Informationen:

- „EDI-Dokumentquellentransaktionen anzeigen"
- „EDI-Dokumentempfängertransaktionen anzeigen"
- „Quellenaustausch für EDI-Transaktion suchen" auf Seite 127
- „Zielaustausch für untergeordnete EDI-Transaktion suchen" auf Seite 127

Weitere Informationen zum Entfernen eines EDI-Austauschs aus seinem Umschlag und zum Einfügen eines EDI-Austauschs in einen Umschlag finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

EDI-Dokumentquellentransaktionen anzeigen

WebSphere Partner Gateway entfernt eingehende EDI-Transaktionen aus dem zugehörigen EDI-Austausch.

Gehen Sie wie folgt vor, um die hierbei generierten untergeordneten EDI-Transaktionen anzuzeigen:

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste von Dokumenten an.
4. Klicken Sie neben der Dokument-ID auf das Symbol **Details anzeigen**.
5. Klicken Sie im Abschnitt **Untergeordnete Elemente des Dokuments** auf **Ziel**, um die Details der untergeordneten Dokumentelemente anzuzeigen.

EDI-Dokumentempfängertransaktionen anzeigen

WebSphere Partner Gateway fügt abgehende EDI-Transaktionen in einem Austausch in einen Umschlag ein.

Gehen Sie wie folgt vor, um die untergeordneten Elemente der EDI-Transaktion anzuzeigen, die im generierten Austauschelement enthalten sind:

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
2. Geben Sie die Suchkriterien an, die zum Suchen der von WebSphere Partner Gateway empfangenen EDI-Austauschelemente benötigt werden.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Dokumente an, die mit Ihren Suchkriterien übereinstimmen.
4. Klicken Sie neben der ID des Dokuments, das Sie anzeigen möchten, auf das Symbol **Details anzeigen**.
5. Klicken Sie im Abschnitt **Untergeordnete Elemente des Dokuments** auf **Ziel**, um die Details der untergeordneten Dokumentelemente anzuzeigen.

Quellenaustausch für EDI-Transaktion suchen

Um den Quellenaustausch einer EDI-Transaktion zu ermitteln, können Sie die Dokumentanzeige verwenden. Führen Sie die folgenden Arbeitsschritte aus:

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste von Dokumenten an.

   Für alle EDI-Transaktionen werden nun die Dokument-IDs der Quellenaustauschelemente angezeigt.

Zielaustausch für untergeordnete EDI-Transaktion suchen

Um den Zielaustausch einer untergeordneten EDI-Transaktion zu ermitteln, können Sie die Dokumentanzeige verwenden:

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste von Dokumenten an.
4. Klicken Sie neben der Dokument-ID auf das Symbol **Details anzeigen**.
5. Klicken Sie im Abschnitt **Dokumentereignisse** auf **Informationen**.
6. Klicken Sie neben der in den Umschlag eingefügten EDI-Transaktion in der Spalte **Ereignisname** auf das Symbol **Erweitern**.
7. Suchen Sie die Aktivitäts-ID des Umschlags und kopieren Sie diese aus der Liste **Ereignisdetails**.
8. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
9. Fügen Sie die Aktivitäts-ID des Umschlags ins Feld **Referenz-ID** ein und klicken Sie dann auf **Suchen**.

   In der Dokumentanzeige werden nun die Zielaustauschinformationen angezeigt.

Dokumentvalidierungsfehler

Gehen Sie wie folgt vor, um Dokumentvalidierungsfehler anzuzeigen: Klicken Sie auf der Seite **Dokumentdetails**, Registerkarte **Dokumentanzeige**, auf das Symbol **Dokumente anzeigen**. Auf der Seite **Dokumentvalidierungsfehler** werden die folgenden Felder angezeigt:

- XML-Feld: Zeigt den XPath-Ausdruck des XML-Elements an, das den Fehler verursacht hat.

- Wertbeschreibung: Zeigt den fehlerhaften Wert an, der für das gezeigte Element nicht akzeptiert wird.
- Fehlerbeschreibung: Beschreibt die Fehlerbedingung und den erwarteten korrekten Elementwert.

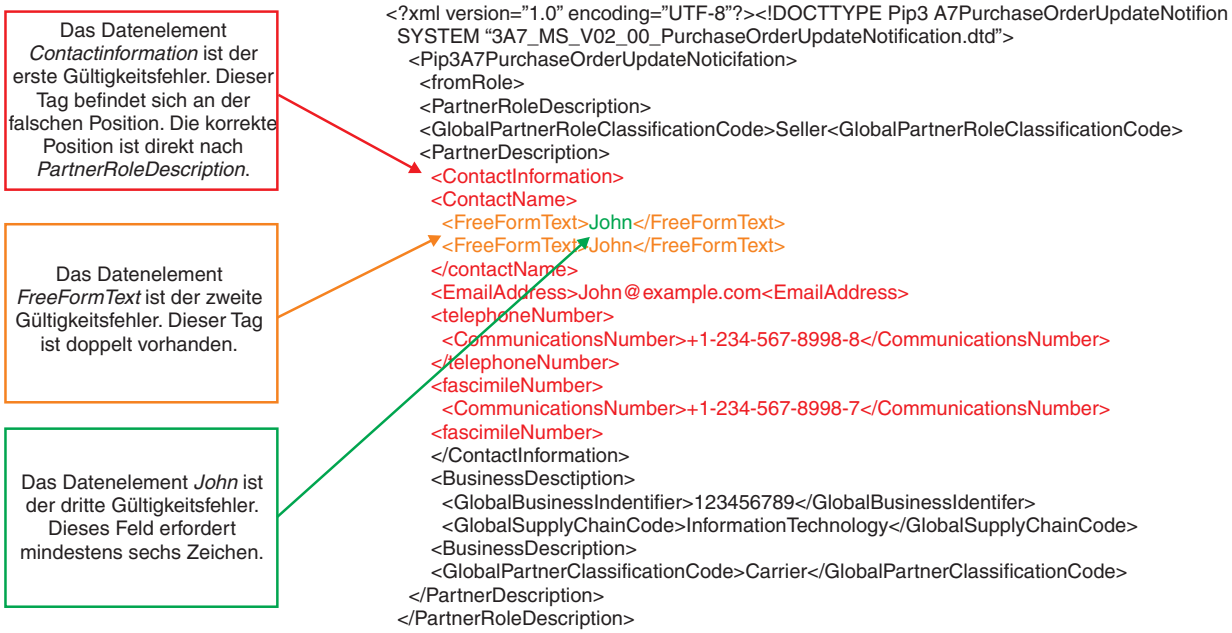
Datenvalidierungsfehler anzeigen

Mithilfe des farbig codierten Textes, der in XML-Feldern verwendet wird, die Validierungsfehler enthalten, können Sie schnell und einfach nach Dokumenten suchen, deren Verarbeitung fehlgeschlagen ist. Felder, in denen ein Validierungsfehler festgestellt wurde, sind rot markiert. Wenn bis zu drei verschiedene Validierungsfehler innerhalb eines verschachtelten XML-Feldes auftreten, werden verschiedene Farben benutzt, um zwischen den Fehlerfeldern zu unterscheiden, wie auch in Tabelle 33 dargestellt.

Tabelle 33. Farblich markierte Dokumentvalidierungsfehler

Wert	Beschreibung
Rot	Erster Validierungsfehler
Orange	Zweiter Validierungsfehler
Grün	Dritter Validierungsfehler

Im Folgenden sehen Sie ein Beispiel für verschachtelte XML-Validierungsfehler



Beispiel für nicht verschachtelte XML-Validierungsfehler:

Einzelheiten über das Anzeigen von Validierungsfehlern in einem unformatierten Dokument finden Sie in Abschnitt „Unformatierte Dokumente anzeigen” auf Seite 121.

Einschränkungen: Die Community Console zeigt nur die ersten 100 KB eines unformatierten Dokuments. Validierungsfehler über 100 KB können nicht angezeigt werden.

Momentan bearbeitetes Dokument stoppen

In diesem Abschnitt wird beschrieben, wie ein in der Verarbeitung befindliches Dokument, das teilweise von einem Partner an einen anderen Partner gesendet wurde, gestoppt wird. Ein in der Verarbeitung befindliches, teilweise gesendetes Dokument kann gestoppt werden, um den Verarbeitungsfortschritt des an den empfangenden Partner zugestellten Dokuments zu verfolgen und auf diese Weise Probleme, die möglicherweise beim Übertragungsprozess auftreten, zu beheben. Klicken Sie auf **Prozess stoppen**, um ein Dokument zu stoppen, das momentan zugestellt wird. Wenn Sie für ein Dokument in der Konsole auf **Prozess stoppen** klicken, beginnt das System mit dem Prozess zum Stoppen des Dokuments und das Symbol **Stopp übergeben** wird angezeigt. Wenn der Hubbetreiber auf **Prozess stoppen** klickt, wird die Zustellung des aktuellen Dokuments gestoppt. Daher wird das Dokument nicht an den empfangenden Partner zugestellt. Wenn die Zustellung des teilweise gesendeten Dokuments gestoppt wird, wird ein Fehlerereignis protokolliert. Dieses Fehlerereignis enthält hilfreiche Informationen für den Hubbetreiber zur Fehlersuche.

Anmerkung: Es kann bis zu einer Stunde dauern, bevor das System die Verarbeitung eines Dokuments stoppt. Während dieser Zeit zeigt die Dokumentanzeige den Dokumentstatus weiterhin als "wird ausgeführt" an.

Fehlgeschlagene und erfolgreiche Dokumente erneut senden

Sie können fehlgeschlagene Dokumente erneut senden, nachdem Sie die Fehlerursache korrigiert haben. Außerdem können Sie bereits erfolgreich verarbeitete Dokumente erneut senden, falls erforderlich. So kann z. B. ein Partner anfordern, dass

ein Dokument erneut gesendet wird, weil das Originaldokument auf dem Client-Server verloren gegangen ist, bevor es mit dem Back-End-System in Kontakt kam.

Administratoren können die beiden folgenden grundlegenden Dokumenttypen erneut senden:

- **Eingehende** Dokumente, die in WebSphere Partner Gateway vom Back-End-System oder einem Partner empfangen werden. Bei diesen Dokumenten kann es im Empfänger, in der DAE (Document Acquisition Engine) oder in der BPE (Business Process Engine) zu Fehlern kommen.
- **Abgehende** Dokumente, die von WebSphere Partner Gateway an das Back-End-System oder den Partner gesendet werden. Bei diesen Dokumenten kann es entweder in der BPE oder im Zustellmanager zu Fehlern kommen.

Wenn Sie ein fehlgeschlagenes **eingehendes** Dokument erneut senden möchten, wählen Sie **Eingang** aus, und klicken Sie auf **Erneut senden**. Daraufhin wird das Dokument abhängig davon, in welcher Komponente der Fehler auftrat, von der DAE oder der BPE erneut übergeben. In der DAE können Fehler bei **eingehenden** Dokumenten in folgenden Fällen auftreten:

- Die Größe des empfangenen Dokuments überschreitet die maximal zulässige Dokumentgröße.
- Die Überprüfung der Unbestreitbarkeit des empfangenen Dokuments ist fehlgeschlagen.
- Der Versand des Dokuments an die BPE ist fehlgeschlagen.

In der BPE können Fehler bei **eingehenden** Dokumenten in folgenden Fällen auftreten:

- Fehler beim festgelegten eingehenden Arbeitsablauf
  - Beim Entpacken können in den Nachrichten Fehler bei der Entschlüsselung der Nachricht oder bei der Überprüfung der Signatur auftreten. Diese Fehler können durch Fehler in der Zertifikatskonfiguration beim Partner oder auf dem Hub hervorgerufen werden.
  - Die B2B-Funktionalitäten des Partners wurden nicht konfiguriert.
- Fehler beim variablen Arbeitsablauf
  - Die Validierungszuordnungen wurden nicht konfiguriert.
  - Es wurden fehlerhafte Umsetzungszuordnungen konfiguriert.

Anmerkung: Dokumente, bei denen Fehler im Empfänger aufgetreten sind, werden erneut übergeben, nachdem der Administrator den Fehler behoben hat.

Wenn Sie ein fehlgeschlagenes **ausgehendes** Dokument erneut senden möchten, wählen Sie **Ausgang** aus, und klicken Sie auf **Erneut senden**. Daraufhin wird das Dokument abhängig davon, in welcher Komponente der Fehler auftrat, von der BPE oder dem Zustellmanager erneut übergeben.

Fehler bei **abgehenden** Dokumenten können in folgenden Fällen auftreten:

- Bei einem BPE-Fehler ist die erneute Übergabe des **abgehenden** Dokuments selbst nicht sinnvoll. In diesem Fall sollte das **eingehende** Dokument nochmals übergeben werden. Hierdurch wird sichergestellt, dass alle Fehler im BPE-Datenfluss, die bereits korrigiert wurden, auch berücksichtigt werden. Als Beispiel für eine derartige Korrektur kann ein Fehler bei der Transformation aufgeführt werden. Bei BPE-Fehlern in **abgehenden** Dokumenten kann es sich um Fehler im festgelegten abgehenden Arbeitsablauf handeln. Hierbei kann das Packen der

Nachricht während der Verschlüsselung oder des Erstellens der Signatur aufgrund fehlerhafter Zertifikatskonfigurationen für den Partner oder den Hub fehlschlagen.

- Bei Fehlern im Zustellmanager gilt Folgendes:
  - Wurde das Problem durch einen Fehler im BPE-Datenfluss verursacht, muss das **eingehende** Dokument nochmals übergeben werden. Hierdurch wird sichergestellt, dass alle Korrekturen, die am BPE-Datenfluss durchgeführt wurden, auch übernommen werden. Dies gilt z. B. dann, wenn die Zielinformationen fehlerhaft waren.
  - Wurde das Problem durch einen anderen Fehler verursacht (z. B. durch einen Ausfall des Zieltransports), kann das **abgehende** Dokument nochmals übergeben werden. Allerdings können Sie in diesem Fall auch das **eingehende** Dokument erneut übergeben.

Implizit wird davon ausgegangen, dass in der Zwischenzeit keine Änderungen vorgenommen wurden, die zum Scheitern der erneuten Übergabe führen könnten. Dies gilt insbesondere für die DAE und die BPE. Wurde das **eingehende** Dokument z. B. verschlüsselt, dann wird davon ausgegangen, dass die zur Entschlüsselung des Dokuments verwendeten Zertifikate nicht geändert wurden und mit den Zertifikaten identisch sind, die zur Verschlüsselung des Dokuments verwendet wurden. Der Administrator muss hierbei alle potenziellen Auswirkungen eines erneuten Versands berücksichtigen.

Wenn das **eingehende** Dokument erneut gesendet wird, wird es durch sämtliche Schritte des Workflowprozesses geleitet. Beispiel: Wenn ein Dokument die AS2-Anforderung eines Partners repräsentiert und eine MDN erforderlich ist, wird die MDN an den Partner gesendet, obwohl eine MDN eventuell schon bei der ersten Verarbeitung des Dokuments gesendet wurde. Die Prüfung der doppelten Dokument-ID wird umgangen. Allerdings wird je nach Geschäftsprotokoll eine doppelte Dokument-ID möglicherweise entdeckt und eine entsprechende Warnung ausgegeben.

Gehen Sie wie folgt vor, um ein Dokument erneut zu senden:

1. Klicken Sie auf **Anzeigen** > **Dokumentanzeige**. Das System öffnet das Fenster **Dokumentanzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste von Dokumenten an.
4. Wählen Sie das Dokument oder die Dokumente aus, die Sie erneut senden möchten.

   Anmerkung: Wenn Sie ein mit Ping überprüftes ebMS-Dokument erneut senden, wird ein neues Pingdokument erstellt.
5. Klicken Sie auf **Erneut senden**.

   Nach der Verarbeitung des erneuten Versands erhalten Sie eine Bestätigungsnachricht.

ebMS-Anzeige

Der ebXML-Nachrichtenübertragungsservice (ebMS genannt) bietet eine standardisierte Methode zum Austausch von Geschäftsnachrichten zwischen ebXML-Geschäftspartnern. ebMS ermöglicht den zuverlässigen Austausch von Geschäftsnachrichten, ohne ausschließlich mit proprietären Technologien und Lösungen zu arbeiten. Eine ebXML-Nachricht enthält Strukturen für einen Nachrichtenheader (der für das Weiterleiten und die Zustellung notwendig ist) und einen Nutzdaten-

bereich. Eine ebXML-Nachricht ist ein Kommunikationsprotokoll, das von mit einem Umschlag versehenen MIME- oder Multipart-Nachrichten unabhängig ist.

ebMS-Prozesse suchen

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**. Das System öffnet das Fenster **ebMS-Anzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.

Wert	Beschreibung
Startdatum und Zeit	Datum und Uhrzeit des Prozessbeginns.
Enddatum und Zeit	Datum und Uhrzeit des Prozessendes.
Quellenpartner	Gibt den absendenden Partner an.
Zielpartner	Gibt den empfangenden Partner an.
Quellengeschäfts-ID	Geschäfts-ID des einleitenden Partners.
Betriebsmodus	Produktion, Test, Externer Partner für RN-Simulator oder Interner Partner für RN-Simulator. Der Typ "Test" ist nur auf Systemen verfügbar, die den Betriebsmodus "Test" unterstützen.
Protokoll	Für die Partner verfügbare Protokolle.
Dokumenttyp	Der Name des Quellendokumenttyps, mit dem das Dokument weitergeleitet wird.
Dialog-ID	Eindeutige ID zum Identifizieren des Datenaustauschs.
Sortieren nach	Ergebnisse sortieren nach: • Zielzeitmarke • Dokumenttyp Der Standardwert ist "Zielzeitmarke".
Absteigend oder Aufsteigend	"Absteigend" zeigt zuerst die neuste Zeitmarke oder den Anfang des Alphabets an. "Aufsteigend" zeigt zuerst die älteste Zeitmarke oder das Ende des Alphabets an. Der Standardwert ist "Absteigend".
Ergebnisse pro Seite	Zeigt *n* Ergebnisse pro Seite an.

3. Klicken Sie auf **Suchen**. Das System zeigt die ebMS-Prozesse an, die Ihren Suchkriterien entsprechen.

ebMS-Prozessdetails anzeigen

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**. Das System öffnet das Fenster **ebMS-Anzeige - Suche**.
2. Wählen Sie die Suchkriterien in den Listen aus.
3. Klicken Sie auf **Suchen**. Das System zeigt die Ergebnisse Ihrer Suche an, wie in Tabelle 34 beschrieben.

Tabelle 34. ebMS-Verarbeitungsdetails

Wert	Beschreibung
Partner	Partner, die in den Geschäftsprozess eingebunden sind.
Zeitmarken	Datum und Uhrzeit, zu dem bzw. der das erste Dokument verarbeitet wird.
Dokumenttyp	Spezifischer Geschäftsprozess, z. B. ebMS (2.0): ALMService.
Betriebsmodus	Zeigt die Art des Dokuments an, das ausgetauscht wird.
Synchron	
Prozess-Status	Status des Prozesses, wie vom Empfänger angegeben.

Tabelle 34. ebMS-Verarbeitungsdetails (Forts.)

Wert	Beschreibung
Dialog-ID	Eindeutige Zahl, die dem Prozess durch den einleitenden Partner zugeordnet wird.
Quellenpartner	Einleitender Partner.
Zielpartner	Empfangender Partner.

4. Klicken Sie neben dem ebMS-Prozess, den Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt Details und zugehörige Dokumente für den ausgewählten Prozess an, einschließlich des Dialogstatus. Der Dialogstatus gibt an, welcher Prozess als nächstes erfolgt (Beispiel: Warten auf Bestätigung). Wenn der Dialogstatus abgeschlossen ist, wurden alle untergeordneten Elemente verarbeitet.
5. Klicken Sie neben dem Dokument, das Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt das Dokument und die zugehörigen Ereignisdetails an. Wenn Sie die vollständige Datei anzeigen wollen, können Sie sie mithilfe der Option zum Kopieren auf die lokale Platte herunterladen.

Unformatierte Dokumente anzeigen

Verwenden Sie diese Prozedur, um ein unformatiertes Dokument anzuzeigen, das einer ebMS-Transaktion zugeordnet ist.

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**. Das System öffnet das Fenster **ebMS-Anzeige - Suche**.
2. Geben Sie die Suchkriterien ein oder wählen Sie sie aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Prozesse an.
4. Klicken Sie neben dem Prozess, den Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt Prozessdetails und zugehörige Dokumente für den ausgewählten Prozess an.
5. Klicken Sie neben dem Dokumenttyp auf das Symbol **Unformatiertes Dokument anzeigen**, um das unformatierte Dokument anzuzeigen.

Einschränkungen:

1. Unformatierte Dokumente, die größer als 100 KB sind, werden abgeschnitten. Wenn sich die Signatur z. B. unten im unformatierten Dokument (Datei mit Erweiterung `.rno`) befindet und die Größe des unformatierten Dokuments 100 KB überschreitet oder wenn die Signatur nach den ersten 100 KB der `.rno`-Datei aufgeführt ist, wird die Signatur nicht in der Dokumentanzeige angezeigt.
2. Die Anzeige für unformatierte Dokumente zeigt möglicherweise keine Dokumentanhänge an. Klicken Sie zum Anzeigen von Anhängen in der Anzeige für unformatierte Dokumente auf die Verknüpfung **Kopieren**, um die Datei einschließlich Anhängen auf Ihrem lokalen Datenträger zu speichern.

Tipps:

- Zur Fehlerbehebung von Dokumenten, deren Verarbeitung fehlgeschlagen ist, siehe auch „Datenvalidierungsfehler anzeigen" auf Seite 128.
- Die Anzeige für unformatierte Dokumente zeigt den HTTP-Header mit dem unformatierten Dokument an.

Dokumentstatus anfordern und anzeigen

Mit dieser Prozedur können Sie den Status eines Dokuments anzeigen.

Anmerkung: Status können nur angefordert werden, wenn der Dokumentstatus anstehend ist und die Funktion "Status anfordern" aktiviert ist.

1. Klicken Sie auf **Anzeigen** > **ebMS-Anzeige**. Das System öffnet das Fenster **ebMS-Anzeige - Suche**.
2. Geben Sie die geeigneten Suchkriterien ein oder wählen Sie sie aus.
3. Klicken Sie auf **Suchen**. Das System zeigt eine Liste der Prozesse an.
4. Klicken Sie neben dem Prozess, den Sie anzeigen möchten, auf das Symbol **Details anzeigen**. Das System zeigt Prozessdetails und zugehörige Dokumente für den ausgewählten Prozess an.
5. Wählen Sie in der Liste mit den Details ein Dokument aus und klicken Sie auf **Status anfordern**.
6. Wenn das System den Status empfängt, wird **Status anzeigen** auf der Seite angezeigt. Klicken Sie auf **Status anzeigen**.

   Wenn das Dokument immer noch anstehend ist, zeigt der Status den letzten Stand des mit einer Zeitmarke versehenen Dokuments an.

Zielwarteschlange

In der **Zielwarteschlange** können Dokumente angezeigt werden, die in der Warteschlange stehen, um von einem beliebigen Ziel im System übermittelt zu werden. Mit der Zielwarteschlange können Sie außerdem alle Ziele anzeigen, für die Dokumente zur Zustellung in der Warteschlange stehen, sowie Dokumente in einer Warteschlange anzeigen und entfernen und Ziele aktivieren oder inaktivieren. Weitere Informationen finden Sie in Kapitel 9, „Zielwarteschlange verwalten”, auf Seite 95.

Kapitel 12. Produktionsdatenverkehr simulieren

Der RosettaNet Partner Simulator (RN-PS) kann eingesetzt werden, bevor und nachdem die Hub-Community aktiviert wurde, um den Produktionsdatenverkehr (Anforderungen, Antworten und Bestätigungen) zwischen dem internen Partner und einem externen Partner zu simulieren; der externe Partner wird in dieser Beschreibung von RN-PS als VTP bezeichnet (Virtual Test Partner - virtueller Testpartner).

Der Zweck des RN-PS ist Folgender:
- Bietet die Möglichkeit, einen externen Partner zu simulieren, der eine RN-Anforderung über den Hub an den internen Partner sendet.
- Bietet die Möglichkeit, das Unternehmenssystems des internen Partners zu simulieren, das eine RNSC-Anforderung (RNSC = RosettaNet Service Content) über den Hub an den externen Partner sendet.

Der interne Partner verwendet den RN-PS, um zu prüfen, ob die Dokumente korrekt formatiert wurden und gültige Geschäftsinhalte enthalten.

Der RN-PS ermöglicht dem internen Partner das Testen seiner Back-End-Systeme (Document Manager und Empfänger), ohne dass diese Tests von den eigenen Back-End-Anwendungen aus gestartet und ohne dass Daten von einem Partner übertragen werden müssen. Somit können Tests ausgeführt werden, ohne Testsysteme oder Mitarbeiter der technischen Unterstützung einzusetzen.

Zur Einleitung des Tests lädt der interne Partner ein Testdokument hoch. Diese Komponente akzeptiert ausschließlich RNIF Version 2.0 (DTD-basierte PIPs); sie ist nicht mit RNIF Version 1.1 kompatibel. Das Testdokument muss eine RosettaNet Service Content-Datei sein; Sie können kein RosettaNet-Objekt (RNO) hochladen. Service-Content ist die primäre Komponente der Nutzdaten einer RosettaNet-Geschäftsnachricht. Es handelt sich dabei um ein XML-Dokument, das den Geschäftsinhalt darstellt, der von einem bestimmten PIP angegeben wurde. Die Nutzdaten enthalten außerdem etwaige Dateianhänge. WebSphere Partner Gateway verwendet das Testdokument, um Routing- und Verarbeitungsinformationen anzugeben.

Wenn ein RN-Dokument mithilfe des RN-PS an WebShere Partner Gateway gesendet wird, wird eine Dokumentbestätigung generiert. Wenn eine 3A4-Bestätigung an den RN-PS gesendet wird, schließt Document Manager den Austausch mit 0A1.

Beachten Sie, dass während des Installationsprozesses ein Sinkziel (d. h. ein Bit-Bucket) erstellt wird, um Bestätigungen während des Testprozesses zu empfangen:

`http://<hostname>:<port#>/console/sink`

oder

`https://<hostname>:<port#>/console/sink`

Dieses Kapitel enthält die folgenden Abschnitte:

Tests vorbereiten

Bevor Sie den Test starten, müssen Sie die folgenden Tasks ausführen, die abhängig von der zu simulierenden Rolle (Anforderung oder Antwort des internen Partners bzw. eines Partners) variieren können:

1. Prüfen Sie die von Ihnen konfigurierten Verbindungen und vergewissern Sie sich, dass das Testszenario korrekt konfiguriert wurde. Stellen Sie insbesondere sicher, dass die in der Verbindung konfigurierten Ziele aktiv sind.
2. Prüfen Sie, ob Ihre Empfänger aktiviert und mit der korrekten URL für ankommende Nachrichten konfiguriert sind. Für die unterschiedlichen Empfänger tritt unterschiedlicher Datenverkehr auf.

   Diese Voraussetzung findet nur dann Anwendung, wenn Sie ein Dokument testen, das eine Antwort erfordert. Weitere Informationen zu Empfängern finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.
3. Prüfen Sie die Geschäfts-IDs im Header Ihres Testdokuments. Die Geschäfts-IDs steuern den Routing-Prozess und legen fest, wohin das Dokument gesendet wird.

   Wenn Sie z. B. Ihr Dokument an sich selbst, also den internen Partner senden, muss die "Empfänger"-Geschäfts-ID im Dokument-Header Ihre eigene Geschäfts-ID sein. Das System verwendet die "Empfänger"-Geschäfts-ID zum Suchen nach der korrekten Verbindung.

Im Folgenden wird ein Beispiel für die "Absender-" und "Empfänger-"-Geschäfts-IDs in einem Testdokument dargestellt (nicht relevante Zeilen wurden ausgelassen):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Preamble SYSTEM "3A4_MS_V02_02_PurchaseOrderRequest.dtd">
<Pip3A4PurchaseOrderRequest>
   <fromRole>
      <GlobalBusinessIdentifier>987654321</GlobalBusinessIdentifier>
   <toRole>
      <GlobalBusinessIdentifier>567890123</GlobalBusinessIdentifier>
```

Testszenarios definieren

Mit dem RN-PS können Sie die Szenarios testen, die in Tabelle 35 dargestellt sind und für den Datenaustausch zwischen Ihnen und Ihren Partnern gelten.

Tabelle 35. Testszenarios

Szenario	Ziel der Verbindung	URL
Unidirektional abgehend - vom internen Partner an einen externen Partner. Simulieren des internen Partners.	VTP_Owner	VTP_OWNER
Unidirektional eingehend - vom externen Partner an den internen Partner. Simulieren des externen Partners.	VTP_TP	Gilt nicht für dieses Szenario.
Bidirektional abgehend - vom internen Partner an einen externen Partner (Anforderung hochladen). Simulieren des internen Partners.	VTP_Owner	VTP_OWNER

Tabelle 35. Testszenarios (Forts.)

Szenario	Ziel der Verbindung	URL
Bidirektional eingehend - vom externen Partner an den internen Partner (Anforderung hochladen). Simulieren des externen Partners.	VTP_TP	VTP_TP
Bidirektional abgehend - vom internen Partner an einen externen Partner (Antwort hochladen).	VTP_TP	VTP_TP
Simulieren des externen Partners. Bidirektional eingehend - vom externen Partner an den internen Partner (Antwort hochladen).	VTP_Owner	VTP_Owner

Beispielszenarios

Dieser Abschnitt beschreibt die Schritte zum Konfigurieren des RN-PS, sodass zwei unidirektionale RosettaNet-Interaktionen (RN-Interaktionen) simuliert werden können. Die Schritte zum Einrichten der RN-Interaktionen werden hier im Zusammenhang mit dem Einrichten von RN-PS beschrieben. Weitere Informationen zur allgemeinen Konfiguration von RosettaNet finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

Sie sehen die Verzeichnisse und die Hubkonfigurationseinstellungen, die der RN-PS verwendet, sodass Sie besser nachvollziehen können, wie Sie der RN-PS beim Debugging von Routingoperationen zwischen Partnern unterstützen kann.

Interner Partner

Richten Sie ein HTTP-Sinkziel für den internen Partner ein. Dies ist ein HTTP-Ziel, das an die URL `http://<konsolen-ip>:<konsolenport>/console/sink` sendet.

Das Sinkziel sollte für den internen Partner als RN-PS-Standardpartner und RN-PS-Managerziel festgelegt werden.

Externer Partner

Richten Sie für den Partner wie zuvor für den internen Partner ebenfalls ein HTTP-Sinkziel ein.

RosettaNet-PIP-XML-Dateien

Das hier beschriebene Szenario ist die 3A4-Interaktion. Die Simulation "Externer-Partner-an-internen-Partner" verwendet XML-Dateien, die den Inhalt der 3A4-Bestellanforderung enthalten.

Die Simulation "Interner-Partner-an-externen-Partner" verwendet XML-Dateien, die dem RNSC-Inhalt der 3A4-Bestellbestätigung entsprechen. Diese XML-Dateien befinden sich in Ihrem lokalen Dateisystem.

Sie finden zugehörige Informationen im Handbuch *WebSphere Partner Gateway Hubkonfiguration*. Wenn Sie die Dateien erstellen, achten Sie darauf, dass die Empfänger- und Absender-IDs mit den IDs des internen Partners und des externen Partners übereinstimmen, die an den entsprechenden Stellen dieser Dateien definiert sind.

Konsol- und Routerserver konfigurieren

Wenn Sie für Ihre Simulation eine Verschlüsselung oder digitale Signaturen verwenden möchten, benötigen Sie Zertifikate mit einem öffentlichen und einem privaten Schlüssel. Verwenden Sie für den privaten Schlüsselspeicher das p8-Format und für das öffentliche Zertifikat das DER-Format.

1. Kopieren Sie die PKCS#8- and DER-Dateien in das Verzeichnis `common/security/vtp`.
2. Kopieren Sie die DER-Datei in das Verzeichnis `common/security/ca`.
3. Wenn es sich um ein selbst signiertes Zertifikat handelt, muss das CA-Zertifikat als Zertifikat des Typs "Root und Intermediate" hochgeladen werden, wobei die Konsole gestartet sein muss. Wenn es sich um ein von einer CA signiertes Zertifikat handelt, muss das CA-Zertifikat als Zertifikat des Typs "Root und Intermediate" hochgeladen werden. Wenn der Zertifikatspfad bis zum Rootzertifikat erstellt werden soll, müssen alle CA-Zertifikate in der Zertifikatskette hochgeladen werden.
4. Ändern Sie die Konfiguration der Community Console, sodass sie auf die Zertifikats- und Schlüsselspeicherdatei verweist.
   a. Verwenden Sie die Konsole, um die RN-PS-Eigenschaften anzuzeigen. Navigieren Sie zu **Systemverwaltung** > **Konsolenverwaltung** > **RN-Simulator**.
   b. Klicken Sie auf das Symbol **Ändern**, damit die Anzeige in den Bearbeitungsmodus versetzt wird. Führen Sie die folgenden Eingaben durch und verwenden Sie dabei die auf Ihr System zutreffenden Werte. Sie müssen die DER- und p8-Dateiformate in der dargestellten Form verwenden.

      ```
      bcg.console.certs.vtp.CertificateDir=C:/<INSTALLATIONSVERZEICHNIS>/common
      /security/vtp
      bcg.certs.vtp.Certificate=testcert.der
      bcg.certs.vtp.PrivateKey=testkey.p8
      bcg.certs.vtp.Passwd=password
      bcg.certs.vtp.VerifySig=false
      bcg.vtp.RouterIn=C:/<INSTALLATIONSVERZEICHNIS>/common/router_in
      ```

   c. Klicken Sie auf die Schaltfläche **Speichern**, damit die Änderungen wirksam werden.
5. Wenn der Konsolserver aktiv ist, starten Sie ihn erneut. Wenn er nicht aktiv ist, starten Sie ihn jetzt.
6. Stellen Sie sicher, dass die Document Manager-Konfiguration korrekt eingerichtet ist.
   a. Verwenden Sie die Konsole, um die Document Manager-Sicherheitseigenschaften anzuzeigen. Navigieren Sie zu **Systemverwaltung** > **DocMgr-Verwaltung** > **Sicherheit**.
   b. Klicken Sie auf das Symbol **Ändern**, damit die Anzeige in den Bearbeitungsmodus versetzt wird.
   c. Ändern Sie den Wert der Eigenschaft `bcg.certs.vtp.CertificateDir`, sodass sie auf dasselbe Verzeichnis verweist wie die Konsole in Schritt 4b. Speichern Sie diese Einstellung für die Eigenschaft.

      Anmerkung: Diese Verzeichnisse sind im Hinblick auf den Server benannt, auf dem die Komponenten installiert sind. Document Manager und die Konsole sollten ein Dateisystem demselben Verzeichnis zuordnen.
7. Wenn der Document Manager-Server aktiv ist, starten Sie ihn erneut. Wenn er nicht aktiv ist, starten Sie ihn jetzt.

3A4-Konnektivität konfigurieren

Wenn Sie mit dem RosettaNet-Routing vertraut sind, konfigurieren Sie die RosettaNet-Konnektivität zwischen einem externen Partner und einem internen Partner, indem Sie die im Folgenden aufgeführten Schritte ausführen.

Wenn Sie nicht mit dem RosettaNet-Routing vertraut sind, finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration* Unterstützung beim Ausführen der folgenden Tasks:

1. Importieren Sie die RN- und RNSC-Dateien, die die 3A4-Interaktionen unterstützen.

   Laden Sie die folgenden Dateien in der gezeigten Reihenfolge hoch. Die Dateien befinden sich im Verzeichnis `/B2Bintegrate/rosettanet` auf der Installations-CD:

   - `Package_RNIF_V02.00.zip`
   - `BCG_Package_RNIFV02.00_3A4V02.02.zip`
   - `Package_RNSC_1.0_RNIF_V02.00.zip`
   - `BCG_Package_RNSC1.0_RNIFV02.00_3A4V02.02.zip`
2. Definieren Sie die Interaktionen für die 3A4-Bestellanforderungen und Bestätigungen, die über den Hub weitergeleitet werden sollen.
3. Konfigurieren Sie die B2B-Funktionalität des internen Partners und des externen Partners als Quelle und Empfänger der 3A4-Partneranforderungen und -bestätigungen, die RNSC-Inhaltsdaten verwenden.
4. Erstellen Sie die Partnerverbindungen zwischen dem internen Partner und dem externen Partner, die für das Szenario benötigt werden, das simuliert werden soll.
5. Richten Sie die Attribute der Verbindung so ein, dass optional digitale Signatur und Verschlüsselung angegeben und die Sicherheitsnebenprodukte verwendet werden, die sich auf Ihrem System befinden.

Wenn in Ihrem Dateisystem 3A4-Anforderungs- und 3A4-RNSC-Beispieldateien im XML-Format gespeichert sind, können Sie mit dem RosettaNet Partner Simulator alle internen Routingfunktionen testen. Wählen Sie die Seite **RosettaNet Partner Simulator** aus und klicken Sie anschließend auf **Durchsuchen**. Wählen Sie eine Datei aus dem Dateisystem aus, die den Inhalt enthält, den Sie weiterleiten möchten, und klicken Sie anschließend auf **Weiterleiten**.

Das Dokument wird aus dem Dateisystem gelesen und in den Hub hochgeladen. Es wird zum Routing an Document Manager übergeben, wobei die Verbindung verwendet wird, die Sie im Hub konfiguriert haben.

Anforderungen und Antworten hochladen und anzeigen

Sie müssen die Fähigkeit Ihres Systems testen, Anforderungen und Antworten zu senden. Das Fenster **Dokument hochladen** wird verwendet, um beide Dokumenttypen hochzuladen.

Wenn Sie eine Anforderung senden, verwenden Sie das zweite Fenster der Komponente, **Dokumenttyp anzeigen**, um das Dokument zu prüfen und sicherzustellen, dass es ordnungsgemäß verarbeitet wurde (anstehende Antwort für ein geöffnetes Dokument). Prüfen Sie Ihre interne Anwendung, um sicherzustellen, dass das Dokument ordnungsgemäß empfangen und verarbeitet wurde. Bearbeiten Sie die Ab-

schnitte "Empfänger" und "Bestimmungsort" der Anforderung mit einem Texteditor, um eine Antwort zu erstellen. Laden Sie anschließend die Antwort hoch.

Wenn Sie eine Antwort senden, können Sie auch das Fenster **Dokumenttyp anzeigen** verwenden, um das Dokument zu untersuchen. Es ist nicht notwendig, eine Antwort zu bearbeiten.

Im Fenster **Dokumenttyp anzeigen** werden keine Dokumente mit anstehender Bestätigung angezeigt.

Nachdem das Hochladen abgeschlossen ist, wird die RN-PS-Sicht durch das Fenster mit den Routingergebnissen ersetzt, das die Links zur RosettaNet-Anzeige und zur Dokumentanzeige enthält. Über diese beiden Links gelangen Sie schnell und einfach zu den entsprechenden Anzeigen, in denen Sie die Routingergebnisse prüfen können. Sie sollten einen Moment abwarten, damit Document Manager die Nachricht bearbeiten kann, bevor Sie versuchen, die Ergebnisse anzuzeigen.

Dokumenttyp einleiten und anzeigen

Diese Funktion bietet ein komfortables Verfahren zum Testen interner Anwendungen, indem der Start und der Empfang von uni- und bidirektionalen RosettaNet-PIPs (Partner Interface Processes) simuliert wird.

Gehen Sie wie folgt vor, um einen Dokumenttyp einzuleiten:

1. Klicken Sie auf **RosettaNet Partner Simulator** > **Dokumenttyp einleiten**. Das System öffnet das Fenster **Dokument hochladen**.
2. Klicken Sie auf **Durchsuchen**, um das RosettaNet Service Content-Dokument zu suchen, das Sie hochladen möchten. Das Dokument muss eine digitale Signatur aufweisen.
3. Klicken Sie auf **Weiterleiten**, um den Testprozess zu starten. Das Dokument wird auf der Basis der dort angegebenen Route-Informationen über das System zur richtigen Zieladresse weitergeleitet.
   - Wenn das Dokument erfolgreich weitergeleitet wurde, zeigt das System eine Nachricht mit den Links zu den RosettaNet- und Dokumentanzeigen. Mit diesen Links können Sie den Routingfortschritt des Dokuments verfolgen.
   - Wenn während des Dokumentroutings ein Fehler auftritt, zeigt das System eine Fehlernachricht an, in der eine Liste der vom System generierten Ereignisse enthalten ist. Korrigieren Sie anhand dieser Informationen die Fehler im Dokument und übergeben Sie es erneut durch den RN-PS.
4. Wenn Sie ein Szenario für eine unidirektionale Übertragung simulieren, ist der Test damit abgeschlossen.

Geöffnetes Dokument suchen

1. Klicken Sie auf **RosettaNet Partner Simulator** > **Dokumentenflüsse anzeigen**.
2. Klicken Sie auf das Symbol **Details anzeigen**, um die Option **Dokumenttyp** zu öffnen und anzuzeigen. Das System öffnet das Fenster für den geöffneten RN-PS-Dokumenttyp.
3. Klicken Sie auf das Symbol **Unformatiertes Dokument anzeigen**, um das unformatierte Dokument anzuzeigen.

Geöffnetes Dokument beantworten

1. Verwenden Sie einen Texteditor, um die Empfänger- und Zielabschnitte des Prozesses zu bearbeiten, für die ein Antwortdokument benötigt wird. (Ändern Sie hierbei VTP_OWNER in VTP_TP, oder ändern Sie VTP_TP in VTP_OWNER.) Führen Sie außerdem die erforderlichen Änderungen an der Empfänger-URL durch. Weitere Informationen zu den Testszenarios finden Sie in Tabelle 36.

Tabelle 36. Testszenarios

Szenario	Ziel der Verbindung	URL
Bidirektional abgehend - vom internen Partner an einen externen Partner (Anforderung hochladen). Simulieren des internen Partners.	VTP_TP	VTP_TP
Unidirektional eingehend - von einem externen Partner an den internen Partner. Simulieren des externen Partners.	VTP_OWNER	VTP_OWNER
Bidirektional abgehend - vom internen Partner an einen externen Partner (Antwort hochladen). Simulieren des externen Partners.	VTP_OWNER	VTP_OWNER
Bidirektional eingehend - vom externen Partner an den internen Partner (Antwort hochladen).	VTP_TP	VTP_TP

2. Klicken Sie auf **RosettaNet Partner Simulator** > **Dokumenttyp anzeigen**.
3. Klicken Sie auf **Antworten** neben dem Dokument, das ein Antwortdokument erfordert.
4. Klicken Sie auf **Durchsuchen** und wählen Sie das bearbeitete Dokument aus.
5. Klicken Sie auf **Weiterleiten**. Das Dokument wird auf der Basis der dort angegebenen Route-Informationen über das System an die richtige Zieladresse weitergeleitet.
6. Klicken Sie auf **Dokumenttyp anzeigen**, um das Dokument anzuzeigen.

Geöffnetes Dokument entfernen

1. Klicken Sie auf **RosettaNet Partner Simulator** > **Dokumenttyp anzeigen**.
2. Klicken Sie neben dem angezeigten Dokument auf **Entfernen**. Das Dokument wird aus dem System gelöscht.

Kapitel 13. Archivierung

WebSphere Partner Gateway stellt eine Archivierungsfunktion zum Archivieren und Bereinigen von Systemdaten bereit. Über die WebSphere Partner Gateway-Konsole können Sie die Task der Archivierungsfunktion so terminieren, dass sie automatisch ohne manuellen Eingriff ausgeführt wird. Wenn Fehler auftreten, können Sie anhand des Berichts und des zugehörigen generierten Fehlerereignisses Maßnahmen zur Fehlerbehebung ergreifen.

Die Task der Archivierungsfunktion wird bei der Installation des WebSphere Partner Gateway-Hubs konfiguriert. Über die Konsole kann die Task der Archivierungsfunktion aktiviert oder inaktiviert werden. Darüber hinaus können Sie die Datensicherung wiederherstellen und nach bestimmten Dokumenten suchen, indem Sie die erforderlichen Parameter in den Filterkriterien angeben.

Als WebSphere Partner Gateway-Systemadministrator können Sie die folgenden Operationen ausführen oder überwachen:

- Die Tasks der Archivierungsfunktion anzeigen und ändern: Abschnitt „Konfiguration der Archivierungsfunktion"
- „Laufzeittasks der Archivierungsfunktion" auf Seite 146: Eine Liste der Laufzeitaktivitäten während der Archivierung abrufen.
- „Berichte der Archivierungsfunktion" auf Seite 147: Den Status der einzelnen Tasks der Archivierungsfunktion anzeigen.
- Bereits archivierte und bereinigte Daten wiederherstellen: Abschnitt „Task der Archivierungsfunktion wiederherstellen" auf Seite 149
- „Benutzereingriff bei der Archivierung" auf Seite 152: Wenn der automatische Zeitplan der Archivierungsfunktion aus irgendwelchen Gründen fehlschlägt, können die Daten manuell archiviert werden.

Konfiguration der Archivierungsfunktion

Eine Task der Archivierungsfunktion ist ein terminierter Prozess, der zur konfigurierten Zeit automatisch ausgeführt wird. Die Task wird während der Installation der WebSphere Partner Gateway-Komponenten konfiguriert. Als Systemadministrator können Sie die Konfigurationsdetails der Archivierungsfunktion anzeigen und ändern. Ferner können Sie die Konfiguration der Archivierungsfunktion für WebSphere Partner Gateway exportieren oder importieren.

Task der Archivierungsfunktion anzeigen

Melden Sie sich zum Anzeigen der Task der Archivierungsfunktion als Administrator an und führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Konfigurieren**.
2. Die folgenden Informationen werden angezeigt:

Tabelle 37. Konfiguration der Archivierungsfunktion

Abschnitt	Feld	Beschreibung
Allgemein	Taskname	Der Name der Archivierungstask. Der Name ist eine Konstante und kann nicht geändert werden.
	Beschreibung	Eine Kurzbeschreibung der Task. Die Beschreibung ist eine Konstante und kann nicht geändert werden.
	Zeit der letzten Ausführung	Das Datum und die Zeit für die Task, die zuletzt ausgeführt wurde. Dieses Feld wird abhängig von der Ausführungszeit der Archivierungsfunktion automatisch aktualisiert und kann nicht bearbeitet werden.
	Zeit der nächsten Ausführung	Das Datum und die Zeit für die Task, die als nächstes ausgeführt werden soll. Dieses Feld wird abhängig von der Ausführungszeit der Archivierungsfunktion automatisch aktualisiert und kann nicht bearbeitet werden.
	Status	Der Status der Task. Er wird im nicht editierbaren Modus angezeigt. Die folgende Werte sind gültig: • Terminiert: Der Status ist standardmäßig auf **Terminiert** festgelegt. Dies bedeutet, dass die Task für die Ausführung terminiert ist. • Wird ausgeführt: Dieser Status wird angezeigt, wenn die Task der Archivierungsfunktion momentan ausgeführt wird. • Wird gestoppt: Dieser Status wird angezeigt, wenn Sie in der Konsole auf **Stoppen** klicken. • Wird terminiert: Dieser Status wird angezeigt, wenn die Konfigurationsänderungen in der Datenbank gespeichert werden. • Wird inaktiviert: Dieser Status wird angezeigt, wenn Sie in der Konsole auf **Inaktivieren** klicken. • Inaktiviert: Dieser Status wird angezeigt, wenn Sie die Task inaktivieren. • Inaktiviert und fehlgeschlagen: Dieser Status wird angezeigt, wenn eine Task während der Ausführung fehlschlägt. Klicken Sie auf 'Wieder aufnehmen', um die Task zu terminieren. Ist der Status **Inaktiviert**, **Wird gestoppt** oder **Wird ausgeführt** können die folgenden Parameter nicht bearbeitet werden:

Tabelle 37. Konfiguration der Archivierungsfunktion (Forts.)

Abschnitt	Feld	Beschreibung
Bereinigung	Aufbewahrungsdauer für Daten in Tagen	Gibt die Anzahl der Tage für die Aufbewahrung der Daten im System an. Danach werden die Daten archiviert oder bereinigt.
	Daten für die Unbestreitbarkeit (NonRep) kopieren	Dieser Wert ist standardmäßig aktiviert, sodass die Unbestreitbarkeitsdaten in der angegebenen Archivposition gespeichert werden. Sie können diesen Wert inaktivieren, wenn die Daten nicht gesichert werden sollen.
	Archivposition für unbestreitbare Dateien	Dieses Feld ist sichtbar, wenn das Kontrollkästchen **Daten für die Unbestreitbarkeit (NonRep) kopieren** ausgewählt ist. Geben Sie das Zielverzeichnis für die Sicherung der Unbestreitbarkeitsdateien an. Das standardmäßig definierte Ziel lautet wie folgt: `<pos_des_gemeins_dateisystems> /dataBackup`
	Archivposition für unbestreitbare Datenbank	Dieses Feld ist sichtbar, wenn das Kontrollkästchen **Kopieren** ausgewählt ist. Geben Sie das Zielverzeichnis für die Sicherung der Datenbank an. Das standardmäßig definierte Ziel lautet wie folgt: `<DBLoader>/dbBackup` (für DB2) oder `<ORACLE_HOME>/oradata/ <ORACLE_SID>/dbBackup` (für Oracle). **Anmerkung:** Sie müssen einen vollständig qualifizierten Pfad angeben, für den der Datenbankbenutzer über Schreibberechtigungen verfügt.
Zeitplan für Bereinigung	Täglicher, Wöchentlicher oder Angepasster Zeitplan	Der Zeitplan für die Ausführung der Task der Archivierungsfunktion (täglich, wöchentlich oder benutzerdefiniert). Die Zeitangabe erfolgt im Format HH:MM (Greenwich Mean Time).
Archivierungskriterien	Die folgenden Parameter werden zur optionalen Filterung der zu archivierenden Daten verwendet. Sie werden nur zur Datensicherung und nicht zur Bereinigung verwendet; d. h., die Daten werden ungeachtet dieser Werte bereinigt. Dieser Abschnitt wird nur angezeigt, wenn das Kontrollkästchen **Daten für die Unbestreitbarkeit (NonRep) kopieren** ausgewählt wurde.	
	Sendender Partner	Der Name des sendenden Partners. Der Standardwert ist **Alle**.
	Paket	Das Paket (Paketname und -version), das archiviert werden muss. Der Standardwert ist **Alle**.
	Protokoll	Das Protokoll (Protokollname und -version), das archiviert werden muss. Der Standardwert ist **Alle**.
	Dokumenttyp	Das Dokument (Dokumenttyp und -version), das archiviert werden muss. Der Standardwert ist **Alle**.

Änderung der Task der Archivierungsfunktion

Führen Sie die folgenden Schritte aus, um die Task der Archivierungsfunktion zu ändern:

1. Klicken Sie auf **Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Konfigurieren**. Die Task der Archivierungsfunktion wird im Anzeigemodus angezeigt.
2. Klicken Sie auf das Symbol **Bearbeiten**, um die erforderlichen Parameter zu ändern. Detaillierte Informationen zu diesen Parametern finden Sie in Tabelle 37 auf Seite 144.
3. Klicken Sie auf **Speichern**, um die Konfiguration der Archivierungsfunktion zu speichern. Der Status wird in **Wird terminiert** geändert.
4. Es wird ein Ereignis veröffentlicht, um die Schedulerkomponente auszulösen. Der Scheduler liest die Taskkonfiguration und aktualisiert die WebSphere Application Server-Konfiguration. Die Datenbanktabellen werden mit den Konfigurationsdaten aktualisiert, die während der Ausführung der Task der Archivierungsfunktion und der Berichterstellung verwendet werden.
5. Der Status wird dann von **Terminiert** in **Wird terminiert** geändert.

Eine fehlgeschlagene Task der Archivierungsfunktion können Sie zurücksetzen, indem Sie **Wieder aufnehmen** auswählen.

Konfiguration der Archivierungsfunktion exportieren und importieren

Detaillierte Informationen zum Exportieren und/oder Importieren der Konfiguration der Archivierungsfunktion finden Sie in Kapitel 6, „Partnermigration verwalten", auf Seite 69.

Laufzeittasks der Archivierungsfunktion

Während der Laufzeit wird die Archivierungsaktivität wie folgt ausgeführt:

1. Die Task der Archivierungsfunktion wird vom System gestartet.
2. Die Konfiguration wird gelesen und die entsprechenden Daten werden in den Sicherungspositionen gespeichert.
3. Das gemeinsame Dateisystem und die Datenbanktabellen werden bereinigt.

Im Folgenden wird der Laufzeitdatenfluss der Archivierungsfunktion beschrieben:

1. Die terminierte Task der Archivierungsfunktion wird gemäß dem konfigurierten Zeitplan ausgeführt.
2. Die Archivierungsfunktion setzt sich in der Datenbank selbst auf den Status **Wird ausgeführt**. Derselbe Status wird in diesem Fall in der Konsole angezeigt.
3. Die Archivierungsfunktion liest die gespeicherte Konfiguration aus der Datenbank. Die Konfiguration wird während des Statusübergangs von **Wird terminiert** in **Terminiert** in der Datenbank gespeichert.
4. Wenn das Attribut **Kopieren** in der Konfiguration der Archivierungsfunktion ausgewählt wurde, geschieht Folgendes:
   a. Die Archivierungsfunktion entnimmt die Sicherung des Unbestreitbarkeitsspeichers aus der Datenbank. Die Zeilen aus der Tabelle LG_MSG_ARCHIVE werden in die Dateien in dem Verzeichnis exportiert, das in der Archivzielposition der Datenbank angegeben wurde. Die Zeilen aus der Tabelle LG_CERT_ARCHIVE werden ebenfalls exportiert.

b. Die Archivierungsfunktion kopiert den Inhalt des Unbestreitbarkeitsordners in die Sicherungsposition.

   Anmerkung: Die Kriterien bezüglich der Datensicherung basieren auf der Konfiguration der Task der Archivierungsfunktion.

5. Die Archivierungsfunktion bereinigt die Dateien aus dem gemeinsamen Dateisystem. Alle Dateien, die älter als das angegebene Begrenzungsdatum sind, werden gelöscht.
6. Die Archivierungsfunktion bereinigt die Daten aus den Tabellen in der Datenbank. Alle Daten, die vor dem Begrenzungsdatum aktualisiert oder erstellt wurden, werden gelöscht.
7. Dann wird die Task der Archivierungsfunktion als **Erfolgreich** markiert und die Zeitmarke in den Datenbanktabellen des Berichts wird aktualisiert.

Szenarios mit Ausnahmebedingung

Sollten während der beschriebenen Laufzeitphasen Fehler auftreten, wird die Ausführung der Task der Archivierungsfunktion gestoppt. In einem solchen Szenario kommt es zu den folgenden Aktivitäten:

- Die Archivierungsfunktion protokolliert den aufgetretenen Fehler in der Serverprotokolldatei.
- Der Task der Archivierungsfunktion wird ein Fehlerereignis zugeordnet. Dieses Fehlerereignis wird in der Datenbank protokolliert.
- Es kann auch ein Alert für ein bestimmtes Fehlerereignis definiert werden, damit ein Alert generiert wird, sobald ein bestimmter Fehler auftritt.
- Die Task der Archivierungsfunktion stoppt die weitere Zeitplanung. Die Konfiguration der Archivierungsfunktion muss nach der Behebung des Fehlers manuell zurückgesetzt werden.

Wichtig: Wird die Task der Archivierungsfunktion ausgeführt, ohne dass für die angegebene Position des Dateiziels Schreibberechtigungen erteilt wurden, wird eine Datenbereinigung ausgeführt. Obwohl der Export der Daten aus der Tabelle LG_MSG_ARCHIVE wie erwartet unvollständig ist, muss die Datenbereinigung nicht auftreten. Wenn sich die Archivierungsfunktion im Status 'Inaktiviert und fehlgeschlagen' befindet und Probleme beim Kopieren von Unbestreitbarkeitsdaten in das Dateisystem auftreten, können Sie die Unbestreitbarkeitsdaten manuell sichern.

Berichte der Archivierungsfunktion

Melden Sie sich zum Anzeigen des Berichts der Archivierungsfunktion als Administrator an und navigieren Sie zu **Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Konfigurieren**. Auf dieser Seite werden die vorhandenen Taskinstanzen der Archivierungsfunktion angezeigt, die bereits ausgeführt wurden.

Die folgenden Informationen werden angezeigt, wenn Sie auf den Bericht der Archivierungsfunktion zugreifen:

- Gestartet um (Datum/Uhrzeit): Das Datum und die Uhrzeit
- Beendet um (Datum/Uhrzeit): Das Datum und die Uhrzeit
- Status: 'Erfolgreich', 'Fehlgeschlagen', 'Gestoppt' oder 'Wird ausgeführt'
- Anzahl der bereinigten Zeilen sowie die Start- und Endzeit. Diese Informationen stammen aus den folgenden Tabellen:

Tabelle 38. Datenbereinigungstabellen

Daten	Tabelle
Nachrichtenarchiv (Message Archive)	LG_MSG_ARCHIVE
Aktivitätenprotokollierung (Activity Logging)	LG_ACTIVITY_RNDTL
	LG_ACTIVITY_RNHDR
	LG_AS_DTL
	LG_AS_HDR
	LG_STATUS_ACTIVITY
	LG_B2BPROCESS_HDR
	LG_VALIDATION
	LG_ACTIVITY_DTL
	LG_ACTIVITY_ENDSTATE
	BP_PROCESS_LOG
	LG_DELIVERY_LOG
	LG_SYNCH_REQ_RESP
	LG_ACTIVITY_EVENT
	LG_ACTIVITY
	LG_STACKTRACE
	LG_EVENT
	LG_ACK
	LG_CHAIN
	LG_EDI_FA_RECONCILE
	LG_ENVELOPE_INCLUSION

Tabelle 38. Datenbereinigungstabellen (Forts.)

Daten	Tabelle
Statusengine (State Engine)	BP_RNSTATEHDRAUDITLOG
	BP_RNMSGDIGEST
	BP_SPONSOR_STATE
	BP_RNSTATEDTL
	BP_RNSTATEHDR
	BP_AS_STATE_DTL
	BP_AS_STATE_HDR
	BP_STATE_HDR
	BP_RM_STATE_DTL
	BP_RM_STATE_HDR
	BP_SPONSOR_STATE_EBMS
	BP_DUPCHECK
	LG_SUMMARY_MI
	LG_SUMMARY_RN
	LG_SUMMARY_RN_MI
	LG_EVENT_EVENTSUMMARY
	LG_EVENTSUMMARY
	LG_ACTIVITY_SUMMARY
	LG_SUMMARY

- Anzahl der aus LG_MSG_ARCHIVE gelöschten Zeilen.
- Konfigurationseinstellungen, die für eine bestimmte Task aktiviert wurden.
- Konfigurierter Bereinigungszeitplan.
- Verwendete Archivierungskriterien wie z. B. sendender Partner, Paket, Protokoll und Dokumenttyp. Diese Angabe wird nur angezeigt, wenn bei der Ausführung der Archivierungstask die Option **Daten für die Unbestreitbarkeit (NonRep) kopieren** ausgewählt war.

Task der Archivierungsfunktion wiederherstellen

WebSphere Partner Gateway ermöglicht die Wiederherstellung der Daten, die archiviert und aus dem System gelöscht wurden.

Eine Wiederherstellung kann nur dann ausgeführt werden, wenn das Dateisystem und die Datenbank von WebSphere Partner Gateway verfügbar sind und mindestens eine Archivierungs- und Bereinigungstask erfolgreich ausgeführt wurde.

Gehen Sie wie folgt vor, um eine Wiederherstellung auszuführen:

1. Melden Sie sich als Administrator an und navigieren Sie zu **Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Wiederherstellen**.
2. Geben Sie den Datumsbereich an, indem Sie das **Startdatum** und das **Enddatum** eingeben.
3. Geben Sie das Verzeichnis für **Archivposition für unbestreitbare Dateien** an, in dem die Daten gespeichert sind. Diese Speicherposition wird nach Dateien

durchsucht, die während der Archivierung aus dem Ordner NONREP gesichert wurden. Der Standardwert wird aus der letzten Konfiguration der Archivierungstask übernommen. Die Wiederherstellung schlägt fehl, wenn sie im angegebenen Pfad keine Daten lesen kann, beispielsweise wenn das Verzeichnis nicht vorhanden ist.

4. Geben Sie das Verzeichnis für die **Archivposition für unbestreitbare Datenbank** an. Diese Speicherposition wird nach Dateien durchsucht, die während der Archivierung aus dem Ordner NONREP gesichert wurden. Der Standardwert wird aus der letzten Konfiguration der Archivierungstask übernommen. Die Wiederherstellung schlägt fehl, wenn sie im angegebenen Pfad keine Daten lesen kann, beispielsweise weil das Verzeichnis nicht vorhanden ist.
5. Wählen Sie das Kontrollkästchen **Anhängen** aus, wenn die Daten bei der Wiederherstellung angefügt werden sollen. Ist dieses Kontrollkästchen nicht ausgewählt, werden vorhandene Daten durch die wiederhergestellten Daten überschrieben. Das Kontrollkästchen ist standardmäßig nicht ausgewählt.
6. Klicken Sie auf **Wiederherstellen**. Die Konsole veröffentlicht das Ereignis für den Server.
7. Im Folgenden werden die serverseitigen Aktivitäten beschrieben:
   a. Die Daten werden in den Tabellen LG_MSG_RESTORE und LG_CERT_ARCHIVE wiederhergestellt. Der Server-Thread sucht in der Protokolltabelle für den Export nach den Dateien, die die Daten für die angegebenen Unterdatenträger enthalten, und liest diese Daten während der Wiederherstellungsoperation. Nach Abschluss der Datenwiederherstellung wird die Protokolltabelle aktualisiert und die Markierung auf **Importiert** gesetzt.
   b. Die Dateien werden in den Unterordner 'dataRestore' NONREP des gemeinsamen Dateisystems auf den entsprechenden Unterdatenträgern kopiert. Die Daten werden aus den Sicherungsdateien gelesen, die die Dokumente enthalten, die an den im Datumsbereich angegebenen Tagen verarbeitet wurden und sich in den Sicherungspositionen befinden.
8. Klicken Sie auf **Aktualisieren**, um den Status der Wiederherstellungstask anzuzeigen. Nach Abschluss der Task wird in der Konsole der Status **Erfolgreich** angezeigt. Ist ein Fehler aufgetreten, wird der der Status als **Fehlgeschlagen** angezeigt.

Archivierte Daten von WebSphere Partner Gateway V6.1 und früheren Versionen wiederherstellen

Die Funktion für die konsolbasierte Wiederherstellung (aus einem Archiv) in WebSphere Partner Gateway V6.2 bietet keine Unterstützung für die Sicherungsdatenbankarchive, die unter WebSphere Partner Gateway-Versionen vor Version 6.1 erstellt wurden. Sie unterstützt jedoch die Wiederherstellung von Archiven unbestreitbarer Dateien, die mit Versionen vor WebSphere Partner Gateway Version 6.1 erstellt wurden. Wenn es sich um eine DB2-Datenbank handelt und die Archivsicherung unter WebSphere Partner Gateway V6.1 oder einer späteren Version erstellt wurde, können Sie die Wiederherstellung mithilfe der in WebSphere Partner Gateway V6.2 bereitgestellten Funktion 'restore' ausführen. Bei einer Oracle-Datenbank tritt bei dem Versuch, die Daten wiederherzustellen, der folgende Fehler auf:

```
"Exception while doing the db restore
java.sql.SQLException: ORA-20999: 20002 AR_IMPORT_DATA ORA-29913: error
 in executing ODCIEXTTABLEOPEN callout
ORA-29400: data cartridge error
KUP-11010: unable to open at least one dump file for load
ORA-06512: at "BCGAPPSD.AR_IMPORT_DATA", line 338"
```

Zur Fehlerumgehung können Sie das Format der Oracle-Exportdateien ändern. Hierzu müssen Sie über eine andere Installation von WebSphere Partner Gateway V6.2 verfügen (d. h., eine Installation, die von der Produktionsumgebung abgegrenzt ist). Führen Sie die folgenden Schritte aus, um die unter WebSphere Partner Gateway V6.1 oder einer höheren Version erstellten Datenbankarchive wiederherzustellen:

1. Verwenden sie das Script 'bcgDBNonRepImport', um die Tabellendaten in die Tabelle LG_MSG_ARCHIVE zu importieren.
2. Führen Sie die Archivierungsfunktion über die Konsole aus. Auf diese Weise werden die Exportdateien der Datenbank in dem Format erstellt, das von WebSphere Partner Gateway V6.2 unterstützt wird und über die Konsole wiederhergestellt werden kann. Die Schritte zum Wiederherstellen der archivierten Daten entsprechen den im vorigen Abschnitt beschriebenen Schritten für die DB2-Datenbank. Damit die Sicherung der unbestreitbare Dateien der Version 6.0 über die Konsole von WebSphere Partner Gateway V6.2 ausgeführt werden kann, muss das Datum der letzten Änderung für das Verzeichnis innerhalb des Bereichs zwischen dem in der Anzeige **Archivierungsfunktion - Wiederherstellen** ausgewählten Startdatum und dem Enddatum liegen. Ursache hierfür ist, dass die Verzeichnisstruktur für unbestreitbare Dateien in Version 6.0 nicht im Format JJJJMMTT angegeben ist.

Nach wiederhergestellten Dokumenten suchen

Sie können nach den erforderlichen wiederhergestellten Dokumenten suchen, indem Sie bestimmte Suchkriterien angeben. Führen Sie dazu die folgenden Schritte aus:

1. Melden Sie sich als Administrator an und navigieren Sie zu **Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Wiederherstellen > Wiederhergestellte Dokumente suchen**.
2. Für die Suche nach einem bestimmten Dokument können Sie die folgenden Filterkriterien verwenden:
   - Datumsbereich
   - Quellenpartner
   - Paket
   - Protokoll
   - Dokumenttyp
   - Ergebnisse pro Seite
3. Klicken Sie auf **Suchen**. Die Liste der Tasks der Archivierungsfunktion wird zusammen mit den entsprechenden Details aus der Tabelle LG_MSG_RESTORE abgerufen und in Tabellenformat angezeigt. Die folgenden Informationen werden angezeigt:
   - Unformatierte Nachricht anzeigen - Klicken Sie auf das entsprechende Symbol, um die Details der unformatierten Nachricht zu einem bestimmten Datensatz anzuzeigen.
   - Sendender Partner - Klicken Sie auf den Namen des Partners, um das vollständige Partnerprofil anzuzeigen.
   - Paket
   - Protokoll
   - Dokumenttyp
   - Unterdatenträger

- Zertifikatsname - Klicken Sie auf den Zertifikatsnamen, um die Zertifikatsdetails anzuzeigen.

4. Klicken Sie auf **Zurücksetzen**, um die Werte auf die standardmäßigen, für das System angegebenen Werte zurückzusetzen.

Benutzereingriff bei der Archivierung

In bestimmten Fällen funktioniert der automatische Zeitplan der Archivierungsfunktion aus verschiedenen Gründen nicht mehr. Die erforderlichen Daten können in einem solchen Fall manuell archiviert werden. In den folgenden Abschnitten wird die manuelle Datenarchivierung detailliert beschrieben.

Task der Archivierungsfunktion über die Konsole einleiten

Als WebSphere Partner Gateway-Administrator können Sie die sofortige Ausführung der Task der Archivierungsfunktion über die Konsole einleiten. Diese Initialisierung erfolgt unabhängig von den geplanten Tasks.

Führen Sie die folgenden Schritte aus:

1. Navigieren Sie zu **Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Konfigurieren** und klicken Sie auf **Jetzt ausführen**.

   Anmerkung: Wird die Task bereits ausgeführt, ist der Link **Jetzt ausführen** inaktiviert.
2. Der Server startet die Ausführung der Task. Wurde während der Konfiguration die Option **Kopieren** ausgewählt, werden die Daten in die angegebene Position kopiert.

Aktive Task der Archivierungsfunktion stoppen

Führen Sie die folgenden Schritte aus, um eine aktive Task der Archivierungsfunktion abzubrechen:

1. Navigieren Sie zu **Hubadmin > Hubkonfiguration > Archivierungsfunktion > Archivierungsfunktion - Konfigurieren**. Auf dieser Seite wird die vorhandene Task der Archivierungsfunktion mit dem Status **Wird ausgeführt** angezeigt.
2. Klicken Sie auf **Stoppen**, um die Task abzubrechen.
3. Klicken Sie auf **Ja**, wenn Sie zur Bestätigung der Operation aufgefordert werden. Daraufhin wird der Status **Wird gestoppt** angezeigt.
4. Der Server stoppt die Task vollständig und aktualisiert den Status in den Berichtstabellen in der Datenbank. Darüber hinaus wird das Ereignis zur Terminierung der nächsten Task veröffentlicht.
5. Der Scheduler terminiert die Task der Archivierungsfunktion für die nächste Ausführung und der Status wird auf **Terminiert** gesetzt.

   Anmerkung: Wenn Sie versuchen, die aktive Task zu stoppen, werden die Daten unter Umständen teilweise archiviert und/oder bereinigt. Es besteht keine Möglichkeit, die Operation rückgängig zu machen. Deshalb können die Datenbanktabellen für den Zeitraum vor dem Begrenzungsdatum, das während der Bereinigungsoperation angegeben wurde, inkonsistente Daten enthalten. In der Konsole wird dasselbe dargestellt. Diese Abweichungen werden bei der nächsten erfolgreichen Bereinigungsoperation korrigiert. Dabei muss das Begrenzungsdatum größer-gleich dem Datum sein, das beim Stoppen der Task der Archivierungsfunktion angegeben wurde.

Einschränkungen der Archivierungsfunktion

Aufgrund der nativen Datenbankunterstützung für den serverseitigen Import und Export ist die Archivierungs- und Wiederherstellungsfunktionalität von WebSphere Partner Gateway in den folgenden Versionen eingeschränkt:

- Oracle 9i unterstützt keinen Import oder Export über Datenbankaufrufe. Der Export oder Import von Datenbankdaten muss mit den bereitgestellten Scripts "bcgDBNonRepExport" und "bcgDBNonRepImport" ausgeführt werden.
- DB2 Version 8 unterstützt keinen Import über Datenbankaufrufe. Daher muss der Import von Datenbanktabellen mit dem bereitgestellten Script "bcgDBNonRepImport" ausgeführt werden.

Kapitel 14. Funktionen für Protokollierung und Traceerstellung verwenden

Eine der Aufgaben des WebSphere Partner Gateway-Administrators besteht darin, Probleme zu diagnostizieren, die bei der Verarbeitung von Dokumenten auftreten können. Die bei der Diagnose solcher Probleme verwendeten Tools sind die Protokollierung und die Traceerstellung. Der Administrator muss wissen, wie das System zu konfigurieren ist, sodass es die für die Diagnose von Problemen notwendigen Informationen bereitstellt.

WebSphere Application Server bietet ausgereifte Protokollierungs- und Traceerstellungsfunktionalitäten, die den Anwendungen, deren Host WebSphere Application Server ist, zur Verfügung stehen. WebSphere Partner Gateway-Komponenten sind Anwendungen mit WebSphere Application Server als Host, und sie verwenden die Protokoll- und Tracefunktionalitäten von WebSphere.

Die Dokumentation zu WebSphere Application Server enthält allgemeine Informationen zur Konfiguration von Protokollierung und Traceerstellung, um diese Funktionen jedoch für WebSphere Partner Gateway verwenden zu können, müssen Sie verschiedene Dinge wissen und beachten. Im vorliegenden Kapitel finden Sie eine Zusammenfassung der wichtigsten Punkte, die Sie für die Verwendung der Konsole von WebSphere Application Server wissen müssen, um die Protokollierung und die Traceerstellung steuern zu können. Zusätzlich zu diesen allgemeinen Informationen finden Sie außerdem spezielle Punkte dazu, wie Sie die Protokollierung und die Traceerstellung verwenden können, um WebSphere Partner Gateway-Probleme zu lösen.

Protokoll- und Tracedateien

In diesem Abschnitt werden die für WebSphere Partner Gateway verwendeten Protokoll- und Tracedateien beschrieben.

SystemOut.log und SystemErr.log

Immer wenn eine Anwendung in den Standardausgabestrom oder den Standardfehlerstrom schreibt, wird eine Protokollnachricht geschrieben. Anwendungsentwickler können Nachrichten in diese Ströme schreiben, um allgemeine Informationen über den Status der Programme bereitzustellen. Beispiel: Wenn eine Anwendung initialisiert wird, werden oftmals Protokollnachrichten geschrieben, um zu überprüfen, ob auf die von der Anwendung verwendeten Subsysteme zugegriffen wurde, und ob die Anwendung selbst gestartet wurde. Falls Ausnahmebedingungen auftreten, werden diese in Form einer Protokollnachricht von der Anwendung aufgezeichnet, die die Ausnahmebedingung festgestellt hat. Der Stack-Trace, der den Systemstatus anzeigt, wenn eine Ausnahmebedingung aufgetreten ist, wird gespeichert, indem er in den Standardfehlerstrom geschrieben wird.

Protokollnachrichten werden in die folgenden WebSphere Application Server-Dateien geschrieben:

- `SystemOut.log` für die Aufzeichnung von Nachrichten, die in den Standardausgabestrom geschrieben werden.
- `SystemErr.log` für die Aufzeichnung von Nachrichten, die in den Standardfehlerstrom geschrieben werden.

Es besteht keine Möglichkeit, Protokollnachrichten zu filtern, sodass nur bestimmte geschrieben und andere ausgelassen werden. Da sie in jedem Fall geschrieben werden, sind Protokollnachrichten meistens kurz und allgemein gehalten. Oftmals sind sie insofern nützlich, als dass sie Informationen zum Status des Systems bereitstellen und Hinweise dazu geben können, welche Art der detaillierten Traceerstellung Sie verwenden sollten, wenn ein Problem auftritt.

Tracedatei

Anders als Protokollnachrichten werden Tracenachrichten von Anwendungen nur dann geschrieben, wenn das System dafür konfiguriert wurde. WebSphere Partner Gateway-Anwendungen enthalten zahlreiche Tracenachrichten, die verwendet werden können, um ausführliche Informationen zum Systembetrieb zu erhalten. Tracenachrichten werden allein in eine Tracedatei geschrieben, d. h., ohne etwaige Protokollnachrichten. Die in "SystemOut.log" und "SystemErr.log" protokollierten Nachrichten sind auch in der Tracedatei enthalten. Mit der Konsole von WebSphere Application Server werden Tracenachrichten anhand von zwei Kriterien gefiltert:

- Wertigkeit der Nachricht.
- Ursprung der Nachricht.

Sie können WebSphere Application Server mit Folgendem konfigurieren: Name der Tracedatei, Format der Tracedatei, Art und Weise, wie die Tracedatei verwaltet wird, und die Art der Nachrichten, die in die Tracedatei geschrieben werden. Jede WebSphere Partner Gateway-Anwendung verfügt über Standardeinstellungen im Hinblick auf diese Konfigurationswerte.

Anmerkung: Die von den Benutzern von WebSphere Partner Gateway und WebSphere Business Integration Connect übergebenen Transaktionen werden in unterschiedlichen Zeitzonen aufgezeichnet, da sich die Benutzer in unterschiedlichen Regionen befinden. Um für diese Transaktionen über eine gemeinsame Referenzzeitzone zu verfügen, führen WebSphere Partner Gateway und WebSphere Business Integration Connect interne Zeitkonvertierungen für die bcg*-Protokolle aus und zeichnet sie in GMT auf. Es wird jedoch keine Option bereitgestellt, mit der die Zeitzone in diesen Protokollen geädert werden kann, um Überlappungen und Konflikte zu vermeiden. Für die Protokolldateien "SystemOut", "SystemErr" und "bcg_server" wird die Zeitzone UTC (Universal Time Coordinated - koordinierte Weltzeit) verwendet.

Protokolldateiverwaltung

Die Protokolldateien `SystemOut.log` und `SystemErr.log` befinden sich auf der Workstation, auf der die Anwendung implementiert ist, und zwar im folgenden Pfad: *<WebSphere_Partner_Gateway_installationsverzeichnis>*`/wasND/profiles/`*<profilname>*`/logs/`*<servername>*.

Bei der Verwaltung der Protokolldateien wird die Größe des Plattenspeicherplatzes gesteuert, die diesen Dateien zur Verfügung steht. Eine gewisse Begrenzung der Größe ist notwendig, da die Dateien ansonsten zu groß werden und Ihren Systemstatus beeinträchtigen können. Zur Steuerung der Dateigrößen werden die Dateien als eine Gruppe von Umlaufprotokolldateien gepflegt. Sie können die Anzahl der Dateien in der Gruppe konfigurieren, sowie die Größe, auf die eine Datei anwachsen darf, bevor mit der Protokollierung in der nächsten Datei der Gruppe fortgefahren wird. Dadurch wird der Gesamtplattenspeicherplatz begrenzt, der von den Protokolldateien belegt werden kann.

Vor dem Konfigurieren der Protokolldateien müssen Sie feststellen, ob Ihr WebSphere Partner Gateway-System im einfachen Modus oder im verteilten Modus installiert wurde. Weitere Informationen zum einfachen Modus und zum verteilten Modus finden Sie im Handbuch *WebSphere Partner Gateway Installation*. Es ist wichtig für Sie, den bei der Installation verwendeten Modus zu kennen, da sich die Zugriffsart auf WebSphere Application Server im einfachen und im verteilten Modus voneinander unterscheidet.

Für ein System im einfachen Modus finden Sie die Administrationskonsole von WebSphere Application Server unter `http://<serveradresse>:58090/admin`, wobei "serveradresse" die Adresse der Workstation ist, auf der das System installiert wurde. Port 58090 ist der vom Installationsprogramm verwendete Standardwert, es kann jedoch auch ein anderer Port festgelegt sein, wenn während der Installation nicht der Standardport verwendet wurde.

Wenn Sie ein System im verteilten Modus verwenden, sucht die Administrationskonsole von WebSphere Application Server nach dem Deployment Manager. Sie finden die Adresse des Deployment Managers auch, wenn Sie zu `http://<deployment-mgr-adresse>:55090/admin` navigieren. Port 55090 ist der vom Installationsprogramm verwendete Standardwert, es kann jedoch auch ein anderer Port festgelegt sein, wenn während der Installation nicht der Standardport verwendet wurde.

Für beide Modi sind die Schritte zur Konfiguration der Umlaufprotokolldateien, die vom Server verwendet werden, dieselben.

1. Suchen Sie den Server in der Konsole, indem Sie im linken Teilfenster auf **Server/Anwendungsserver** klicken, wodurch die Servernamen im rechten Teilfenster angezeigt werden.
2. Zeigen Sie die Details des zu konfigurierenden Servers an, indem Sie den Servernamen in der Liste auswählen.
3. Blättern Sie weiter, bis Sie die Überschrift **Fehlerbehebung** unten auf der Seite sehen. Klicken Sie unter **Fehlerbehebung** auf **Protokollierung und Traceerstellung**.
4. Klicken Sie auf **JVM-Protokolle**, um die Details der Protokollierungskonfiguration anzuzeigen.
5. Das angezeigte Fenster enthält die Registerkarte **Konfiguration** und die Registerkarte **Laufzeit**.

   Anmerkung:

   a. Änderungen, die auf der Seite **Konfiguration** durchgeführt werden, werden wirksam, nachdem der Server erneut gestartet wurde. Die Änderungen bleiben auch nach mehreren Serverneustarts bestehen.
   b. Änderungen, die auf der Seite **Laufzeit** durchgeführt werden, werden sofort wirksam, bleiben jedoch bei einem Serverneustart nicht bestehen, es sei denn, die Option **Laufzeitänderungen auch in der Masterkonfiguration speichern** ist ausgewählt.

   Die Hauptmerkmale der Seite **Konfiguration** sind:

   - Sie sehen auf der Seite zwei Sektionen, eine für die Konfiguration der Standardausgabeprotokollierung, die andere für die Konfiguration der Standardfehlerprotokollierung.
   - Sie können den Namen und den Pfad der Dateien ändern, in denen die Protokollnachrichten für den Server gespeichert werden.

- Sie können das für die Protokollnachrichten verwendete Format ändern. Beide Formate stellen die von der Anwendung geschriebene Nachricht bereit. Die Unterschiede zwischen dem Basis- und dem erweiterten Format bestehen darin, wie viele *Metainformationen* mit jeder Nachricht angegeben werden. *Metainformationen* sind Informationen wie z. B. der Zeitpunkt, zu dem das Protokoll geschrieben wurde (Basis und erweitert) sowie der Name des Threads (nur erweitert), der die Informationen geschrieben hat.
- Sie können steuern, wie die umlaufende Protokollierung konfiguriert wird. Es stehen Optionen zur Einstellung der Größe, der Anzahl der Dateien im Umlauf sowie die Auslösemethode für den Überlauf (Dateigröße oder Zeitpunkt) zur Verfügung.

Das Hauptmerkmal auf der Seite **Laufzeit** ist, dass Sie die Protokolldateien anzeigen können, indem Sie für eine bestimmte Datei auf **Anzeigen** klicken. Die angezeigten Zeilennummern können geändert werden, indem der gewünschte Bereich von Zeilennummern eingegeben und die Anzeigeseite aktualisiert wird.

Eine vollständige Beschreibung dieser Merkmale finden Sie in der Dokumentation zu WebSphere Application Server.

Tracedateiverwaltung

Zur Verwaltung von Tracedateien gehört Folgendes:

- Steuerung der Größe des Plattenspeicherplatzes, den Tracedateien beanspruchen können.
- Festlegen der Namen und Pfade für die Tracedateien.
- Festlegen des Formats der Tracedatei.
- Feststellung, welche WebSphere Partner Gateway-Komponenten Traceinformationen in die Dateien schreiben.
- Festlegen der Tracestufe für die ausgewählten Komponenten.

Die Tracekonfiguration wird mit der Administrationskonsole von WebSphere Application Server festgelegt.

Konfiguration der Traceerstellung in einem System mit einfachem Modus

Die Einrichtung der Traceerstellung auf einem System mit einfachem Modus weicht geringfügig von der Einrichtung der Traceerstellung auf einem System mit verteiltem Modus ab. Verwenden Sie die Administrationskonsole von WebSphere Application Server, um die Traceerstellung für ein System mit einfachem Modus zu konfigurieren, und navigieren Sie dazu zu `http://<serveradresse>:58090/admin`.

Der Port 58090 ist der vom Installationsprogramm verwendete Standardwert, es kann jedoch auch ein anderer Port festgelegt sein, wenn während der Installation nicht der Standardport verwendet wurde.

1. Suchen Sie den Server mit einfachem Modus mit dem Namen "Server1" in der Konsole, indem Sie im linken Teilfenster auf **Server/Anwendungsserver** klicken, wodurch die Servernamen im rechten Teilfenster angezeigt werden.
2. Zeigen Sie die Details von "Server1" an, indem Sie in der Liste auf diesen Namen klicken.
3. Blättern Sie weiter, bis Sie die Überschrift **Fehlerbehebung** unten auf der Seite sehen. Klicken Sie auf **Protokollierung und Traceerstellung** unter **Fehlerbehebung**.

4. Klicken Sie auf **Diagnose-Trace**, um die Details der Tracekonfiguration anzuzeigen.

Standardmäßig wird die Tracedatei für WebSphere Partner Gateway-Anwendungen im einfachen Modus wie in Tabelle Tabelle 39 gezeigt konfiguriert. Da alle WebSphere Partner Gateway-Anwendungen auf "Server1" implementiert sind, werden alle Tracenachrichten in dieselbe Tracedatei geschrieben. Die Tracedatei wird in das standardverzeichnis *<WebSphere_Partner_Gateway_installationsverzeichnis>*/wasND/profiles/*<profilname>*/logs/*<servername>* geschrieben. Dies ist dasselbe Standardverzeichnis, in das die Protokolldateien geschrieben werden.

Tabelle 39. Tracekonfiguration für einfachen Modus

Anwendung	Tracedateiname	Format	Anzahl Dateien	Maximale Dateigröße
Alle Anwendungen (Konsole, Empfänger und Document Manager)	trace.log	Basis	1	20 MB

Das Installationsprogramm für den einfachen Modus legt die Protokollierungsstufe standardmäßig nicht fest. Die Protokollierungsstufe steuert die Menge der Traceinformationen, die von den Komponenten bereitgestellt werden. Wenn Sie die Traceerstellung für die WebSphere Partner Gateway-Anwendungen durchführen möchten, müssen Sie die Protokollierungsstufen angeben. Informationen zur Änderung der Protokollierungsstufen finden Sie im Abschnitt „Protokolldetailstufen festlegen” auf Seite 161.

Traceerstellung in einem System mit verteiltem Modus einrichten

Verwenden Sie die Administrationskonsole von WebSphere Application Server für den Deployment Manager, um Tracedateien in einer Installation mit verteiltem Modus zu verwalten. Sie finden sie, wenn Sie zu http://*<serveradresse>*/55090/admin navigieren.

Der Port 55090 ist der vom Installationsverantwortlichen verwendete Standardwert, dieser Port kann jedoch auch ein anderer sein, wenn während der Installation nicht der Standardport verwendet wurde.

1. Suchen Sie den Server, für den Sie ein Trace durchführen möchten, indem Sie auf **Server/Anwendungsserver** im linken Teilfenster klicken, wodurch die Servernamen im rechten Teilfenster angezeigt werden.
2. Zeigen Sie die Details des Servers an, den Sie konfigurieren möchten, indem Sie den Servernamen in der Liste auswählen.
3. Blättern Sie weiter, bis Sie die Überschrift **Fehlerbehebung** unten auf der Seite sehen. Klicken Sie unter **Fehlerbehebung** auf **Protokollierung und Traceerstellung**.
4. Klicken Sie auf **Diagnose-Trace**, um die Details der Tracekonfiguration anzuzeigen.

Standardmäßig werden die Tracedateien für WebSphere Partner Gateway-Anwendungen im verteilten Modus wie in Tabelle 40 auf Seite 160 gezeigt konfiguriert. Die Tracedateien werden in das Verzeichnis *<WebSphere_Partner_Gateway_installationsverzeichnis>*/wasND/profiles/

<*profilname*>/logs/<*servername*> geschrieben. Dies ist dieselbe Speicherposition, unter der auch die Protokolldateien abgelegt werden.

Tabelle 40. Tracekonfiguration für verteilten Modus

Anwendung	Tracedateiname	Format	Anzahl Dateien	Maximale Dateigröße
Empfänger	bcg_receiver.log	Erweitert	10	10 MB
Document Manager	bcg_router.log	Erweitert	10	50 MB
Konsole	bcg_console.log	Erweitert	10	50 MB
Nachrichtenserver	trace.log	Basis	1	20 MB

Das Installationsprogramm legt die Protokollierungsstufe für alle Komponenten von WebSphere Partner Gateway-Anwendungen so fest, dass Tracenachrichten der schwerwiegendenden Stufe protokolliert werden. Die Protokollierungsstufe steuert die Menge der Traceinformationen, die von den Komponenten bereitgestellt werden. Informationen zur Änderung der Protokollierungsstufen finden Sie im Abschnitt „Protokolldetailstufen festlegen" auf Seite 161.

Für beide Systemtypen verwendete Traceerstellungstasks

1. Suchen Sie den Server in der Konsole, indem Sie im linken Teilfenster auf **Server/Anwendungsserver** klicken, wodurch die Servernamen im rechten Teilfenster angezeigt werden.
2. Zeigen Sie die Details des zu konfigurierenden Servers an, indem Sie den Servernamen in der Liste auswählen.
3. Blättern Sie weiter, bis Sie die Überschrift **Fehlerbehebung** unten auf der Seite sehen. Klicken Sie unter **Fehlerbehebung** auf **Protokollierung und Traceerstellung**.
4. Klicken Sie auf **JVM-Protokolle**, um die Details der Protokollierungskonfiguration anzuzeigen. Das Fenster umfasst zwei Seiten: **Konfiguration** und **Laufzeit**.

   Anmerkung:

   a. Änderungen, die auf der Konfigurationsseite durchgeführt werden, werden wirksam, nachdem der Server neu gestartet wurde. Die Änderungen bleiben auch nach mehreren Serverneustarts bestehen.
   b. Änderungen, die auf der Laufzeitseite durchgeführt werden, werden sofort wirksam, bleiben jedoch nicht nach einem Serverneustart bestehen, es sei denn, die Option **Laufzeitänderungen auch in der Konfiguration speichern** ist ausgewählt.
5. Die Seiten **Konfiguration** und **Laufzeit** enthalten auf der rechten Seite beide einen Link mit dem Namen **Detailstufe für Protokoll ändern**. Über diesen Link haben Sie folgende Möglichkeiten:
   - WebSphere Partner Gateway-Komponenten für das Schreiben in die Tracedatei aktivieren.
   - Die Protokollierungsstufe für die einzelnen aktivierten Komponenten auswählen. Die Protokollierungsstufe steuert die Menge der Traceinformationen, die von den Komponenten bereitgestellt werden. Informationen zum Festlegen der Protokollierungsstufen finden Sie im Abschnitt „Protokolldetailstufen festlegen" auf Seite 161.

Hauptmerkmale auf der Seite **Konfiguration**, die Sie auf jeden Fall beachten sollten:

- Die Traceerstellungsdaten werden erst in die genannte Datei geschrieben, wenn Sie **Protokoll aktivieren** auswählen, die Änderungen speichern und den Server erneut starten. Navigieren Sie zu **Protokollierung und Traceerstellung > Diagnose-Trace-Service**, um das Protokoll zu aktivieren.
- Tracenachrichten können in einen Speicherpuffer oder in eine Datei geschrieben werden. Dies legen Sie fest, indem Sie eins der Optionsfelder unter **Traceausgabe** auswählen.
  - Wenn Sie die Option **Speicherpuffer** auswählen, müssen Sie den Speicherinhalt mit einer geeigneten Methode in einer Datei speichern, sodass Sie die Nachrichten anzeigen können.
  - Wenn Sie die Option **Tracedatei** verwenden, konfigurieren Sie ein Umlaufprotokoll. Die Vorgehensweise hat hierbei Ähnlichkeiten mit der Vorgehensweise beim Konfigurieren der Umlaufprotokollierung für das System. Durch Verwendung der Umlaufprotokollierung können Sie das Wachstum der Tracedateien begrenzen, sodass diese nicht zu viele ihrer Dateisystemressourcen beanspruchen. Sie können außerdem den Pfad und den Dateinamen für die Tracedateien konfigurieren.
  - Die Option **Format der Traceausgabe** kann entweder **Basis** oder **Erweitert** lauten. Tracedateien können außerdem in einem Binärformat geschrieben werden, das als Format für den **Log Analyzer** (Protokollanalyseformat) bezeichnet wird. Wenn Sie das Protokollanalyseformat angeben, können Sie eine Traceausgabedatei öffnen, indem Sie das Tool Log Analyzer verwenden. Der Log Analyzer ist eine Anwendung, die in WebSphere Application Server enthalten ist. Weitere Informationen zur Protokollanalyse finden Sie in der Dokumentation zu WebSphere Application Server.

Einer der wichtigsten Vorteile der Seite **Laufzeit** besteht darin, dass Sie die Traceprotokollierung dynamisch ändern können, ohne den Server erneut starten zu müssen. Sie können etwaige Änderungen, die Sie während der Laufzeit ausführen, in der permanenten Konfiguration abbilden, wenn Sie vor dem Speichern die Option **Laufzeitänderungen auch in der Konfiguration speichern** auswählen.

Eine vollständige Beschreibung dieser Eigenschaften finden Sie in der Dokumentation zu WebSphere Application Server.

Protokolldetailstufen festlegen

Wenn Probleme auftreten, benötigen die Mitarbeiter der Service- und Unterstützungsfunktionen möglicherweise die Tracedateien, um den Hintergrund des Problems verstehen zu können. Als Administrator des Systems müssen Sie dieses so konfigurieren, dass eine Traceerstellung erfolgt, die bei der Diagnose von Problemen hilfreich ist. Dies ist Sinn und Zweck der Festlegung von Protokollierungsstufen. Durch Festlegen der Protokollierungsstufe für einen Server bewirken Sie Folgendes:

- Sie bestimmen, welche WebSphere Partner Gateway-Komponenten (Java-Klassen) Tracenachrichten schreiben.
- Sie bestimmen, welche Nachrichtentypen in den Tracedateien enthalten sein sollen und verwenden dabei eine Wertigkeitsskala mit fünf Stufen.

Tracenachrichten werden nach Wertigkeitsstufen klassifiziert, die wiederum aus den Stufen abgeleitet werden, welche von WebSphere Partner Gateway Version 6.0 oder früheren Versionen dieses Produkts verwendet wurden. Diese älteren Wertigkeitsstufen sind den Wertigkeitsstufen von WebSphere Application Server zugeordnet, die in Tabelle Tabelle 41 auf Seite 162 aufgeführt sind. Die Tabelle zeigt, wie die neuen Stufen zu verwenden sind, um dieselbe Tracestufe zu erzielen.

Tabelle 41. Wertigkeitsstufen von WebSphere Application Server

Wertigkeitsstufe in Version 6.1	Wertigkeitsstufe in Version 6.2
SCHWERWIEGEND	SCHWERWIEGEND
FEHLER	ERNST
WARNUNG	WARNUNG
INFORMATION	INFORMATION
DEBUGGING	AM FEINSTEN

Auf die Protokolldetailstufen kann über einen Link zugegriffen werden, der sich auf den Seiten **Konfiguration** und **Laufzeit** der Diagnose-Trace-Funktion für einen Anwendungsserver befindet. Wenn Sie auf diesen Link klicken, wird eine Seite geöffnet, die eine Baumstrukturanzeige der Komponenten präsentiert. Komponenten werden durch Java-Paketnamen für die Klassen dargestellt, die Traceinformationen bereitstellen können, wenn Sie von einem Anwendungsserver ausgegeben werden.

Anmerkung: Die Java-Paketnamen für WebSphere Partner Gateway-Klassen beginnen alle mit dem Präfix `com.ibm.bcg`, sodass Sie die einzelnen Komponenten suchen können, indem Sie nach Paketen mit dem entsprechenden Präfix suchen.

Es gibt drei Möglichkeiten, die Protokolldetailstufen festzulegen:

- Wenn Sie die Protokolldetails auf Komponentenebene über den Komponentenbaum festlegen möchten:
  1. Wählen Sie das Element aus.
  2. Wählen Sie die erforderliche Traceerstellungsstufe aus.
  3. Klicken Sie auf der Seite auf **OK**, damit die Änderung wirksam wird.
- Wenn Sie die Protokolldetails auf Gruppenebene über den Gruppenbaum festlegen möchten:
  1. Wählen Sie den Gruppennamen aus.
  2. Wählen Sie die erforderliche Traceerstellungsstufe aus.
  3. Klicken Sie auf **OK**, damit die Änderung wirksam wird.

  Anmerkung: Bestimmte Gruppen von Komponenten stehen für WebSphere Partner Gateway-Subsysteme, wie z. B. den Empfänger oder die Document Manager-Statusengine. Sie können die Subsysteme anzeigen, indem Sie auf den Link **Gruppen** klicken. Die WebSphere Partner Gateway-Gruppennamen können identifiziert werden, da sie alle mit dem Präfix `BCG` beginnen. Alle Gruppennamen beschreiben den Zweck der Klassen und Pakete, die in der Gruppe vorhanden sind.
- Wenn Sie die Protokolldetails durch direktes Eingeben von Paket- und Klassennamen festlegen möchten: Die Namen in den Baumstrukturanzeigen sind nur ein Bruchteil der Pakete und Klassen, aus denen WebSphere Partner Gateway-Anwendungen bestehen. Möglicherweise werden Sie zur Traceerstellung für Klassen aufgefordert, die nicht in den Listen vorhanden sind.

Wenn Sie Änderungen auf der Konfigurationsseite vornehmen, stellen Sie sicher, dass die Konfiguration gemäß der Nachricht, die oben auf der Seite angezeigt wird, in der Masterkonfiguration gespeichert wird.

WebSphere Partner Gateway-Tracenachrichten identifizieren

Wenn Sie die Traceerstellung mit dem Format "Erweitert" konfiguriert haben, enthalten die Tracenachrichten den Klassennamen, den Methodennamen, den Ersteller, die Thread-ID, den Threadnamen und andere Informationen im Hinblick auf die Nachricht. Das Basisprotokollformat enthält die erforderlichen Informationen, wie beispielsweise die Zeitmarke, die Thread-ID, die Quellenklasse, die Quellenmethode, die Prioritätsstufe und die Protokollnachricht.

Anmerkung: Beim Auftreten eines Fehlers protokolliert WebSphere Partner Gateway keine Ereignisse im Zusammenhang mit der Funktion zur Erfassung von Fehlerdaten beim ersten Auftreten (First Failure Data Capture - FFDC). Verwenden Sie die FFDC-Protokolle nur dann, wenn Sie von der Produktunterstützung dazu aufgefordert werden oder wenn bestimmte Anleitungen zur Fehlerbehebung dies empfehlen.

Traceerstellung für EDI-, XML- und ROD-Unterkomponenten

Zeitweilig kann es sinnvoll sein, die Traceerstellung für einige EDI-, XML- und ROD-Komponenten (Flachdatei) zu aktivieren, die in Zusammenhang mit Validierungszuordnungen und Transformationszuordnungen verwendet werden, welche vom DIS-Client erstellt wurden. Sie werden aktiviert über `WebSphere Partner Gateway-Konsole > Systemverwaltung > Funktionsverwaltung > EDI-Eigenschaften`. Informationen zu den Tracestufeneinstellungen und dem Zweck der jeweiligen Eigenschaft finden Sie in Tabelle 55 auf Seite 264.

Protokoll- und Tracenachrichten von WebSphere Application Server interpretieren

Nachrichten und Fehler, die aus den Konsolenprozessen von WebSphere Application Server stammen, werden in den Protokollen von WebSphere Partner Gateway angezeigt. Einige dieser Nachrichten mögen zunächst wie Fehler erscheinen, sind jedoch Informationsnachrichten und stellen kein Problem für die WebSphere Partner Gateway-Anwendung dar. Der Wert der Stufe wird über die Konfigurationsdaten beim Erstellen des Protokollprozesses festgelegt und kann zur Laufzeit über die Administrationskonsole geändert werden. Mit den folgenden Informationen können Sie die WebSphere Application Server-Nachrichten interpretieren, die Sie möglicherweise in Ihren Systemausgabeprotokollen vorfinden.

WebSphere Application Server-Ereignistypen

Ein Feld mit einem Zeichen, das den Nachrichten- oder Traceereignistyp angibt. Nachrichtentypen werden in Großbuchstaben angezeigt. Zu den gültigen Werten gehören die folgenden:

F Nachricht zu schwerwiegendem Fehler (F = Fatal)

E Fehlernachricht (E = Error)

W Warnung

A Prüfnachricht (A = Audit)

I Informationsnachricht

C Konfigurationsnachricht (C = Configuration)

D Detaillierte Nachricht

O Nachricht, die von der Benutzeranwendung oder internen Komponenten direkt in `SystemOut.log` geschrieben wurden.

R Nachricht, die von der Benutzeranwendung oder internen Komponente direkt in `SystemErr.log` geschrieben wurden.

Z Platzhalter, der angibt, dass der Typ nicht erkannt werden konnte.

Protokollierung für den integrierten FTP-Server

In diesem Abschnitt wird die Integration der Ereignisnachrichten für erfolgreiche und fehlgeschlagene Aktionen des FTP-Servers beschrieben. Wenn WebSphere Partner Gateway Partner ein Dokument an den integrierten FTP-Server von WebSphere Partner Gateway senden will, erstellt der integrierte FTP-Server ein Benachrichtigungsereignis über die Clientverbindung. Nach einer Untersuchung der Antwortcodes des FTP-Servers wird die entsprechende Ereignisnachricht über die Verbindung in der WebSphere Partner Gateway-Datenbank protokolliert.

Ereignisnachrichten für erfolgreiche und fehlgeschlagene Aktionen des FTP-Servers

Die vom FTP-Server für verschiedene Aktionen (beispielsweise das Herstellen einer Verbindung, das Anmelden eines Benutzers, das Hochladen einer Datei oder das Trennen einer Verbindung) generierten Ereignisnachrichten werden als Ereignisse in der WebSphere Partner Gateway-Datenbank protokolliert. Diese Ereignisse können in WebSphere Partner Gateway Console mithilfe der vorhandenen Ereignisanzeige angezeigt werden.

Mögliche Antwortcodes für ein Verbindungsereignis lauten wie folgt:

- 220 Service ready for new user (Service bereit für neuen Benutzer).
- 530 No server access from the IP (Kein Servicezugriff von der IP).
- 530 Maximum number of server connections has been reached (Maximale Anzahl Serververbindungen erreicht).

Nachdem die Verbindung hergestellt wurde, werden die Benutzerdaten authentifiziert. Nach dem Ausführen der Benutzerauthentifizierung erstellt der FTP-Server ein Benachrichtigungsereignis über die Clientanmeldung. Die entsprechende Ereignisnachricht über die Anmeldung wird in der WebSphere Partner Gateway-Datenbank protokolliert. Mögliche Antwortcodes für die Benutzerauthentifizierung lauten wie folgt:

- 501 Syntax errors in parameters or arguments (Syntaxfehler in Parametern oder Argumenten).
- 503 Login with USER first (Zuerst mit dem Benutzernamen anmelden).
- 202 Already logged-in (Bereits angemeldet).
- 21 Maximum number of anonymous login has been reached (Maximale Anzahl anonymer Anmeldungen erreicht).
- 421 Maximum number of login has been reached (Maximale Anzahl Anmeldungen erreicht).
- 230 User logged in, proceed (Benutzer angemeldet; fortfahren).

Nachdem der Benutzer erfolgreich angemeldet wurde, versucht der FTP-Sender des Partners, das Dokument auf den FTP-Server hochzuladen (put). Wenn die Datei hochgeladen ist, generiert der FTP-Server ein Benachrichtigungsereignis über das Ende der Hochladeoperation.

Mögliche Antwortcodes für ein Ereignis für den Hochladebeginn lauten wie folgt:

- 150 File status okay; about to open data connection (Dateistatus ordnungsgemäß; Datenverbindung wird geöffnet).
- 226 Transfer complete (Übertragung abgeschlossen).
- 550 Invalid paths (Ungültige Pfade).
- 550 Permission denied (Berechtigung verweigert).
- 425 Can't open data connection (Datenverbindung kann nicht geöffnet werden).
- 426 Data connection error (Fehler bei der Datenverbindung).
- 551 Error on output file (Fehler in der Ausgabedatei).

Nachdem das Dokument erfolgreich auf die FTP-Position hochgeladen wurde, wird die FTP-Verbindung getrennt. Der FTP-Server generiert ein Benachrichtigungsereignis über das Trennen der Verbindung. Das Ereignis wird in der WebSphere Partner Gateway-Datenbank protokolliert.

Protokoll- und Ausnahmebedingungsinformationen im Zusamenhang mit dem integrierten FTP-Server

Der Code des FTP-Servers generiert intern Protokoll und Ausnahmebedingungsinformationen. Diese Informationen sind in den Protokolldateien verfügbar, die auf dem System generiert werden, auf dem der FTP-Server installiert ist. Diese Protokolldateien werden separat geprüft und analysiert, um Details zu Fehler- und Debuginformationen zu erhalten. Das Format der Protokolldatei ist den Formaten ähnlich, die von anderen Komponenten von WebSphere Partner Gateway verwendet werden.

Protokollierung für den integrierten SFTP-Server

In diesem Abschnitt werden die Ereignisnachrichten für Aktionen des SFTP-Servers beschrieben. Wenn WebSphere Partner Gateway Partner ein Dokument an den integrierten SFTP-Server von WebSphere Partner Gateway senden will, erstellt der integrierte SFTP-Server ein Benachrichtigungsereignis über die Clientverbindung. Nach einer Untersuchung der Antwortcodes des SFTP-Servers wird die entsprechende Ereignisnachricht über die Verbindung in der WebSphere Partner Gateway-Datenbank protokolliert. Auf der Seite mit den Ereigniscodes in der Konsole werden die SFTP-Ereignisse im Bereich von BCG620001 bis BCG620008 aufgelistet.

Kapitel 15. Konfigurationsverwaltung für den FTP- und SFTP-Server

Die Konfigurationseigenschaften des FTP-Servers werden in der WebSphere Partner Gateway-Datenbank gespeichert. Navigieren Sie in der Konsole zur Option **Systemverwaltung** > **FTP-Verwaltung**.

Sie können den FTP- und SFTP-Server über die Seite **Server starten/stoppen** der Konsole starten bzw. stoppen.

Die Konfiguration des FTP-Servers ist in die folgenden sechs Registerkarten gegliedert:

- **Ereigniseigenschaften**

  Auf der Seite **Ereigniseigenschaften** werden die editierbaren Konfigurationseigenschaften für die Protokollierung der Ereignisnachrichten des FTP-Servers angezeigt.
- **Listenereigenschaften**

  Auf der Seite **Listenereigenschaften** werden alle editierbaren Eigenschaften angezeigt.
- **Verbindungseigenschaften**

  Auf der Seite **Verbindungseigenschaften** werden alle editierbaren Eigenschaften angezeigt.
- **Eigenschaften von IP Restrictor**

  Mithilfe von IP Restrictor könne Sie den Zugriff auf den FTP-Server auf der Basis von IP-Adressen einschränken. Klicken Sie auf **Hinzufügen**, um eine neue IP-Adresse hinzuzufügen. IP-Adressen können mit den Platzhalterzeichen *, ? und - angegeben werden. Die Reihenfolge der Regeln ist wichtig. Wenn ein Client den Kontakt zum Server herstellt, werden die Regeln von oben nach unten ausgewertet. Klicken Sie auf **Speichern**, um die Änderungen zu speichern. Der FTP-Server wird neu gestartet, damit die Änderungen wirksam werden. Sind alle passiven Ports von Clientverbindungen belegt, muss der nächste Client warten, bis ein Port verfügbar wird. Der zulässige Bereich liegt zwischen 0 und 65535. Mithilfe der Eigenschaft **config.data-connection.passive.ports** können passive Ports als einzelner Port, mehrere Ports oder als Portbereich angegeben werden.
- **Datenbankeigenschaften**

  Auf der Seite **Datenbankeigenschaften** können Sie Eigenschaften, wie beispielsweise **Hostname**, **Benutzername**, **Kennwort** oder **Port**, eingeben. Diese Werte werden automatisch im FTP-Server gespeichert.
- **Andere Eigenschaften**

  Auf der Seite **Andere Eigenschaften** werden alle editierbaren Eigenschaften angezeigt.

Die Seite **SFTP-Eigenschaften** enthält die Werte für den Port, die maximale Anzahl der Authentifizierungsanforderungen und das Authentifizierungszeitlimit für den SFTP-Server.

FTP- und SFTP-Benutzerverwaltung

Verwenden Sie die Seite **FTP-Benutzerverwaltung**, um die FTP- und SFTP-Benutzer zu verwalten. Navigieren Sie in der Konsole zur Option **Kontenadmin** > **FTP-Benutzerverwaltung**. Auf der Seite **FTP-Benutzerverwaltung** können Sie die folgenden Tasks ausführen:

- Suchen Sie auf der Basis der gewünschten Suchkriterien nach FTP- und SFTP-Benutzern auf verschiedenen Partnern.
- Bearbeiten Sie Informationen zu FTP- und SFTP-Benutzern.
- Erstellen Sie FTP- und SFTP-Benutzer.
- Zeigen Sie Informationen zur FTP- und SFTP-Konfiguration an und bearbeiten Sie sie.

Kapitel 16. Verlagerung und erneute Implementierung von WebSphere Partner Gateway

Wenn die IP-Adresse oder der Hostname der WebSphere Partner Gateway-Umgebung geändert wird, müssen in der Regel die Systemkonfigurationsdateien auf allen Maschinen, auf denen WebSphere Partner Gateway-Komponenten installiert sind, aktualisiert werden.

WebSphere Partner Gateway 6.2.1 stellt eine Option zur automatischen Aktualisierung der Konfigurationsdateien bereit, wenn die IP-Adresse, der Hostname, die Datenquellendetails oder die Portnummer einer Serverkomponente oder von Deployment Manager geändert wird. Die folgenden Änderungen werden nach der Implementierung von WebSphere Partner Gateway unterstützt:

- „Hostnamen und IP-Adresse von WebSphere Partner Gateway ändern" auf Seite 170
- „Hostnamen und Portnummer der Datenbank ändern" auf Seite 171. Wenn Sie den Hostnamen oder die Portnummer der Datenbank ändern, müssen Sie diese Angaben auch für die in WebSphere Application Server definierte Datenquelle aktualisieren, mit deren Hilfe WebSphere Partner Gateway eine Verbindung zur Datenbank herstellt.
- „Portnummern ändern" auf Seite 172

In diesem Kapitel werden auch Beispielszenarios für unterschiedliche Installations- und Implementierungstopologien beschrieben.

Anmerkung: Bei den in diesem Kapitel genannten Befehlen muss die Groß-/Kleinschreibung nicht beachtet werden.

Einschränkungen

Bei der automatischen Aktualisierung von Hostnamen oder IP-Adressen muss Folgendes beachtet werden:

- Stellen Sie sicher, dass Sie vor Änderung der Parameter eine Sicherung vornehmen. Wenn Sie die vorhandene Konfiguration mithilfe von *backupconfig.bat* sichern, kann die Konfiguration bei Bedarf wiederhergestellt werden. Detaillierte Informationen hierzu finden Sie im Abschnitt „Voraussetzungen".
- Bestimmte Eigenschaften wie FTP-Host oder Benutzername und Kennwort für die Datenbankquelle müssen manuell geändert werden.

Voraussetzungen

Einfacher Modus

Bevor Sie mit der Verlagerung und erneuten Implementierung beginnen, müssen Sie die vorhandene Konfiguration sichern. Gehen Sie dazu wie folgt vor:

1. Stoppen Sie den Anwendungsserver.
2. Führen Sie den folgenden Befehl aus:
   `<installationspfad_der_WPG_komponenten>/WASND/Profiles/<ProfileName>/bin/backupConfig.bat`.

Verteilter Modus

1. Stoppen Sie alle Anwendungsserver, Knoten und Deployment Manager.
2. Führen Sie die folgenden Befehle aus, um die Konfigurationsdateien von Deployment Manager und der in Deployment Manager installierten Komponenten zu sichern:
   - `<installationspfad_für_Deployment_Manager>/WASND/Profiles/<ProfileName>/bin/backupConfig.bat`
   - `<installationspfad_der_WPG_komponenten>/WASND/Profiles/<ProfileName>/bin/backupConfig.bat`. Führen Sie diesen Befehl auf allen Maschinen aus, auf denen WebSphere Partner Gateway-Komponenten installiert sind.

Konfigurationsdetails wiederherstellen

Die Konfigurationsdetails können nur dann wiederhergestellt werden, wenn Sie die Konfiguration gemäß den im obigen Abschnitt beschriebenen Schritten gesichert haben. Führen Sie die folgenden Befehle aus, um die Konfiguration zu sichern:

- `<installationspfad_für_Deployment_Manager>/WASND/Profiles/<ProfileName>/bin/restoreConfig.bat`
- `<installationspfad_der_WPG_komponenten>/WASND/Profiles/<ProfileName>/bin/restoreConfig.bat`

Hostnamen und IP-Adresse von WebSphere Partner Gateway ändern

In den folgenden Abschnitten werden detaillierte Schritte zum Ändern der Hostnamen und IP-Adressen von WebSphere Partner Gateway-Komponenten beschrieben. Weitere Informationen finden Sie im Abschnitt zum Installationsmodus von WebSphere Partner Gateway.

Anmerkung: Stoppen Sie den Server, bevor Sie die Schritte zum Ändern des Hostnamens und der IP-Adresse ausführen.

Einfacher Modus

Führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Konfigurationsdateien gesichert wurden, bevor Sie bedeutende Änderungen vornehmen. Detaillierte Informationen hierzu finden Sie im Abschnitt „Voraussetzungen” auf Seite 169.
2. Ändern Sie die Datenquelle. Führen Sie dazu bcgChangeDataSource.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und der Portnummer als Eingabeparameter aus: `bcgChangeDataSource.bat/sh <neue_IP-adresse/neuer_hostname> <PORTNUMMER>`. Diese ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_einfachen_modus>/bin`.
3. Ändern Sie den Hostnamen. Führen Sie dazu bcgChangeNodeHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse als Eingabeparameter aus: `bcgChangeNodeHostname.bat/sh <neue_IP-adresse/neuer_hostname>`. Diese ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_einfachen_modus>/bin`.

Anmerkung: Nach der erfolgreichen Änderung des Hostnamens bzw. der IP-Adresse werden die Anwendungsserver automatisch gestartet.

Verteilter Modus

Führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die Konfigurationsdateien gesichert wurden, bevor Sie bedeutende Änderungen vornehmen. Detaillierte Informationen hierzu finden Sie im Abschnitt „Voraussetzungen" auf Seite 169.

   Anmerkung: Stoppen Sie den Knotenagenten von Deployment Manager, bevor Sie die Schritte zum Ändern des Hostnamens und der Portnummer ausführen.
2. Ändern Sie das DMGR-Profil. Führen Sie dazu bcgChangeDmgrHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse als Eingabeparameter aus: `bcgChangeDmgrHostname.bat/sh <neue_IP-adresse/neuer_hostname>`. Diese ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_Deployment Manager>/bin`. Durch diesen Befehl wird der Hostname bzw. die IP-Adresse des DMGR-Profils geändert und Deployment Manager gestartet.
3. Ändern Sie die Knotenzuordnungen unter Verwendung des neuen DMGR-Hostnamens. Führen Sie dazu bcgChangeDmgrHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und dem SOAP-Port als Eingabeparameter aus: `bcgChangeDmgrHostname.bat/sh <neue_IP-adresse/neuer_hostname> <SOAP-PORTNUMMER>`. Diese ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_hub>/bin`.
4. Ändern Sie den Hostnamen der WebSphere Partner Gateway-Komponenten. Gehen Sie dazu wie folgt vor:
   a. Führen Sie bcgChangeNodeHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und dem aktuellen Knotennamen als Eingabeparameter aus: `bcgChangeNodeHostname <neue_IP-adresse/neuer_hostname> <knotenname_der_maschine>`. Die ausführbare Datei befindet sich im Ordner `<BCG_DMGR_HOME>/bin`.
   b. Führen Sie auf der Maschine mit den WebSphere Partner Gateway-Komponenten bcgChangeNodeHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse, dem DMGR-Hostnamen und dem DMGR-SOAP-Port als Eingabeparameter aus. Der Befehl lautet wie folgt: `bcgChangeNodeHostname <neue_IP-adresse/neuer_hostname> <Dmgr_IP-adresse/Hostname> <DMGR-SOAP-port>`. Diese ausführbare Datei befindet sich im Ordner `<BCG_Hub_HOME>/bin`.

Anmerkung: Nach der erfolgreichen Änderung des Hostnamens bzw. der IP-Adresse wird Deployment Manager automatisch gestartet. Der Knoten und die Anwendungsserver müssen jedoch manuell gestartet werden.

Hostnamen und Portnummer der Datenbank ändern

Eine detaillierte Beschreibung der Schritte zur Änderung des Hostnamens und der Portnummer der Datenbank finden Sie im entsprechenden Abschnitt. Stellen Sie sicher, dass vor der Durchführung bedeutender Änderungen die Konfigurationsdateien gesichert werden. Detaillierte Informationen hierzu finden Sie im Abschnitt „Voraussetzungen" auf Seite 169.

Einfacher Modus

Führen Sie den Befehl `bcgChangeDataSource.bat/sh <neue_IP-adresse/neuer_hostname> <PORTNUMMER>` aus. Diese ausführbare Datei befindet sich im Ordner `<BCG_SIMPLE_HOME/bin>`.

Verteilter Modus

Gehen Sie wie folgt vor, um den Hostnamen und die Portnummer für die folgenden Datenbanken zu ändern:

- MAS-Datenbank: Führen Sie den Befehl `bcgChangeMASDataSource.bat/sh <neue_IP-adresse/neuer_hostname> <PORTNUMMER>` aus. Diese ausführbare Datei befindet sich im Ordner `<BCG_HUB_DMGR/bin>`.
- WebSphere Partner Gateway-Anwendungsdatenbank: Führen Sie den Befehl `bcgChangeDataSource.bat/sh <neue_IP-adresse/neuer_hostname> <PORTNUMMER>` aus. Diese ausführbare Datei befindet sich im Ordner `<BCG_HUB_DMGR/bin>`.

Anmerkung: Wenn Sie nur einen einzelnen Parameter ändern wollen, können Sie für den Parameter, der nicht geändert werden soll, die Angabe <None> machen. Führen Sie beispielsweise den folgenden Befehl aus, wenn nur die IP-Adresse geändert werden soll: `bcgChangeDataSource 9.182.10.12 NONE`.

Portnummern ändern

Stellen Sie sicher, dass die Konfigurationsdateien gesichert wurden, bevor Sie Änderungen vornehmen. Detaillierte Informationen hierzu finden Sie im Abschnitt „Voraussetzungen" auf Seite 169.

Führen Sie zum Ändern der Portnummer den folgenden Befehl aus: `bcgChangePorts.bat <Porttyp> <Portnummer> <Servertyp> <Hostname>`. Für den Porttyp muss einer der folgenden Werte verwendet werden:

- BOOTSTRAP_ADDRESS
- SIB_ENDPOINT_ADDRESS
- WC_defaulthost

Die Portnummer muss ein beliebiger Wert zwischen 0 und 65535 sein.

Für den Servertyp muss einer der folgenden Werte verwendet werden:

- simple
- console
- router
- receiver
- simpledistributed

Verlagerung und erneute Implementierung - Beispiele

Je nach WebSphere Partner Gateway-Installation und -Implementierungstopologie müssen die Scripts für Verlagerung und erneute Implementierung auf einer oder mehreren Maschinen ausgeführt werden. In den folgenden Abschnitten werden verschiedene Szenarien beschrieben, in denen die Änderungen aktualisiert werden müssen. Ferner werden die hierzu erforderlichen Schritte erläutert.

Beispiel 1: Einfache verteilte Installation

In diesem Szenario wurde WebSphere Partner Gateway in einem einfachen verteilten Modus installiert. Es gelten die folgenden Voraussetzungen:

- Maschine A - Die Datenbank wurde installiert.
- Maschine B - Deployment Manager und WebSphere Partner Gateway-Komponenten wurden installiert. Der Hostname dieser Maschine wird aktualisiert.

Führen Sie die folgenden Schritte aus, um den Hostnamen oder die IP-Adresse zu ändern:

1. Stellen Sie sicher, dass die Konfigurationsdateien gesichert wurden, bevor Sie bedeutende Änderungen vornehmen. Detaillierte Informationen hierzu finden Sie im Abschnitt „Voraussetzungen" auf Seite 169.
2. Ändern Sie den Hostnamen oder die IP-Adresse des DMGR-Profils wie folgt:
   a. Führen Sie auf **Maschine B**, auf der Deployment Manager installiert ist, den Befehl bcgChangeDmgrHostname.bat/sh mit einem neuen Hostnamen/ einer neuen IP-Adresse als Eingabeparameter aus. Beispiel: `bcgChangeDmgrHostname.bat 9.1.1.1`. Die ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_Deployment Manager>/bin`. Durch diesen Befehl wird der Hostname bzw. die IP-Adresse des DMGR-Profils geändert und Deployment Manager gestartet.
   b. Greifen Sie in **Maschine B** auf den Knoten zu, auf dem die WebSphere Partner Gateway-Komponenten installiert sind. Führen Sie den Befehl bcgChangeDmgrHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und dem SOAP-Port als Eingabeparameter aus. Beispiel: `bcgChangeDmgrHostname.bat 9.1.1.1 55880`. Die ausführbare Datei befindet sich im Ordner `<<installationsverzeichnis_für_hub>/bin>`.

   Der Hostname bzw. die IP-Adresse von Deployment Manager für den Knoten in Maschine B wird nun geändert. Alle Änderungen von Deployment Manager werden für diesen Knoten synchronisiert.

   Anmerkung: Wenn mehrere Knoten vorhanden sind, führen Sie die Scripts für die einzelnen Knoten aus.
3. Ändern Sie den Hostnamen oder die IP-Adresse des Knotens, auf dem die WebSphere Partner Gateway-Komponenten installiert sind. Führen Sie die folgenden Schritte aus:
   a. Führen Sie auf **Maschine B**, auf der Deployment Manager installiert ist, den Befehl bcgChangeNodeHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und dem Aktuellen Knotennamen als Eingabeparameter aus. Beispiel: `bcgChangeNodeHostname.bat 9.1.1.2 bcgnode_B`. Die ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_Deployment Manager>/bin`.
   b. Greifen Sie auf **Maschine B** auf die Knoten zu, auf denen die WebSphere Partner Gateway-Komponenten installiert sind. Führen Sie den Befehl bcgChangeNodeHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse, dem DMGR-Hostnamen und dem DMGR-SOAP-Port als Eingabeparameter aus. Beispiel: `bcgChangeNodeHostname.bat 9.1.1.2 9.1.1.1 55880`. Die ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_hub>/bin`.

Anmerkung: Die Knoten und der Anwendungsserver müssen manuell gestartet werden. DMGR wird automatisch gestartet.

Beispiel 2: Vollständig verteilte Installation

Die Voraussetzungen für dieses Szenario lauten wie folgt:

- Maschine A - Die Datenbank ist installiert. Die Portnummer dieser Maschine wird aktualisiert.
- Maschine B - Deployment Manager ist installiert. Die IP-Adresse dieser Maschine wird aktualisiert.

- Maschine C - Die Komponenten sind installiert. Die IP-Adresse dieser Maschine wird aktualisiert.

Führen Sie die folgenden Schritte aus, um den Hostnamen oder die IP-Adresse von Deployment Manager und den WebSphere Partner Gateway-Komponenten zu ändern:

1. Stellen Sie sicher, dass die Konfigurationsdateien gesichert wurden, bevor Sie bedeutende Änderungen vornehmen. Detaillierte Informationen hierzu finden Sie im Abschnitt „Voraussetzungen" auf Seite 169.
2. Ändern Sie den Hostnamen oder die IP-Adresse des DMGR-Profils wie folgt:
   a. Führen Sie auf **Maschine B**, auf der Deployment Manager installiert ist, den Befehl bcgChangeDmgrHostname.bat/sh mit einem neuen Hostnamen/ einer neuen IP-Adresse als Eingabeparameter aus. Beispiel: `bcgChangeDmgrHostname.bat 9.1.1.1`. Die ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_Deployment Manager>/bin`. Durch diesen Befehl wird der Hostname bzw. die IP-Adresse des DMGR-Profils geändert und Deployment Manager gestartet.
   b. Greifen Sie auf **Maschine C** auf den Knoten zu, auf dem die WebSphere Partner Gateway-Komponenten installiert sind. Führen Sie den Befehl bcgChangeDmgrHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und dem SOAP-Port als Eingabeparameter aus. Beispiel: `bcgChangeDmgrHostname.bat 9.1.1.1 55880`. Die ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_hub>/bin`.

   Der Hostname bzw. die IP-Adresse von Deployment Manager für den Knoten in Maschine C wird nun geändert. Alle Änderungen von Deployment Manager werden für diesen Knoten synchronisiert.

   Anmerkung: Wenn mehrere Knoten vorhanden sind, führen Sie die Scripts für die einzelnen Knoten aus.
3. Ändern Sie den Hostnamen oder die IP-Adresse des Knotens, auf dem die WebSphere Partner Gateway-Komponenten installiert sind. Führen Sie die folgenden Schritte aus:
   a. Führen Sie auf **Maschine B**, auf der Deployment Manager installiert ist, den Befehl bcgChangeNodeHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und dem Aktuellen Knotennamen als Eingabeparameter aus. Beispiel: `bcgChangeNodeHostname.bat 9.1.1.2 bcgnode_C`. Die ausführbare Datei befindet sich im Ordner `<installationsverzeichnis_für_Deployment Manager>/bin`.
   b. Greifen Sie auf **Maschine C** auf die Knoten zu, auf denen alle WebSphere Partner Gateway-Komponenten installiert sind. Führen Sie den Befehl bcgChangeNodeHostname.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse, dem DMGR-Hostnamen und dem DMGR-SOAP-Port als Eingabeparameter aus. Beispiel: `bcgChangeNodeHostname.bat 9.1.1.2 9.1.1.1 55880`.
4. Ändern Sie den Hostnamen und den Port der Datenbank. Stellen Sie sicher, dass DMGR (Document Manager) betriebsbereit ist, bevor Sie die folgenden Schritte ausführen:
   a. Führen Sie auf **Maschine C**, auf der die WebSphere Partner Gateway-Komponenten installiert sind, den Befehl bcgChangeDataSource.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und einem neuen Port als Eingabeparameter aus. Beispiel: `bcgChangeDataSource.bat 9.1.1.2 55880`.

Stellen Sie sicher, dass Sie den neuen Hostnamen bzw. die neue IP-Adresse und die neue Portnummer der auf **Maschine A** installierten Anwendungsdatenbank angeben.

b. Führen Sie auf **Maschine C**, auf der die WebSphere Partner Gateway-Komponenten installiert sind, den Befehl bcgChangeMASDataSource.bat/sh mit einem neuen Hostnamen/einer neuen IP-Adresse und einem neuen Port als Eingabeparameter aus. Beispiel: `bcgChangeMASDataSource.bat 9.1.1.2 55880`. Stellen Sie sicher, dass Sie den neuen Hostnamen bzw. die neue IP-Adresse und die neue Portnummer der auf **Maschine A** installierten MAS-Datenbank angeben.

Anmerkung: Starten Sie alle Server manuell erneut.

Kapitel 17. Fehlerbehebung

Dieses Kapitel enthält Informationen zur Fehlerbehebung, mit denen Sie Probleme erkennen und lösen können. „Anahng B - Fehlgeschlagene Ereignisse” auf Seite 213 enthält eine Auflistung der Fehlerereignisse und ihrer zugehörigen Beschreibungen.

In diesem Kapitel werden die folgenden Themen behandelt:

• „AS-Signaturfehler für den Inhaltstyp "interop"" auf Seite 208

Lange Verarbeitungszeit für große, verschlüsselte AS-Dokumente vermeiden

Die Verarbeitung großer, verschlüsselter AS-Dokumente kann auf einigen weniger leistungsfähigen Hardwarekonfigurationen einige Zeit in Anspruch nehmen. Gehen Sie wie folgt vor, um Verzögerungen zu vermeiden:

1. Setzen Sie das Attribut **AS komprimiert** auf **Ja**, um die Größe des gesendeten Dokuments zu verringern.
2. Führen Sie die Schritte im Abschnitt „Fehler "Zu wenig Speicher" vermeiden" aus, um die Speicherkapazität zu erhöhen und die Verarbeitung verschlüsselter Dokumente zu beschleunigen.

Lange Verarbeitungszeit für große, verschlüsselte Dokumente vermeiden

Große Dateien können vor dem Senden komprimiert werden. Die Unterstützung für große Dateien, deren Größe im Bereich von Gigabyte liegt, wurde für AS2 und AS3 erweitert. In Version 6.2 ist die maximale Größe von Dateien, die unter Verwendung von Bytefeldgruppen verarbeitet werden, konfigurierbar. Ist die Menge des zugeordneten Speichers größer als die Größe des verfügbaren Heapspeichers, tritt ein Fehler des Typs "OutOfMemoryError" auf. Ist der Umfang der Daten kleiner als der verfügbare Speicher kann dennoch ein Fehler des Typs "OutOfMemoryError" auftreten, wenn die Menge an zugeordnetem Speicher den verfügbaren Speicher übersteigt. Die maximale Dateigröße, die mithilfe von Bytefeldgruppen verwendet werden kann, wird über die Eigenschaft **bcg.maximumFileSizeForByteArrays** angegeben. Melden Sie sich als Hubbetreiber an und navigieren Sie zur Registerkarte **Systemverwaltung** > **Gemeinsame Attribute**. Überschreiben Sie den Standardwert der Eigenschaft **bcg.maximumFileSizeForByteArrays**, und geben Sie die maximale Größe von Dateien an, die mit Bytefeldgruppen verwendet werden sollen. Durch das Erhöhen des Werts für diese Eigenschaft wird die Leistung verbessert. Um Fehler aufgrund von fehlendem Speicher zu vermeiden, muss der Wert der Eigenschaft **bcg.maximumFileSizeForByteArrays** so festgelegt werden, dass sehr große Dateien unter Verwendung von Datenströmen (Streams) und nicht als Bytefeldgruppen verarbeitet werden. Ist die Größe des Hauptspeichers (RAM) beispielsweise 512 MB, kann der Wert der Eigenschaft **bcg.maximumFileSizeForByteArrays** auf 20 MB festgelegt werden. Alle Dokumente, die größer als 20 MB sind, werden mit Datenströmen und nicht mit Bytefeldgruppen verarbeitet. Dokumente, die kleiner als 20 MB sind, werden im Speicher verarbeitet.

Fehler "Zu wenig Speicher" vermeiden

Die folgenden Bereiche können dazu beitragen, dass zu wenig Speicher vorhanden ist:

- Document Manager-Hauptspeicherkonfiguration

  Diese Konfiguration legt die Speicherkapazität fest, die der zu Grunde liegenden Java-Anwendung zugeordnet wird.

- Document Manager-Auslastung.

  Sie können konfigurieren, wie viele Threads von den Unterkomponenten verwendet werden dürfen. Wenn die konfigurierte Anzahl an Threads und gleichzeitig die Auslastung sehr hoch ist, ist mehr Speicherkapazität erforderlich, um alle Dokumente handhaben zu können.

- Dokumentstruktur der Dokumente, die verarbeitet werden.

  Je nach Struktur der Dokumente kann mehr Speicher erforderlich sein, um ein Dokument zu verarbeiten, insbesondere bei großen Dokumenten. Die betroffenen Bereiche sind die Sicherheit (Verschlüsselung, Entschlüsselung, Signaturverifizierung) sowie die Schritte zur XML-Konvertierung und Validierungsverarbeitung (insbesondere bei Dokumenten mit großen Textwerten).

Weitere Informationen zu Fehlern des Typs "OutOfMemoryError" aufgrund großer Dateien finden Sie im Abschnitt „Lange Verarbeitungszeit für große, verschlüsselte Dokumente vermeiden” auf Seite 179.

Document Manager-Hauptspeicherkonfiguration

Zur Verbesserung der Leistung und um den Fehler "Zu wenig Speicher" zu vermeiden können Sie die anfängliche und die maximale Größe des Heapspeichers für die WebSphere Partner Gateway-Komponenten festlegen. Wechseln Sie dazu in die Administrationskonsole von WebSphere Application Server und gehen Sie wie folgt vor:

1. Navigieren Sie zu **Anwendungsserver**.
2. Wählen Sie die betreffende WebSphere Partner Gateway-Komponente aus.
3. Wählen Sie **Java- und Prozessverwaltung** > **Prozessdefinition** > **Java Virtual Machine** aus.
4. Aktualisieren Sie die Werte für **Anfangsgröße des Heapspeichers** und **Maximale Größe des Heapspeichers**.
5. Starten Sie WebSphere Partner Gateway erneut.

Document Manager-Auslastung.

Die Anzahl der Verarbeitungsthreads kann für mehrere Unterkomponenten konfiguriert werden, indem die Systemeigenschaften festgelegt werden. Die Standardwerte dieser Eigenschaften sind niedrig angesetzt, aber möglicherweise sind sie vom Administrator geändert worden. In den Konfigurationstabellen in „Anhang C - Komponentenspezifische Systemattribute” auf Seite 253 finden Sie die Eigenschaften im Zusammenhang mit der Threadkonfiguration.

Dokumentstruktur

Große Dokumente stammen entweder vom externen Partner oder vom internen Partner (Back-End-Anwendung). Stellen Sie fest, ob es Möglichkeiten gibt, die Dokumentgröße zu verkleinern, z. B. durch geringere Batchgrößen oder durch die Verwendung kleinerer Dokumente.

Größe des Heapspeichers erhöhen

Immer wenn eine große Anzahl an Dokumenten (ungefähr 40) gesendet wird, die 50 MB groß sind und deren Verschlüsselung, Signatur und Komprimierung über AS3 liegt, muss die Größe des Heapspeichers erhöht werden. Wird die Größe des Heapspeichers nicht erhöht, schlagen Dokumente möglicherweise mit dem Fehler "OutOfMemory" (zu wenig Speicher) fehl.

Der Fehler "OutOfMemory" wird dadurch verursacht, dass der Arbeitsspeicher nicht ausreicht, damit WebSphere Partner Gateway die Dokumente im Ganzen weiterleiten kann. Deshalb wird empfohlen, dass Sie die Größe des Heapspeichers erhöhen. Führen Sie die folgenden Schritte aus, um die Größenparameter des Heapspeichers für den Document Manager-Server zu erhöhen:

1. Melden Sie sich an der Admininistrationskonsole von WebSphere Application Server an.
2. Wählen Sie in der WebSphere Application Server-Admininistrationskonsole für den Server bcgDocMgr die Optionen **Java- und Prozessverwaltung** > **Prozessdefinition** > **Java Virtual Machine** aus.
3. Setzen Sie den Parameter **Anfangsgröße des Heapspeichers** auf 1024.
4. Setzen Sie den Parameter **Maximale Größe des Heapspeichers** auf 1536. Falls das System über mehr als 2 GB verfügt, kann die maximale Größe des Heapspeichers auf einen Wert über 1536 gesetzt werden.

Daten für mehrere Sprachen sortieren

WebSphere Partner Gateway hängt für das Sortieren von Daten von den zu Grunde liegenden Datenbanken ab. Wenn Ihre Installation mehrere Sprachen unterstützt und Ihre Unicode-Daten nicht richtig sortiert werden, lesen Sie die Informationen in diesem Abschnitt.

DB2

Seit Version 6.0 konfiguriert WebSphere Partner Gateway DB2 so, dass die Sortiereinstellung UCA400_NO verwendet wird. DB2 Version 8.2 unterstützt nicht alle Sonderzeichen für alle Sprachen (wie in der Unicode-Standardversion 4.0, Technical Standard Nr. 10 beschrieben). Wenden Sie sich in diesen Fällen direkt an die zuständige DB2-Unterstützungsfunktion.

Oracle

Oracle-Datenbanken verwenden dynamische Änderungen von Sortierfolgen. Damit diese Funktionalität verwendet werden kann, ändert WebSphere Partner Gateway abhängig von der Locale des aktuellen Benutzers den Wert der Sitzungsvariablen NLS_SORT. Tabelle 42 enthält mögliche Benutzer-Locales, die unterstützten WebSphere Partner Gateway-Sprachen und ihre zugehörigen NLS_SORT-Werte. Diese Informationen sind in der Datenbanktabelle PR_LOCALE gespeichert.

Tabelle 42. Locale-Informationen

Browser-Locale	Sprache	NLS_SORT-Wert
pt_BR	Brasilianisches Portugiesisch	BINARY
zh	Chinesisch	SCHINESE_RADICAL_M
de	Deutsch	XGERMAN
en_US	Englisch	BINARY
fr	Französisch	FRENCH_M
it	Italienisch	BINARY
ja	Japanisch	JAPANESE_M
ko	Koreanisch	KOREAN_M
es	Spanisch	SPANISH_M
zh_TW	Traditionelles Chinesisch	TCHINESE_RADICAL_M
Other	Andere	BINARY

Ausreichenden virtuellen Speicher für DB2-Agenten bereitstellen

Der folgende Fehler, der in den WebSphere Partner Gateway-Protokollen auftritt, gibt an, dass der verfügbare virtuelle Speicher für den Datenbankagenten zur Sortierverarbeitung nicht ausreicht. Verringern Sie zur Korrektur dieser Situation den Parameterwert SORTHEAP für die Datenbank, die Sie für WebSphere Partner Gateway erstellt haben. Wenden Sie sich an Ihren Datenbankadministrator, um zu erfahren, wie dieser Parameter in Ihrer Umgebung einzurichten ist.

Im Folgenden sehen Sie ein Beispiel für einen Fehler aufgrund nicht ausreichenden virtuellen Speichers:

```
Error[DBChannelCheck] [main Thread 2] - Error in channel check for
com.ibm.bcg.channel.CheckChannelParameters@ebda9664
com.ibm.ejs.cm.portability.ResourceAllocationException: DB2 SQL error:
SQLCODE: -955, SQLSTATE:57011, SQLERRMC: null

ERROR [BPEEngine] [main Thread 2] - BPE:

ERROR [BPEEngine] [main Thread 2] -
java.lang.ArrayIndexOutOfBoundsException: 0

ERROR [BPEEngine] [main Thread 2] - Error closing
transConn.com.ibm.ejs.cm.exception. WorkRolledbackException: Outstanding
work on this connection which was not committed or rolledback by the user
has been rolledback.
```

DB2 SQL-Fehler beheben

In den folgenden Abschnitten wird die Korrektur bestimmter DB2 SQL-Nachrichten behandelt:

- „Fehler mit SQLCODE-Wert -444"
- „Fehler mit SQLCODE-Wert -289" auf Seite 183
- „Fehler mit SQLCODE-Wert -1225" auf Seite 183
- „SQL-Fehler 0964C: Kein Platz mehr im Transaktionsprotokoll für die Datenbank BCGMAS" auf Seite 183

Fehler mit SQLCODE-Wert -444

Wenn beim Starten einer der WebSphere Partner Gateway-Komponenten (bcgconsole, bcgreceiver, bcgdocmgr) Fehlernachrichten mit dem SQLCODE-Wert -444 auftreten, sollten Sie den Wert des Parameters SHEAPTHRES des DB2-Datenbankmanagers erhöhen. Der Wert für diesen Parameter sollte mindestens doppelt so hoch sein wie der höchste definierte Sortierspeicherwert für eine beliebige Datenbank in der DB2-Instanz. Wenden Sie sich an Ihren Datenbankadministrator, oder lesen Sie die Informationen im DB2-Administratorhandbuch, bevor Sie diese Einstellung ändern. Im Folgenden finden Sie einen Beispielbefehl:

```
db2 UPDATE DBM CFG USING SHEAPTHRES xxxxx IMMEDIATE
```

Wird der SQLCODE -444 auch weiterhin angezeigt, nachdem der Wert für SHEAPTHRES geändert wurde, können Sie die Werte für STMTHEAP und APPLHEAPSZ in der WebSphere Partner Gateway-Datenbank reduzieren. Im Folgenden finden Sie einen Beispielbefehl:

```
db2 UPDATE DB CFG FOR <datenbankname> USING STMTHEAP xxxxx
db2 UPDATE DB CFG FOR <datenbankname> USING APPLHEAPSZ xxxxx
```

Wenden Sie sich an Ihren Datenbankadministrator, oder lesen Sie die Informationen im DB2-Administratorhandbuch, bevor Sie eine dieser Einstellungen ändern.

Sie finden sie auch in der Datei *<db2-ausgangsverzeichnis>*\SQLLIB\bin\db2diag.log.

Fehler mit SQLCODE-Wert -289

Der DB2-Fehlercode -289 gibt an, dass die Datenbank im Dateisystem nicht mehr ausreichend Speicherplatz zur Verfügung hat. Sprechen Sie mit dem Datenbankadministrator ab, ob auf dem Datenbankserver zusätzliche Speicherkapazitäten bereitgestellt werden können.

Alternativ können die WebSphere Partner Gateway-Daten an einer anderen Speicherposition archiviert werden, um Plattenspeicherplatz freizugeben.

Fehler mit SQLCODE-Wert -1225

Wenn zu wenig DB2-Ressourcen im System vorhanden sind, empfangen Sie möglicherweise einen Fehler mit dem SQLCODE-Wert -1225, und in den Serverprotokollen von WebSphere Partner Gateway ist ein Stack-Trace vorhanden. Im Folgenden wird ein Beispiel für diesen SQLCODE-Fehler dargestellt:

```
java.sql.SQLException: com.ibm.db2.jcc.c.SqlException:
DB2 SQL error: SQLCODE: -1225, SQLSTATE: 57049, SQLERRMC: null
```

Dieser Fehler tritt üblicherweise auf, wenn die Transaktionsraten hoch sind (d. h. eine große Anzahl von Dokumenten pro Sekunde) und DB2 diese Transaktionsrate nicht aufrechterhalten kann. Der Datenbankadministrator kann die Datenbank überwachen und optimieren, damit die zwischenzeitlich hohen Transaktionsraten bewältigt werden können. Sie können die Leistung der Datenbankprotokollierung verbessern, indem Sie die folgenden DB2-Parameter optimieren:

- LOGPRIMARY
- LOGSECOND
- LOGFILESIZ

SQL-Fehler 0964C: Kein Platz mehr im Transaktionsprotokoll für die Datenbank BCGMAS

WebSphere Partner Gateway erstellt die Datenbank BCGMAS mit den folgenden Standardkonfigurationswerten:

```
LOGFILSIZ=1024
LOGPRIMARY=13
LOGSECOND=4
```

Die für das DB2-Transaktionsprotokoll erforderliche Speichergröße hängt von verschiedenen Faktoren ab, wie z. B. der höchsten Anzahl an Dokumenten, die von WebSphere Partner Gateway innerhalb eines angegebenen Zeitraums verarbeitet werden. Falls Sie feststellen, dass WebSphere Partner Gateway in den Wartemodus übergeht, während sich noch Dokumente in der Warteschlange befinden, prüfen Sie die FFDC-Protokolle (FFDC - First-Failure Data Capture) im Hinblick auf den Server BCGMAS. Wenn sich dabei herausstellt, dass der Server BGMAS mit dem SQL-Fehler 0964C fehlgeschlagen ist, erhöhen Sie die Größe (über Parameter LOGFILESIZ) und die Anzahl (über Parameter LOGPRIMARY und LOGSECOND) der Transaktionsprotokolle für die Datenbank BCGMAS.

IBM Serviceprotokoll nicht lesbar

In den Vorgängerreleases von WebSphere Partner Gateway konnten Protokolle mit einem Texteditor oder dem Befehl `more` angezeigt werden. Im aktuellen Release liegen mehrere Protokolle im Binärformat vor und können nicht mit einem Texteditor oder durch Eingabe des Befehls `more` in einer Befehlszeile gelesen werden. Wenn Ihr Serviceprotokoll bei Verwendung einer dieser Methoden verzerrt dargestellt wird, konvertieren Sie das Serviceprotokoll vom Binärformat in einfachen Text, indem Sie wie unten gezeigt den Befehl `showlog` von der Workstation aus absetzen, auf der sich das Tool befindet.

```
showlog -format CBE-XML-1.0.1 dateiname
```

Dabei gilt, dass *dateiname* der Dateiname der Serviceprotokolldatei ist. Hinweis: Wenn das Serviceprotokoll sich nicht im Standardverzeichnis befindet, müssen Sie den Namen der Serviceprotokolldatei vollständig qualifizieren.

Der Befehl `showlog` produziert eine Ausgabe im CBE-XML-Format (CBE - Common Base Event). Weitere Beispiele für die Showlog-Scripts finden Sie unter `http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/ttrb_viewsvclog.html`.

WebSphere Application Server-Informationsnachrichten

Einige der WebSphere Application Server-Nachrichten, die als Fehler in den WebSphere Partner Gateway-Systemausgabeprotokollen aufgezeichnet werden, sind eigentlich Informationsnachrichten und weisen nicht auf ein WebSphere Partner Gateway-Problem hin. Weitere Informationen zur Interpretation der Protokoll- und Tracenachrichten von WebSphere Application Server finden Sie im Abschnitt „Protokoll- und Tracenachrichten von WebSphere Application Server interpretieren” auf Seite 163.

Einstellung für Empfängerzeitlimit erhöhen

Wenn ein Partner eine Verbindung zu WebSphere Partner Gateway herstellt und die Fehlernachricht empfängt, dass die Verbindung vom Peer aufgrund eines Socketschreibfehlers abgebrochen wurde, leitet der WebSphere Partner Gateway-Empfänger die Überschreitung des Zeitlimits aufgrund der niedrigen Übertragungsrate des Partners ein.

Wechseln Sie in die Admininistrationskonsole von WebSphere Application Server und gehen Sie wie folgt vor:

1. Navigieren Sie zu **Anwendungen**.
2. Wählen Sie die betreffende WebSphere Partner Gateway-Empfängerkomponente aus.
3. Wählen Sie **Webcontainer** > **Transportkette für Webcontainer** aus.
4. Ändern Sie die Einstellungen für das Zeitlimit für die betreffenden WebSphere Partner Gateway-Empfängerports.

Datenbankabfrageleistung optimieren

Der Befehl RUNSTATS aktualisiert den Datenbankabfragezugriffsplan für jede Tabelle und jeden Index. Wenn Sie die Datenbankabfrageleistung optimieren möchten, sollten Sie RUNSTATS mindestens einmal pro Woche ausführen, sofern die Anwendung und die Datenbankaktivität von IBM WebSphere Partner Gateway nur sehr gering ist. Mit zunehmendem Datenbankverkehr sollten Sie RUNSTATS häufiger ausführen, bis zu einmal täglich.

Anmerkungen:

1. Da RUNSTATS die Datenbanksysteminformationen aktualisiert, können unter bestimmten Umständen eventuell Zeitsperren auftreten. Es wird empfohlen, die WebSphere Partner Gateway-Anwendung in den Wartemodus zu versetzen und den Datenbankzugriff auf die Ausführung von RUNSTATS zu beschränken.
2. Eine Zeitsperre kann auftreten, wenn RUNSTATS und db2rbind gleichzeitig ausgeführt werden. Es wird empfohlen, diese Befehle täglich zu unterschiedlichen Zeiten auszuführen.

Eine weitere Möglichkeit, den DB2-Zugriffsplan zu aktualisieren, besteht über den Befehl `reorgchk`. Führen Sie über ein DB2-Befehlsfenster die folgenden Befehle aus:

1. `db2 connect to <datenbankname>`
2. `db2 -v reorgchk update statistics on table all.`
3. `db2 connect reset.`

Anmerkung: Stellen Sie sicher, dass alle WebSphere Partner Gateway-Komponenten gestoppt sind, bevor Sie mit dieser Prozedur beginnen. Wenn Sie den Befehl `reorgchk` abgeschlossen haben, sollten Sie außerdem die Datenbankinstanz stoppen und erneut starten.

Ereignis 210031 beheben

Sie können das Ereignis 210031 empfangen, während ein Dokument die Unbestreitbarkeit ausführt, wenn einer der folgenden Vorfälle auftritt:

- Die Datenbank- oder Netzverbindung ist ausgefallen.
- Die Netzverbindung zum gemeinsamen Dateisystem ist ausgefallen.
- Der Plattenspeicherplatz des gemeinsamen Dateisystems ist voll.

Um dieses Ereignis zu beheben, sollten Sie in dem mit dem Ereigniscode 210031 fehlgeschlagenen Dokument folgende Bedingungen überprüfen, bevor Sie das Dokument erneut senden:

1. Prüfen Sie, ob die WebSphere Partner Gateway-Datenbank und das Netz zur Datenbankworkstation eingerichtet und aktiv sind.
2. Prüfen Sie, ob zwischen dem gemeinsamen Dateisystem und den WebSphere Partner Gateway-Komponenten Netzkonnektivität besteht.
3. Prüfen Sie, ob das allgemeine Dateisystem über ausreichend freien Speicherbereich verfügt, um die Dokumente zu schreiben.

Dokumente werden bei unterbrochener Netzverbindung oder bei abrupter Beendigung von Document Manager-Server zweimal weitergeleitet

Wenn die Netzverbindung des Systems, auf dem Document Manager ausgeführt wird, abrupt unterbrochen oder während der Verarbeitung eines Dokuments beendet wird, dessen Status noch nicht aktualisiert wurde, wird das Dokument möglicherweise zweimal gesendet. Der Systemadministrator sollte Maßnahmen ergreifen, um unerwartete Systembeendigungen oder nicht planmäßige Ausfallzeiten der Document Manager-Workstation zu vermeiden.

0A1-Generierung mit Datenvalidierungsfehlern

Gemäß 0A1-Spezifikation muss das Attribut "GlobalSupplyChainCode" in der XML-Datei vorhanden sein. Wenn das eingehende 3A7-Dokument diesen Wert nicht enthält, muss er als Attribut zum 0A1-Dokument hinzugefügt werden. "GlobalSupplyChainCode" muss also entweder im 3A7-Dokument definiert sein oder als 0A1-Attribut zur Dokumentdefinition hinzugefügt werden.

Gehen Sie wie folgt vor, um das Attribut hinzuzufügen:

1. Klicken Sie auf **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition**. In der Community Console wird das Fenster **Dokumentdefinitionen verwalten** geöffnet.
2. Klicken Sie auf **Paket: RNIF** > **Protokoll: Rosettanet** > **Dokumenttyp: 0A1** und klicken Sie auf das Symbol **Attributwerte bearbeiten**.
3. Wenn das Attribut "GlobalSupplyChainCode" dort nicht vorhanden ist, klicken Sie auf **Attribute hinzufügen**, um es hinzuzufügen.
4. Wählen Sie einen Wert in der Liste aus.
5. Klicken Sie auf **Speichern**.

EDI-Berichte exportieren nur die ersten 1000 Datensätze

Die Exportfunktion der beiden EDI-Berichte "Bericht für überfällige funktionale EDI-Bestätigungen" und "Bericht für zurückgewiesene EDI-Transaktionen" exportiert nur die ersten 1000 Datensätze, um zu vermeiden, dass das System aufgrund eines Speicherüberlaufs unerwartet beendet wird. Wenn die Anzahl der zu exportierenden Datensätze aus diesen beiden Berichten größer als 1000 ist, exportieren Sie sie direkt aus der zugehörigen Datenbanksicht: `LG_EDI_Overdue_FA_VW` oder `LG_EDI_Rejected_Tx_VW`.

Konsole wird nach Serverneustart nicht gestartet

Wenn Sie WebSphere Partner Gateway installiert, den Konsolenserver gestartet und sich erfolgreich an der Konsole angemeldet haben, jedoch feststellen, dass nach erneutem Starten des Servers die Konsole nicht angezeigt wird und in einer Schleife läuft, sollten Sie sicherstellen, dass Ihre Traceebene nicht auf "WAS.*=finest" (= Am Feinsten) gesetzt wurde. Diese Einstellung wird verwendet, um die genaueste Protokollierung aller zu WebSphere Application Server gehörenden Klassen auszuführen. Das Standardverbindungszeitlimit, innerhalb dessen die WebSphere Partner Gateway-Konsole starten muss, ist mit 180 Sekunden festgelegt, und wenn die Traceebene von WebSphere Application Server auf "AM FEINSTEN" gesetzt wurde, wird durch die Verarbeitungszeit, die für die Protokollierung aller Informationen

und das Herstellen der erforderlichen Datenbankverbindungen benötigt wird, eine Zeitlimitüberschreitung im System verursacht. Ändern Sie die Einstellung und starten Sie den Konsolenserver erneut.

Anmerkung: Wenn die Traceebene auf "AM FEINSTEN" gesetzt wurde, kann dies die Systemleistung beeinträchtigen.

FTP-Scriptingempfänger empfängt Ausnahmebedingung "StringIndexOutofBoundsException"

Wenn Sie die Ausnahmebedingung "StringIndexOutOfBoundsException" beim Herstellen einer Verbindung zu einem Pro FTP-Server empfangen, bitten Sie den Partner darum, alle Leerzeilen aus der Willkommensnachricht für den FTP-Server zu entfernen. Der FTP-Server sendet diese Nachricht immer, wenn ein Client eine Verbindung zum FTP-Server herstellen will.

Fehlerszenario

Im folgenden Beispiel werden die Leerzeilen ("blank line") in der Willkommensnachricht mitangezeigt.

```
ftp myftp.mycompany.com
Connected to myftp.mycompany.com
220-
<blank line>
You have connected to myftp.mycompany.com FTP Server.
<blank line>
Please enter userid and password to login
<blank line>
220 MYCOMPANY FTP Server ready.
User (myftp.mycompany.com:(none)):
```

Korrektes Szenario

Im folgenden Beispiel wurden die Leerzeilen aus der Willkommensnachricht entfernt.

```
ftp myftp.mycompany.com
Connected to ftp myftp.mycompany.com
220-You have connected to myftp.mycompany.com FTP Server.
Please enter userid and password to login
220 MYCOMPANY FTP Server ready.
User (myftp.mycompany.com:(none)):
```

Empfänger konnte Konfigurationsdatei nicht lesen

Wenn der Empfänger die Konfigurationsdatei nicht lesen konnte, wird die folgende Fehlernachricht angezeigt:

```
Unable to update the Receiver Config file java.io.IOException: A file
or directory in the path name does not exist.
```

Dieser Fehler tritt auf, wenn der Empfänger von WebSphere Partner Gateway startet, keine Verbindung zur Datenbank erhält und versucht, die Konfigurationsdaten aus der Datei `BCGReceiverConfiguration.xml` zu lesen. Die Datei `BCGReceiverConfiguration.xml` befindet sich in einem Ordner, der auf der Seite **Systemverwaltung** der Konsole durch das Attribut `bcg.receiver.configpath` angegeben wird.

Stellen Sie sicher, dass der in `bcg.receiver.configpath` angegebene Pfad korrekt ist.

Benutzer für Empfang von Alertbenachrichtigungen konfigurieren

Wenn die SMTP-Konfiguration nicht auf der Seite **Systemverwaltung** der WebSphere Partner Gateway-Konsole angegeben wurde, werden die konfigurierten Alerts nicht an die Benutzer gesendet, da Document Manager die dafür notwendige SMTP-Konfiguration nicht finden kann.

Aktualisieren Sie die Werte der beiden folgenden Attribute, um die Alerts zu konfigurieren:

- Aktualisieren Sie auf der Seite **Systemverwaltung** > **DocMgr-Verwaltung** > **Alertengine** das Attribut **bcg.alertNotifications.mailHost**.
- Aktualisieren Sie auf der Seite **Systemverwaltung** > **DocMgr-Verwaltung** > **Zustellmanager** das Attribut `bcg.delivery.smtpHost`.

Optional können Sie die Werte der Attribute `bcg.alertNotifications.mailFrom` und `bcg.alertNotifications.mailReplyTo` ändern.

Ausnahmebedingung "ClassNotFoundException" für Benutzerexitklassen beheben

Der Fehler "ClassNotFoundException" kann auftreten, wenn eine erforderliche Klasse für die folgenden Benutzerexits nicht gefunden wurde:

- Empfänger-Benutzerexits
- Benutzerexit für angepasste Aktionen
- Absender-Benutzerexits

Wenn der Fehler "ClassNotFoundException" auftritt, prüfen Sie Folgendes:

1. Wenn die Benutzerexits zu Empfänger-Benutzerexits gehören, prüfen Sie, ob die zugehörige JAR-Datei oder die Klassen in einem der folgenden Ordner vorhanden sind:
   - *<WebSphere_Partner_Gateway_installationsverzeichnis>*`/Receiver/lib/userexits`
   - *<WebSphere_Partner_Gateway_installationsverzeichnis>*`/Receiver/lib/userexists/classes`
2. Wenn die Benutzerexits zu Document Manager gehören, prüfen Sie, ob die zugehörige JAR-Datei oder die Klassen in den folgenden Ordnern vorhanden sind:
   - *<WebSphere_Partner_Gateway_installationsverzeichnis>*`/Router/lib/userexits`
   - *<WebSphere_Partner_Gateway_installationsverzeichnis>*`/Router/lib/userexits/classes`
3. Wenn die JAR-Datei oder die Klassendateien für die Benutzerexits an der korrekten Position vorhanden sind, prüfen Sie, ob die zugehörige gemeinsam genutzte Bibliothek der Benutzerexits korrekte Einträge aufweist. Gehen Sie dazu wie folgt vor:
   a. Öffnen Sie die Administrationskonsole von WebSphere Application Server.
   b. Wählen Sie **Umgebung** > **Gemeinsam genutzte Bibliotheken** aus.
   c. Suchen Sie nach `BCG_RCVR_USEREXISTS` und `BCG_ROUTER_USEREXITS`.
   d. Bearbeiten Sie die Daten für gemeinsam genutzte Bibliotheken in diesen Attributen und stellen Sie sicher, dass die zugehörigen JAR-Dateien oder Klassen dem Klassenpfad hinzugefügt werden.

In Datenbank nicht protokollierte Ereignisse und Geschäftsdokumente erneut verarbeiten

Wenn WebSphere Partner Gateway den Status eines Ereignisses oder Dokuments nicht in seiner Datenbank protokollieren kann, werden die Daten in die DATALOGERRORQ-Warteschlange eingefügt, um später erneut verarbeitet zu werden, wenn das Problem gelöst ist.

Verwenden Sie für eine erneute Verarbeitung dieser fehlgeschlagenen Ereignisse und Dokumente das manuelle Dienstprogramm `reprocessDbLoggingErrors.sh`. Dieses Dienstprogramm entfernt sämtliche Ereignisse und Dokumente aus der Warteschlange DATALOGERRORQ und fügt sie erneut in die Warteschlange DATALOGQ ein. Dadurch kann DocumentLogReceiver die Ereignisse und Dokumente erneut in der Datenbank protokollieren.

Das Dienstprogramm stoppt, nachdem es alle in DATALOGERRORQ vorhandenen Ereignisse und Dokumente verarbeitet hat. Etwaige Ereignisse und Dokumente, die nicht protokolliert werden können, werden erneut in DATALOGERRORQ gestellt; dieses Mal stellt das Dienstprogramm jedoch sicher, dass das Ereignis oder Dokument nur ein einziges Mal erneut verarbeitet wird (d. h., das Dienstprogramm beginnt nicht mit einer Endlosschleife von fehlgeschlagenen Ereignissen und Dokumenten).

Gehen Sie wie folgt vor, um die Dienstprogramme `reprocessDbLoggingErrors.sh` oder `reprocessDBLoggingErrors.bat` auszuführen:

1. Prüfen Sie, ob alle Variablen in `reprocessDbLoggingErrors.sh` für alle Router korrekt definiert wurden:

   ```
   REPROCESSOR_HOME=Document Manager installation root
   JAVA_HOME=$REPROCESSOR_HOME/java
   LOG_REPROCESSOR_CLASSES=$REPROCESSOR_HOME/classes
   ```

2. Führen Sie das Dienstprogramm über die Befehlszeile wie folgt aus:

   `./reprocessDbLoggingErrors.sh` oder `reprocessDBLoggingErrors.bat`.

JIT auf WebSphere Application Server inaktivieren, wenn WebSphere Partner Gateway eine Java-Core-Dump-Datei produziert

Wenn die WebSphere Partner Gateway-Komponenten (Empfänger, Document Manager oder die Konsole) abrupt beendet werden und eine Java-Core-Dump-Datei produzieren, liegt das üblicherweise an einem Problem mit dem Java-JIT-Compiler. Wenn dieses Verhalten auftritt, sollten Sie JIT in der Admininistrationskonsole von WebSphere Application Server inaktivieren.

Gehen Sie wie folgt vor, um JIT im WebSphere Application Server zu inaktivieren:

1. Melden Sie sich an der Admininistrationskonsole von WebSphere Application Server an.
2. Klicken Sie unter **Server** auf **Server** und wählen Sie den WebSphere Partner Gateway-Server aus.
3. Wählen Sie auf der Konfigurationsseite **Java- und Prozessverwaltung** > **Prozessdefinition** aus.
4. Wählen Sie in **Weitere Merkmale** die Option **Java Virtual Machine** aus.
5. Wählen Sie das Kontrollkästchen **JIT inaktivieren** aus.

Angepassten Transporttyp definieren

Wenn Sie einen angepassten Transporttyp definieren, dürfen Sie kein Attribut mit dem Namen "URI" erstellen. Dies stünde im Konflikt mit einem reservierten Schlüsselwort in WebSphere Partner Gateway. Daher ist es nicht möglich, ein Ziel mit einem solchen Transporttyp zu erstellen und zu speichern.

Beispiel: <*tns2:attributname*>URI</*tns2:attributname*> darf nicht verwendet werden.

WebSphere Partner Gateway-Fehler BCG210031 und BCG240415 beheben

WebSphere Partner Gateway versucht ständig, dasselbe Dokument zu verarbeiten und gibt die folgenden Fehler aus:

BCG210031: Dokument kann nicht als ablehnbares Dokument (Non-Rep) behandelt werden: {0}.

BCG240415: AS-Packprogrammfehler: {0}

Im Folgenden sehen Sie ein Beispiel für die Nachrichten, die die Datei `router.log` enthält:

```
17 Oct 2005 17:55:30,681 ERROR [BPEEngine] [main Thread 1] - Error in nonRepProcess
17 Oct 2005 17:55:30,681 ERROR [BPEEngine] [main Thread 1] - java.io.FileNotFoundException:
/opt/wbi/ca/common/data/Inbound/process/917/fa/xxx (A file or directory in the path name does not exist.)
at java.io.FileInputStream.open(Native Method)
 at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
 at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
at com.ibm.bcg.util.NonRepudiationDbImpl.copyFile(NonRepudiationDbImpl.java
(Compiled Code))
at com.ibm.bcg.util.NonRepudiationDbImpl.store(NonRepudiationDbImpl.java(Compiled Code))
at com.ibm.bcg.server.BPEBean.doNonRepudiation(BPEBean.java(Compiled Code))
at com.ibm.bcg.server.BPEBean.processDocument(BPEBean.java(Compiled Code))

ASPackaging Exception:java.io.FileNotFoundException:
/opt/wbi/ca/common/data/Inbound/process/917/fa/xxx (A file or directory in the path name does not exist.)
at java.io.FileInputStream.open(Native Method)
 at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
 at java.io.FileInputStream.<init>(FileInputStream.java(Inlined Compiled Code))
at com.ibm.bcg.util.Util.readFile(Util.java(Compiled Code))
at com.ibm.bcg.ediint.ASPackaging.process(ASPackaging.java(Compiled Code))
at com.ibm.bcg.ediint.ASPackaging.process(ASPackaging.java(Inlined Compiled Code))
at com.ibm.bcg.ediint.ASPackagingHandler.process(ASPackagingHandler.java(Compiled Code))
at com.ibm.bcg.server.HandlerProcessWrapper.process(HandlerProcessWrapper.java (Compiled Code))
at com.ibm.bcg.server.DocumentProcessor.process(DocumentProcessor.java(Compiled Code))
at com.ibm.bcg.server.BPEBean.processDocument(BPEBean.java(Compiled Code))
```

Diese Fehler werden generiert, wenn das betroffene Dokument (in den Protokolldateien durch eine eindeutige Kennung bzw. Universal Unique Identifier (UUID) angegeben) im System durch die Warteschlange `main_inboundq` und den Ordner `data\inbound\serialize` kreist.

Gehen Sie wie folgt vor, um diesen Fehler zu beheben:

1. Stoppen Sie Document Manager.
2. Löschen Sie den Inhalt der Warteschlangen.
3. Entfernen Sie den betreffenden UUID-Eintrag aus der Warteschlange `main_inboundq` und dem Ordner `data\inbound\serialize`.

4. Wenn die Verarbeitung nicht beim ersten Mal erfolgreich ist, möglicherweise aufgrund von Ablaufsteuerungsbedingungen, führen Sie die oben beschriebenen Löschvorgänge im System erneut durch.
5. Die Datei `router.log` sollte nun keinen Fehler mehr enthalten, und die CPU-Belastung durch den Router sollte sich wieder normalisieren.

Dateiverzeichnisziel auf einem anderen Laufwerk als C: erstellen

Wenn eine WebSphere Partner Gateway-Zieladresse eines Dateiverzeichnisses für ein anderes Laufwerk als C: definiert wurde, gibt WebSphere Partner Gateway den Fehler `Zielverzeichnis ist nicht vorhanden` zurück. Die Konsole akzeptiert zwar die Erstellung des Dateiverzeichnisziels, generiert jedoch einen Fehler wie den folgenden, der zur Laufzeit auftritt:

```
17 Oct 2005 19:00:12,844 INFO [FileSender] [Gw_1_2] - Exception in delivering the message in first attempt.
 Exception is: java.lang.Exception: Destination directory '/wsi_gateway/inbound/tradingpartner01';
  does not exist at com.ibm.bcg.delivery.FileSender.getFileSystemProperties(FileSender.javA:244)

17 Oct 2005 19:00:12,844 ERROR [SenderFramework] [Gw_1_2] - First attempt failed: reason: java.lang.
 Exception : Destination directory '/wsi_gateway/inbound/tradingpartner01' does not exist
```

Wenn Sie einen Ordner auf einem anderen Laufwerk als C: definieren möchten, verwenden Sie drei Schrägstriche, statt nur zwei. Beispiel:

```
file:///d:\HubMgrGateway
```

Verarbeitung von Partnertransaktionen durch WebSphere Partner Gateway verhindern

Wenn die Verarbeitung von Dokumenten von und an einen Partner verhindert werden soll, muss der WebSphere Partner Gateway-Administrator die für den betreffenden Partner erstellten Verbindungen im Fenster **Verbindungen** der WebSphere Partner Gateway-Konsole inaktivieren.

Obwohl die Inaktivierung des Partnerprofils verhindert, dass die Entität im Menü **Partnerverbindungen** aufgelistet wird, werden dadurch nicht die aktiven Kanäle zwischen diesem Partner und dem internen Partner geschlossen.

Browserfehler ERROR: 500 beheben

Der Browser kann die Fehler `ERROR: 500` und `SRVE0026E: [Servlet Error]-[action]: java.lang.NullPointerException` in der Datei SystemOutlog anzeigen. Diese Fehler können in folgenden Situationen auftreten:

1. Nach der Installation von WebSphere Partner Gateway.
2. Nach dem Starten der Konsole.
3. Nach der Anmeldung als Hubadmin und der Änderung des Standardkennworts.

Diese Fehler können auftreten, weil entweder das Setzen von Cookies im Browser inaktiviert wurde oder weil die Firewall-Einstellungen für Cookies zu streng sind. Gehen Sie wie folgt vor, um diesen Fehler zu beheben:

1. Ändern Sie die Firewall-Sicherheitsstufe auf mittel oder mittel bis hoch.
2. Lassen Sie Cookies für den Browser zu.

Der Browserfehler ERROR: 500 kann auch auftreten, weil einer der Server nicht verfügbar ist.

1. Vergewissern Sie sich, dass sämtliche WebSphere Partner Gateway-Server aktiv sind.
2. Wenn alle Server aktiv sind, prüfen Sie die Protokolle, um die Fehlerursache zu ermitteln.

   Wenn WebSphere Partner Gateway in `C:\IBM\WPG` installiert ist:

   - Die Konsolprotokolle befinden sich in `C:\IBM\WPG\bcghub\was\profiles\bcgconsole\logs\bcgconsole`.
   - Die Empfängerprotokolle befinden sich in `C:\IBM\WPG\bcghub\was\profiles\bcgreceiver\logs\bcgreceiver`.
   - Die Document Manager-Protokolle befinden sich in `C:\IBM\WPG\bcghub\was\profiles\bcgdocmgr\logs\docmgr`.
3. Prüfen Sie in allen Ordnern das Protokoll `SystemErr`. In dieser Datei sollte die Zeitmarke des letzten Zugriffsversuchs enthalten sein.
4. Blättern Sie zum Ende der Datei, um die jüngsten Protokolleinträge anzuzeigen und die Fehlernachrichten zu prüfen.

CRL (Zertifikatswiderrufsliste) für SSL-Transaktionen herunterladen

SSL-Transaktionen (Secure Sockets Layer) können fehlschlagen, wenn Zertifikate verwendet werden, falls die CRL (Certificate Revocation List - Zertifikatswiderrufsliste) nicht verfügbar ist. Bei diesem Problem schlägt die SSL-Transaktion, die die Zertifikate verwendet, mit dem folgenden Fehlerereignis fehl:

BCG240024: CertPath-Validierung ist fehlgeschlagen.

Das Routerprotokoll für das Ereignis 240024 weist auf die Tatsache hin, dass der Widerrufsstatus des Zertifikats nicht festgestellt werden konnte.

Führen Sie die folgenden Schritte aus, um den Fehler zu beheben:

1. Laden Sie die CRL von der Website der Zertifizierungsstelle herunter, die im Feld für die Verteilungspunkte der CRL (CRL Distribution Point - CRL-DP) auf der Registerkarte mit den Details angegeben ist oder von der Download-Site der Zertifizierungsstelle zur Verfügung gestellt wurde.

   Beispiel: http://SVRSecure-crl.verisign.com/SVRTrialRoot2005.crl
2. Kopieren Sie die CRL in den WebSphere Partner Gateway-Ordner common/security/crl.

Anmerkung: Alternativ können Sie über den CRL-DP zur Laufzeit CRLs vom CRL-DP abrufen.

Datenbindung in JMS-Exporten und -Importen in WebSphere Process Server

Wenn Sie die WebSphere Partner Gateway-Datenbindung in JMS-Exporten und -Importen in WebSphere Process Server verwenden, gibt es bestimmte Nachrichten, die falsche oder nicht relevante Informationen liefern. Wenn Sie die WebSphere Partner Gateway-Datenbindung in JMS-Exporten und -Importen in WebSphere Process Server verwenden, werden die folgenden Nachrichten ausgegeben:

```
[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm. bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-MsgTypeMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-MsgType'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
```

```
warning : Error in the element JMS-IBM-PutTimeMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-PutTime'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-Character-SetMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-Character-Set'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXDeliveryCountMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXDeliveryCount'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-EncodingMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-Encoding'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-PutApplTypeMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-PutApplType'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXGroupSeqMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXGroupSeq'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-System-MessageIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-System-MessageID'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXGroupIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXGroupID'

[11/1/05 14:14:07:426 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element x-out-filenameMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'x-out-filename'

[11/1/05 14:14:07:436 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-PutDateMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-PutDate'

[11/1/05 14:14:07:436 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXUserIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXUserID'

[11/1/05 14:14:07:436 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMS-IBM-FormatMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMS-IBM-Format'

[11/1/05 14:14:07:436 PST] 00000080 SystemOut O <<com.ibm.bcg.dataBinding.Utility>>
warning : Error in the element JMSXAppIDMsg :
Class 'BCGPackagingHeaders' does not have a feature named 'JMSXAppID'
```

Die vorstehenden Nachrichten sind keine Fehler und können ignoriert werden.

Testpartnerverbindung für SSL-Verbindungen korrigieren

Wenn die Tools- oder Testpartnerverbindung fehlschlägt, sobald eine HTTPS-Gateway-URL ausgewählt wird, wird die folgende Fehlernachricht angezeigt:

```
Exception during http POST-: null
```

Dieser Fehler kann auftreten, wenn der Befehl POST oder GET verwendet wird.

Die Tools- oder Testpartnerverbindung der Konsole funktioniert nur mit HTTP.

Fehler BCGEDIEV0O56 und BCG210001 beheben

Eine EDI-Transformationszuordnung kann mit dem Kanalprüffehler und mit den Fehlern BCGEDIEV0O56 und BCG210001 auf Oracle-Systemen fehlschlagen; außerdem kann das folgende Warnereignis produziert werden:

```
Warnereignis BCGEDIEV0O56 "Warnung bei Suche in der Konvertierungstabelle":
Die Suche in der Konvertierungstabelle lieferte keinen Eintrag während des
Entfernens eines Umschlags von einer Nachricht.
Weiter: "Kanalprüffehler - Kanalsuche ist fehlgeschlagen.
Nicht genügend Kanalinformationen vorhanden.
```

Dieser Fehler tritt auf, wenn die Oracle-Datenbank nicht mit dem Unicode-Zeichensatz erstellt, sondern fälschlicherweise auf Windows 1252 oder ähnliche Codepages gesetzt wurde, die nicht dem Unicode-Zeichensatz entsprechen.

Gehen Sie wie folgt vor, um den Zeichensatz unter Oracle zu überprüfen:

1. Stellen Sie eine Verbindung zur Oracle-Datenbank her.
2. Wählen Sie NLS_CHARACTERSET in v$nls_parameters aus.
3. Der zurückgegebene Wert sollte AL32UTF8 sein.
   Prüfen Sie dies auf Ihren Oracle-Systemen.

Es gibt keine direkte Art, den Zeichensatz der Datenbank zu ändern, wenn er einmal erstellt wurde. Die Datenbank muss neu erstellt werden, und der Zeichensatz und die nationalen Sonderzeichen müssen in Unicode definiert sein.

Fehler ORA-00988 beheben

Dieser Fehler tritt aufgrund einer Einschränkung in Oracle auf. Wenn ein Kennwort, dass mit einer Zahl beginnt, nicht mit Anführungszeichen angegeben wird, sehen Sie Folgendes:

```
ORA-00988: missing or invalid password(s)
```

Dieser Fehler lässt sich beheben, indem Sie in den Installationsanzeigen von WebSphere Partner Gateway alle Kennwörter für eine Oracle-Datenbank, die mit einer Zahl beginnen, in Anführungszeichen setzen (Beispiel: "123456ABC").

Attribut 'content-type' für Handler für festen Arbeitsablauf konfigurieren

WebSphere Partner Gateway schlägt möglicherweise bei dem Versuch fehl, ein EDI-Dokument weiterzuleiten, das über HTTP empfangen wurde. Ein EDI-Dokument wird mit dem Inhaltstyp 'text/plain' gesendet. Stellen Sie sicher, dass die Handler für den festen Arbeitsablauf korrekt konfiguriert wurden.

Das Attribut 'content-type' wird folgendermaßen festgelegt:

1. Wechseln Sie zu **Hubadmin > Hubkonfiguration > Fester Arbeitsablauf > Eingehend**.
2. Klicken Sie auf **com.ibm.bcg.server.ChannelParseFactory**.
3. Klicken Sie auf **Bearbeiten**.
4. Wählen Sie in der **Konfigurationsliste** den Eintrag für EDIRouterBizProcess-Handler aus und klicken Sie auf **Konfigurieren**.

5. Bearbeiten Sie das Attribut 'content-type', indem Sie dem Inhaltstyp 'text/plain' hinzufügen.

Dadurch wird der EDI-Handler ausgeführt und das Dokument wird als EDI verarbeitet. Die Werte für das Attribut 'content-type' müssen durch ein Komma voneinander getrennt werden.

Das Attribut 'content-type' wird für eine bestimmte Gruppe von Handlern verwendet. Diese Handler sind die folgenden:

- BinaryChannelParseHandler
- XMLRouterBizHandler
- EDIRouterBizProcessHandler
- cXMLChannelParseHandler

Diese Handler werden mit einer Standardliste von Inhaltstypen gefüllt. Gehen Sie wie folgt vor, um diese Inhaltstypen zu ändern:

1. Wechseln Sie zu **Hubadmin > Hubkonfiguration > Fester Arbeitsablauf > Eingehend**.
2. Klicken Sie auf **com.ibm.bcg.server.ChannelParseFactory**.
3. Klicken Sie auf **Bearbeiten**.
4. Wählen Sie in der **Konfigurationsliste** den Handler aus und klicken Sie auf **Konfigurieren**.
5. Bearbeiten Sie das Attribut 'content-type', indem Sie den neuen Inhaltstyp hinzufügen. Stellen Sie sicher, dass die Werte für das Attribut 'content-type' durch ein Komma voneinander getrennt sind.

Anmerkung: Die Werte für das Attribut 'content-type' sollten nur nach ausdrücklicher Empfehlung geändert werden.

Fehler BCG210013 beheben

Ein eingehendes Dokument kann aufgrund des folgenden Fehlers nicht empfangen werden:

```
BCG210013 - Verbindung nicht vollständig konfiguriert
```

Wenn alle anderen Konfigurationen korrekt zu sein scheinen, ist die häufigste Ursache für diesen Fehler eine falsche Empfängerspezifikation.

1. Stellen Sie sicher, dass vor den Definitionen der Empfänger-URL keine Leerzeichen enthalten sind.
2. Versuchen Sie das Problem einzugrenzen, indem Sie eine Test-EDI-Nachricht senden und dazu die anderen für die Partner verfügbaren Geschäfts-IDs verwenden. Versuchen Sie herauszufinden, ob es sich um ein spezielles Problem mit der Geschäfts-ID handelt.
3. Falls der vorherige Schritt fehlschlägt, erstellen Sie einen Debug-Trace des Fehlerszenarios wie folgt:
   a. Beenden Sie WebSphere Partner Gateway.
   b. Ändern Sie für WebSphere Partner Gateway die Debug-Einstellung für den Empfänger und den Router über den folgenden Befehl in AM FEINSTEN:
      ```
      "*=info:com.ibm.bcg.*=finest"
      ```
   c. Löschen Sie die laufenden Protokolle in den folgenden Verzeichnissen (oder sichern Sie sie in einem anderen Ordner):

- Bei der Installation mit einfachem Modus befinden sich die Protokolle in folgendem Verzeichnis:

  <WebSphere_Partner_Gateway_installationsverzeichnis>/wasND/Profiles/bcgprofile/logs/server1
- Bei der Installation mit verteiltem Modus befinden sich die Protokolle in folgendem Verzeichnis:
  - *<hub_installationsverzeichnis>*\wasND\Profiles\bcgprofile\logs\bcgreceiver
  - *<hub_installationsverzeichnis>*\wasND\Profiles\bcgprofile\logs\bcgdocmgr

d. Starten Sie WebSphere Partner Gateway erneut.

e. Führen Sie das Fehlerszenario nur einmal aus.

f. Komprimieren und senden Sie alle Protokolle in den oben genannten Ordnern zusammen mit einem Screenshot der Fehlernachricht in der Konsolenanzeige an die IBM Kundenunterstützung.

Puffergröße zur Vermeidung eines zu geringen Durchsatzes in Dokumentübertragung erhöhen

Die Dokumentübertragungszeit von WebSphere Partner Gateway kann exponentiell zunehmen und bis zu 40 Minuten betragen. Dies wird durch die zu niedrig definierte DB2-Standardpuffergröße verursacht, wodurch die Dokumente, die gerade verarbeitet werden, in die Warteschlange gestellt werden.

Gehen Sie wie folgt vor, um die Puffergröße zu erhöhen:

1. Öffnen Sie den DB2-Befehlszeilenprozessor: **Start** > **Programme** > **IBM DB2** > **Befehlszeilentool** > **Befehlszeilenprozessor**.
2. Stellen Sie mit dem folgenden Befehl eine Verbindung zur Datenbank her:

   ```
   DB2 > connect to bcgapps user <benutzername> using <kennwort>
   ```
3. Erhöhen Sie die Puffergröße mit folgendem Befehl:

   ```
   DB2 alter bufferpool buff32k immediate size 12500
   ```

   Dadurch wird die spezifische Puffergröße von 500 (Standard) auf 12500 erhöht.

Hubinstallationsprogramm von WebSphere Partner Gateway protokolliert Fehlernachrichten

Beim Ausführen des WebSphere Partner Gateway-Launchpads können ähnliche Fehler wie die folgenden angezeigt werden:

```
Jun 14, 2005 8:13:04 PM java.util.prefs.FileSystemPreferences$3 run
WARNING: Could not create system preferences directory. System preferences are unusable.
Jun 14, 2005 8:13:31 PM java.util.prefs.FileSystemPreferences checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code 270913688.
Jun 14, 2005 8:14:01 PM java.util.prefs.FileSystemPreferences checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code 270931432.
Jun 14, 2005 8:14:32 PM java.util.prefs.FileSystemPreferences checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code 270937824.
```

Diese Nachrichten können ohne weiteres ignoriert werden.

Fehler "DB password required" in bcgHubInstall.log

Während der Installation des WebSphere Partner Gateway-Hubs protokolliert das Installationsprogramm die folgenden Fehlernachrichten in `bcgHubInstall.log`:

```
com.ibm.bcg.install.ismp.wizard.conditions.JdbcDatabaseConnectCondition, err,
ERROR: dbPassword is required
```

Diese Fehlernachricht hat keine weiteren Auswirkungen. Die Server können erfolgreich gestartet werden und Dokumente können erfolgreich weitergeleitet werden. Diese Fehlernachricht kann ohne weiteres ignoriert werden.

Widerrufsprüfung und CRL-DP-Unterstützung verwenden

Wenn die Validierung des Zertifikatspfads ('CertPath') fehlschlägt, weil der Widerrufsstatus nicht geprüft werden konnte, weist dies möglicherweise darauf hin, dass die CRL (Certificate Revocation List - Zertifikatswiderrufsliste) nicht verfügbar ist. CRLs können in einem lokalen Ordner zur Verfügung gestellt oder automatisch vom Verteilungspunkt (DP - Distribution Point) für die CRL abgerufen werden (CRL Distribution Point - CRL-DP). Aktivieren Sie die CRL-DP-Unterstützung, wenn Sie die CRLs vom CRL-DP abrufen möchten.

Wenn für den Zugriff auf den CRL-DP ein Proxy-Server verwendet wird, müssen auch der Host und der Port des Proxy-Servers angegeben werden. Für selbst signierte Zertifikate wird keine Widerrufsprüfung ausgeführt.

Weitere Informationen finden Sie im Abschnitt „Eigenschaften für Zertifikatspfad ('CertPath') konfigurieren" auf Seite 58.

Rückgabe von Konsoleninformationen über Dokumentvolumenbericht - Suche

Die Suche des Dokumentvolumenberichts von WebSphere Partner Gateway gibt keine Informationen über die Konsole zurück.

Wenn Sie in der Konsole auf **Tools** > **Dokumentvolumenbericht - Suche** auf **Suchen** klicken, geschieht nichts. Auf der Seite wird nicht die typische rote Informationsnachricht "Nach Ihren Suchkriterien wurden keine Ergebnisse gefunden" angezeigt. Die Seite blinkt kurz und gibt nichts zurück.

Dieses Problem liegt am Popup-Blocker des Browsers, der verhindert, dass die Ergebnisseite (die eine Popup-Seite ist) korrekt angezeigt wird.

Wenn Sie den Popup-Blocker inaktivieren, wird die Seite korrekt angezeigt.

Für Mozilla Firefox:

1. Navigieren Sie zu **Extras** > **Optionen** > **Web-Funktionen**.
2. Löschen Sie den Inhalt des Felds zum Blocken von Popup-Fenstern.

Internet Explorer:

1. Klicken Sie auf **Extras**.
2. Navigieren Sie zu **Optionen > Popup-Killer** und klicken Sie anschließend auf **Popup-Blocker aktivieren**.
3. Klicken Sie auf **Extras** und auf **Internetoptionen**.

4. Navigieren Sie zur Registerkarte **Datenschutz** und klicken Sie dort auf **Popupblocker einschalten**.

Native Bibliothek laden

Wenn die WebSphere Partner Gateway-Komponenten gestartet werden, wird in den Protokollen möglicherweise folgende Nachricht angezeigt:

```
java.lang.UnsatisfiedLinkError: Can't find library AIXNative
(libAIXNative.a or .so) in sun.boot.library.path or java.library.path
```

Das System verwendet eine der folgenden Bibliotheken, je nachdem, auf welchem Betriebssystem WebSphere Partner Gateway ausgeführt wird:

- libWin32Native.dll
- libpLinuxNative.so
- libAixNative.a
- libSolarisNative.so
- libHPNative.so

Dieser Fehler wird zurückgegeben, wenn der Bibliothekspfad nicht korrekt festgelegt wurde. Beheben Sie diesen Fehler wie folgt:

1. Melden Sie sich an der Admininistrationskonsole von WebSphere Application Server an.
2. Wählen Sie **Umgebung** > **Gemeinsam genutzte Bibliotheken** aus.
3. Bearbeiten Sie die folgenden Eigenschaften:
   - BCG_NAV_CONSOLE
   - BCG_NAV_RCVR
   - BCG_NAV_ROUTER_BPE
   - BCG_NAV_ROUTER_DOCMGR
4. Beachten Sie den Pfad, der in "nativer Bibliothekspfad" gezeigt wird.
5. Prüfen Sie im angegebenen Bibliothekspfad, ob die betreffende .dll-Datei, .so-Datei oder .a-Datei vorhanden ist.
6. Wenn die Bibliothek nicht vorhanden ist, kopieren Sie sie aus einer anderen Position.
7. Prüfen Sie, ob die gemeinsam genutzten Bibliotheken jeweils einer WebSphere Partner Gateway-Anwendung zugeordnet sind. Gehen Sie dazu wie folgt vor:
   a. Klicken Sie auf der Anwendungsseite der Administrationskonsole von WebSphere Application Server auf eine der WebSphere Partner Gateway-Anwendungen, die bcgDocMgr enthält.
   b. Klicken Sie auf **Referenzen auf gemeinsam genutzte Bibliotheken**.
   c. Stellen Sie sicher, dass die Anwendung der Bibliothek BCG_NAV_ROUTER_DOCMGR zugeordnet ist. Falls sie der Bibliothek nicht zugeordnet ist, ordnen Sie sie jetzt zu.
   d. Wiederholen Sie diesen Vorgang für andere Anwendungen:
      - Für die gemeinsam genutzte Bibliothek der Konsole ist die zugeordnete Bibliothek BCG_NAV_CONSOLE.
      - Für den WebSphere Partner Gateway-Empfänger ist die zugeordnete gemeinsam genutzte Bibliothek BCG_NAV_RCVR.
      - Für die BPE-Anwendung (Business Process Engine) von WebSphere Partner Gateway ist die zugeordnete gemeinsam genutzte Bibliothek BCG_NAV_ROUTER_BPE.

Fehler TCPC0003E und CHFW0029E beheben

Der Start der WebSphere Partner Gateway-Empfängerkomponente schlägt möglicherweise mit den Fehlern TCPC0003E und CHFW0029E in der Datei `SystemOut.log` fehl. Diese Fehler können aufgrund folgender Rahmenbedingungen auftreten:

1. Da die konfigurierten Ports auch von anderen Anwendungen verwendet werden können, prüfen Sie, ob Portkonflikte bestehen.
2. Portnummern unter 1024 sind privilegierte Ports, die dem Benutzer "Root" vorbehalten sind. Benutzer ohne Rootberechtigung können daher diese Ports nicht belegen, es sei denn, Ihr System wurde eigens dafür konfiguriert, diese Einschränkung handhaben zu können. WebSphere Partner Gateway verwendet zum Starten von Komponenten einen WebSphere Partner Gateway-Benutzer ohne Root-Berechtigung und kann keine Bindung zu privilegierten Ports herstellen. Der Benutzer "bcguser" ist ein Beispiel für einen WebSphere Partner Gateway-Benutzer.

   Anmerkung: Bei WebSphere Partner Gateway können Benutzer ohne Rootberechtigung den Empfänger starten, können aber keine bindung zu privilegierten Ports herstellen.

Ändern Sie die Empfängerports in verfügbare Ports (d. h. in Ports, die nicht von anderen Anwendungen verwendet werden) und in größere Ports als 1024. Im folgenden Beispiel wird gezeigt, wie Sie Port 80 in *nnn* ändern.

1. Stoppen Sie den Empfänger.
2. Suchen Sie in den folgenden Dateien Portnummer 80 und ersetzen Sie sie durch *nnn*:

   Anmerkung: Führen Sie ein Backup aller Dateien vor der Bearbeitung aus.

   a. Bearbeiten Sie im Verzeichnis <*installationspfad*>`bcghub/was/profiles/bcgreceiver` die folgenden Dateien:
      1) `config\cells\DefaultNode\virtualhosts.xml`
      2) `config\cells\DefaultNode\nodes\DefaultNode\serverindex.xml`
      3) `config\templates\servertypes\APPLICATION_SERVER\serverindex.xml`
      4) `installedFilters\wlm\bcgreceiver\target.xml`
      5) `logs\portdef.props`
   b. Bearbeiten Sie <*installationspfad*>`\bcghub\receiver\lib\config\bcg_receiver.properties`.

   Anmerkung: Sie können die Portnummer auch über die Administrationskonsole von WebSphere Application Server ändern. Gehen Sie dazu auf die Seite `Server > Ports` und ändern Sie den Port in **WC_defaulthost**.
3. Starten Sie den Empfänger.
4. Geben Sie die Empfänger-URL in Ihren Browser ein, um sicherzustellen, dass der Empfänger korrekt arbeitet: `http://`<*hostname*>`:xyz/bcgreceiver`. Das ordnungsgemäße Ergebnis ist die Browser-Rückmeldung "Unsupported Operation". Wenn der Browser stattdessen "The page cannot be displayed" zurückgibt, konnte der Empfänger keine erfolgreiche Bindung zu dem Port herstellen.

Ablauf des CA-Zertifikats

Nur die Zertifikate, die für die Verschlüsselung, Signatur und den SSL-Client verwendet werden, werden nach Ablauf inaktiviert. Das CA-Zertifikat wird zwar nicht inaktiviert, wenn es abläuft, es wird jedoch nicht zur Laufzeit verwendet.

Wenn das Root- oder das Intermediate-Zertifikat zwischen zwei Serverneustarts abläuft, werden diese Zertifikate nicht mehr in die Liste der vertrauenswürdigen Zertifikate aufgenommen. Wenn also die Zertifikatspfaderstellung ('CertPath') fehlschlägt, weil ein CA-Zertifikat nicht gefunden werden konnte, ist eine mögliche Ursache ein abgelaufenes CA-Zertifikat.

Wenn ein Root- oder Intermediate-Zertifikat zur Laufzeit abläuft, schlägt die Zertifikatspfaderstellung fehl, und die zugehörige Verschlüsselung, die digitale Signatur oder die SSL-Zertifikate werden in der Geschäftstransaktion nicht verwendet.

Den Gültigkeitsstatus des Zertifikats finden Sie in der WebSphere Partner Gateway-Konsole. In der WebSphere Partner Gateway-Konsole wird der Gültigkeitszeitraum von Zertifikaten auf der Seite **Zertifikatliste** angezeigt. Falls das Zertifikat abgelaufen ist, wird der Gültigkeitszeitraum in rot angezeigt.

Wenn das CA-Zertifikat abgelaufen ist, besorgen Sie sich bei der Zertifizierungsstelle, die das Zertifikat ausgestellt hatte, ein neues Zertifikat. Das neue CA-Zertifikat sollte in die WebSphere Partner Gateway-Konsole hochgeladen werden.

Anmerkung: Wenn das hochgeladene Zertifikat ein selbst signiertes Zertifikat zur Serverauthentifizierung ist und wenn es abgelaufen ist, wird es in der WebSphere Partner Gateway-Konsole inaktiviert.

Ausnahmebedingung VCBaseException in der Datei SystemOut.log

Wenn eine Ausnahmebedingung beim Konfigurieren des Hubs über die Konsole auftritt, zeigt das Konsolprotokoll die Ausnahmebedingung auch als Teil der Protokolldaten an. Wenn Sie z. B. versuchen, eine bereits vorhandene Interaktion zu erstellen, empfangen Sie in der Datei `SystemOut.log` die Ausnahmebedingung VCBaseException. Diese Ausnahmebedingung ist als Teil der Protokollierung akzeptabel.

Größe der Berichtsdatei für Dokumente über 2 GB

Wenn ein Dokument größer als 2 GB ist, zeigt WebSphere Partner Gateway in der Dokumentanzeige die Dateilänge möglicherweise mit 0 KB an. Der Grund dafür ist ein Maximalwert für diesen Datenbankdatentyp.

SSL-Handshake schlägt wegen nicht empfangenen Zertifikats fehl

Dieses Problem tritt während des SSL-Handshake zwischen einem Partner und WebSphere Partner Gateway auf, wenn Sie Daten an einen Partner über SSL (Secure Sockets Layer) mit Clientauthentifizierung senden. Wenn der Partner die Liste der Zertifikate von den Zertifizierungsstellen nicht sendet, sendet WebSphere Partner Gateway das Clientzertifikat nicht. Dies verursacht das Fehlschlagen des SSL-Handshake.

Ändern Sie in den WebSphere Application Server-Installationen die Datei `java.security`, um das Fehlschlagen des SSL-Handshake zu beheben. Die Datei befindet sich im Verzeichnis *<WAS_installationsverzeichnis>*`\java\jre\lib\security`.

Anmerkung: Verwenden Sie unter UNIX den Schrägstrich (/) anstelle des Backslash (\ ).

Die Standardreihenfolge der Provider lautet in der Datei `java.security` wie folgt:

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ibm.jsse.IBMJSSEProvider
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
#security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
```

Stellen Sie in der Datei `java.security` den Provider IBMJSSE2 vor den Provider IBMJSSE, wie im folgenden Beispiel dargestellt.

Anmerkung: Wenn Sie nach der Änderung der Reihenfolge in der Datei `java.security` ein Fixpack für WebSphere Application Server implementieren, werden Ihre Änderungen überschrieben, und die Reihenfolge der Datei muss erneut geändert werden.

```
security.provider.1=com.ibm.crypto.provider.IBMJCE
security.provider.2=com.ibm.jsse2.IBMJSSEProvider2
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.security.jgss.IBMJGSSProvider
security.provider.5=com.ibm.security.cert.IBMCertPath
#security.provider.6=com.ibm.crypto.pkcs11.provider.IBMPKCS11
```

Starten Sie die WebSphere Partner Gateway-Server bcgconsole, bcgreceiver und bcgdocmgr erneut, nachdem Sie die Datei `java.security file` geändert haben.

Warnung über blockierte Threads beheben

Im Folgenden sehen Sie ein Beispiel für eine Nachricht, die Sie möglicherweise in der Datei `SystemOut.log` (`/opt/IBM/bcghub/wasND/Profiles/bcgdocmgr/logs/bcgdocmgr/SystemOut.log`) empfangen und die angibt, dass bestimmte Threads blockiert sind:

```
[7/19/06 14:35:16:839 EDT] 0000000f ThreadMonitor W   WSVR0605W:
Thread "WorkManager.BCGBPEWorkManager : 5" (00000055) has been active for
709464 milliseconds and may be hung. There is/are 15 thread(s) in total in
the server that may be hung.
```

Anmerkung: WebSphere Application Server zeigt möglicherweise die Warnung, dass einige der Threads eventuell blockiert sind. WebSphere Partner Gateway verarbeitet die Threads jedoch trotzdem.

Ändern Sie die folgende Eigenschaft in **Document Manager** > **Empfängerserver**, um diese Nachricht zu beheben:

```
com.ibm.websphere.threadmonitor.interval = 0
```

Dieser Wert befindet sich in **Angepasste Merkmale** unter **Serverinfrastruktur** > **Verwaltung**.

Document Manager-Ausnahmebedingung stoppen

Ignorieren Sie die folgende Ausnahmebedingung, wenn Sie sie beim Stoppen des Document Manager-Servers empfangen, während ein Dokument verarbeitet wird:

```
[2/1/07 14:04:40:546 EST] 00000088 ExceptionUtil E CNTR0020E:
EJB threw an unexpected (non-declared exception during invocation of method "onMessage"
on bean "BeanId(BCGBPE#ejb/bcgBpeEJB.jar#BPEMainEngineMDB, null)".
Exception data: javax.ejb.TransactionRolledbackLocalException:  ;
nested exception is: com.ibm.websphere.csi.CSITransactionRolledbackException:
```

```
  com.ibm.websphere.csi.CSITransactionRolledbackException:
   at com.ibm.ejs.csi.TranStrategy.commit(TranStrategy.java:742)
   at com.ibm.ejs.csi.TranStrategy.postInvoke(TranStrategy.java:181)
   at com.ibm.ejs.csi.NotSupported.postInvoke(NotSupported.java:99)
   at com.ibm.ejs.csi.TransactionControlImpl.postInvoke(TransactionControlImpl.java:581)
   at com.ibm.ejs.container.EJSContainer.postInvoke(EJSContainer.java:3876)
   at com.ibm.bcg.server.common.EJSLocalStatelessTransController_5c554616.onReceive(Unknown Source)
  at com.ibm.bcg.server.common.BaseMDB.onMessage(BaseMDB.java:194)
   at com.ibm.ejs.container.MessageEndpointHandler.invokeMdbMethod(MessageEndpointHandler.java:992)
  at com.ibm.ejs.container.MessageEndpointHandler.invoke(MessageEndpointHandler.java:725)
  at $Proxy0.onMessage(Unknown Source)
   at com.ibm.ws.sib.api.jmsra.impl.JmsJcaEndpointInvokerImpl.invokeEndpoint
         (JmsJcaEndpointInvokerImpl.java:201)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaDispatcher.dispatch(SibRaDispatcher.java:708)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaSingleProcessListener$SibRaWork.run
         (SibRaSingleProcessListener.java:584)
  at com.ibm.ejs.j2c.work.WorkProxy.run(WorkProxy.java:497)
      at com.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java:1469)
 javax.ejb.TransactionRolledbackLocalException:;
nested exception is: com.ibm.websphere.csi.CSITransactionRolledbackException:
   at com.ibm.ejs.csi.TranStrategy.commit(TranStrategy.java:742)
   at com.ibm.ejs.csi.TranStrategy.postInvoke(TranStrategy.java:181)
   at com.ibm.ejs.csi.NotSupported.postInvoke(NotSupported.java:99)
   at com.ibm.ejs.csi.TransactionControlImpl.postInvoke(TransactionControlImpl.java:581)
   at com.ibm.ejs.container.EJSContainer.postInvoke(EJSContainer.java:3876)
   at com.ibm.bcg.server.common.EJSLocalStatelessTransController_5c554616.onReceive(Unknown Source)
  at com.ibm.bcg.server.common.BaseMDB.onMessage(BaseMDB.java:194)
   at com.ibm.ejs.container.MessageEndpointHandler.invokeMdbMethod(MessageEndpointHandler.java:992)
  at com.ibm.ejs.container.MessageEndpointHandler.invoke(MessageEndpointHandler.java:725)
  at $Proxy0.onMessage(Unknown Source)
   at com.ibm.ws.sib.api.jmsra.impl.JmsJcaEndpointInvokerImpl.invokeEndpoint
         (JmsJcaEndpointInvokerImpl.java:201)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaDispatcher.dispatch(SibRaDispatcher.java:708)
  at com.ibm.ws.sib.ra.inbound.impl.SibRaSingleProcessListener$SibRaWork.run
         (SibRaSingleProcessListener.java:584)
  at com.ibm.ejs.j2c.work.WorkProxy.run(WorkProxy.java:497)
```

Obwohl Sie diese Ausnahmebedingung empfangen, sind alle folgenden Zielsetzungen erfüllt:

- Ordnungsgemäße Wiederherstellung
- Kein Dokumentverlust
- Keine Verarbeitung doppelter Dokumente
- Keine Leistungseinbußen nach einem Neustart
- Keine blockierten Dokumente

WebSphere MQ-Nachrichten beheben

In den folgenden Abschnitten wird beschrieben, wie bestimmte MQ-Nachrichten behoben werden können:

- „Fehler MQJMS2007"
- „Fehler MQJMS2013" auf Seite 203

Fehler MQJMS2007

Wenn Sie JMS als Gateway mit WebSphere MQ als Nachrichtenübertragungsservice verwenden, können Sie die folgende Nachricht empfangen, wenn Sie eine bestimmte Nachricht in eine Warteschlange stellen:

```
MQJMS2007: failed to send message to MQ queue.
```

Als Ergebnis kann der Connector keine Nachricht in die Ausgabewarteschlange schreiben. Die Ursache für den Fehler ist möglicherweise, dass das Attribut "Maxi-

mum message length" (maximale Nachrichtenlänge) für die Warteschlange, den Warteschlangenmanager oder Kanal nicht mit einem Wert festgelegt wurde, der größer gleich der umfangreichsten Nachrichtengröße ist.

Gehen Sie wie folgt vor, um das Nachrichtenlängenattribut für die Warteschlange, den Warteschlangenmanager und den Kanal zu ändern:

1. Wechseln Sie in den WebSphere MQ Explorer und dort zu den Eigenschaften des Warteschlangenmanagers.
2. Klicken Sie auf die erweiterte Registerkarte und setzen Sie den Wert des Attributs für die maximale Nachrichtenlänge auf einen Wert, der die Nachrichtengröße übersteigt.
3. Wechseln Sie zu den Eigenschaften des Kanals.
4. Klicken Sie auf die erweiterte Registerkarte und setzen Sie den Wert des Attributs für die maximale Nachrichtenlänge auf einen Wert, der die Nachrichtengröße übersteigt.
5. Wechseln Sie zu den Warteschlangeneigenschaften der Warteschlange, die angegeben wurde, während das Gateway erstellt wurde.
6. Klicken Sie auf die erweiterte Registerkarte und setzen Sie den Wert des Attributs für die maximale Nachrichtenlänge auf einen Wert, der die Nachrichtengröße übersteigt.

Fehler MQJMS2013

Während der Kommunikation von WebSphere Partner Gateway mit WebSphere MQ empfangen Sie eventuell den folgenden Fehler:

```
MQJMS2013 invalid security authentication
```

Führen Sie die folgenden Schritte aus, um diesen Fehler zu beheben:

1. Prüfen Sie, unter welcher Benutzer-ID die Anwendung ausgeführt wird.
2. Stellen Sie sicher, dass die verwendete Benutzer-ID in der Gruppe `mqm` (oder in einer anderen Gruppe mit den notwendigen Berechtigungen) vorhanden ist.
3. Wenn die Benutzer-ID sich nicht in der Gruppe `mqm` befindet, fügen Sie sie der Gruppe `mqm` hinzu, und geben Sie den Befehl `runmqsc REFRESH SECURITY(*)` aus.

Ausnahmebedingung java.security.InvalidKeyException: Unzulässige Schlüsselgröße oder unzulässiger Standardparameter

Wenn Sie versuchen, die Datei `PKCS#12` mit einer stärkeren als der standardmäßig unterstützten Verschlüsselung hochzuladen, oder wenn Sie einen Schlüssel in einer unzulässigen Schlüsselgröße verwenden, die standardmäßig nicht unterstützt wird, wird diese Ausnahmebedingung ausgelöst. Um dieses Problem zu beheben, müssen Sie sich die Richtliniendateien für die uneingeschränkte Verschlüsselungsstärke besorgen und installieren, sofern dies rechtlich zulässig ist. Weitere Informationen über das Ändern der Verschlüsselungsstärke finden Sie im Handbuch *WebSphere Partner Gateway Hubkonfiguration*.

MDN-Status für AS-Transaktionen 'unbekannt'

Nach Fertigstellung eines Upgrades auf WebSphere Partner Gateway Version 6.2 zeigt die AS-Anzeigefunktion in der Community Console für den MDN-Status bei AS-Transaktionen, die vor dem Upgrade erfolgten, einen unbekannten Status an. Es handelt sich um eine Einschränkung der Migrationsprozeduren und -dienstprogramme.

Nach Anwendung von Fixes werden Server nicht gestartet

Möglicherweise werden die Server von Document Manager, dem Knotenagenten und die Anwendungsserver nicht gestartet, wenn Sie kürzlich ein Fix oder ein Fixpack mit dem Aktualisierungsprogramm angewendet haben. Die Datei `SystemOut.log` enthält keine Informationen zu diesem Fehler. Die Datei `startServer.log` zeigt jedoch Folgendes:

```
ADMU3011E: Server launched but failed initialization. startServer.log,
SystemOut.log(or job log in zOS) and other log files under
/home/dwhare/WebSphere61/profiles/Dmgr01/logs/dmgr should contain
failure information.
```

Dieses Problem wird dadurch verursacht, dass ein Fix oder Fixpack als Benutzer "Root" angewendet wird, die WebSphere Application Server-Umgebung jedoch für die Ausführung durch einen Benutzer ohne Rootberechtigung eingerichet wurde.

Anmerkung: Bei vorhandenden Installationen ist der Installationsverantwortliche mit oder ohne Rootberechtigung, der der Eigner der derzeit installierten Dateien ist, der einzige Benutzer, der für die betreffende Installation weitere, nachfolgende Installationen oder Löschoperationen durchführen kann.

Der Grund für das fehlgeschlagene Starten der Server besteht darin, dass der OSGI-Cache wegen eines Berechtigungsproblems nach der Anwendung des Fixpacks nicht aktualisiert wurde. Prüfen Sie dies im Verzeichnis *<WAS_PROFILE_HOME>*`/configuration/` in einer Protokolldatei mit einer Zahlenzeichenfolge, deren Länge dem Dateinamen entspricht. Diese Datei enthält wahrscheinlich einen Fehler wie den folgenden:

```
!ENTRY org.eclipse.osgi 2006-08-24 09:04:14.597
!MESSAGE Error reading configuration:
/home/dwhare/WebSphere61/profiles/Dmgr01/configuration/org.eclipse.osgi/.manager
/.fileTableLock (Permission denied)
!STACK 0
java.io.FileNotFoundException:
/home/dwhare/WebSphere61/profiles/Dmgr01/configuration/org.eclipse.osgi/.manager
/.fileTableLock (Permission denied)
at java.io.FileOutputStream.openAppend(Native Method)
at java.io.FileOutputStream.<init>(FileOutputStream.java:203)
at org.eclipse.core.runtime.internal.adaptor.Locker_JavaNio.lock(Locker_JavaNio.java:34)
at org.eclipse.core.runtime.adaptor.FileManager.lock(FileManager.java:361)
at org.eclipse.core.runtime.adaptor.FileManager.open(FileManager.java:658)
at ...
```

Lösen Sie dieses Problem wie folgt:

1. Stoppen Sie alle verbliebenen WebSphere Application Server-Prozesse, die ausgeführt werden.
2. Ändern Sie die Dateiberechtigungen für die WebSphere-Installation wieder in Benutzer ohne Rootberechtigung.
3. Führen Sie *<WAS_HOME>*`/profiles/<profile>/bin/osgiCfgInit.sh` aus.

   Anmerkung: Führen Sie unter Windows den Befehl "osgiCfgInit.bat" aus. Starten Sie den Server.

Mit dem Befehl `osgiCfgInit` werden die Inhalte der Unterverzeichnisse in *<WAS_HOME>*`/configuration/` aktualisiert. Dieses Verzeichnis wird benutzt, um Daten in den JAR-Dateien unter *<WAS_HOME>*`/plugins/` zwischenzuspeichern.

Wenn die Daten in den JAR-Dateien aktualisiert werden (z. B. wenn ein Service-Pack installiert wird), müssen die zwischengespeicherten Daten aktualisiert wer-

den. Die Aktualisierung des Cachespeichers soll erfolgen, wenn ein Befehl das erste Mal in einem Profil abgesetzt wird, nachdem ein Service-Pack installiert wurde. (Beispiel: Befehl `startServer.sh`). Wenn jedoch eine Ausnahmebedingung wie obenstehend beschrieben auftritt, wird der Cachespeicher nicht aktualisiert, dies muss manuell erfolgen.

Ports für Direktaufruf von WebSphere Application Server korrigieren

Wenn in einem Windows-System die für den Direktaufruf verwendeten Ports nicht korrekt sind, wenn die Einträge im Startmenü verwendet werden, um die Administrationskonsole von WebSphere Application Server Network Deployment zu starten, müssen Sie die Ports ändern. Gehen Sie wie folgt vor, um die Ports zu ändern:

1. Wechseln Sie zu **Start** > **Programme** > **IBM WebSphere** > **Application Server Network Deployment Version 6.1** > **Profile** > **bcgprofile** > **Administrationskonsole**.
2. Klicken Sie mit der rechten Maustaste und wählen Sie die Eigenschaften aus, um die Werte für die Ports zu ändern.

Doppelte Dokumentzustellung bei mehreren Routern vermeiden

Wenn in einer UNIX-Umgebung große Volumen von Dokumenten verarbeitet werden (z. B. mehr als 100.000 Dokumente innerhalb von 24 Stunden) ist es möglich, dass ein Dokument zweimal an ein Gateway zugestellt wird.

Diese Duplizierung tritt auf, wenn mehrere Routerkomponenten vorhanden sind und das allgemeine Dateisystem unter einer UNIX-Umgebung installiert ist. Nehmen Sie die folgenden Attribute in die WebSphere-Variablen aller Routerkomponenten auf, um während der Verarbeitung großer Dokumentvolumen die doppelte Dokumentzustellung zu vermeiden:

1. bcg.dm.checkFileLatency=true.
2. bcg.dm.latencyWaitTime=3000.

Überschriften von Registerkarten auf Bildschirmen mit höherer Auflösung als 1024 darstellen

Die Community Console zeigt auf Bildschirmen, bei denen der Wert für die Auflösungsbreite größer als 1024 Pixel ist, die Überschriften von Registerkarten möglicherweise verzerrt an, wie z. B. bei der Anzeige **Dokumentdetails**.

Dieses Verhalten können Sie ignorieren.

Dokumente werden bei Verwendung von Oracle 9i Release 2 nicht verarbeitet

Wenn Sie Oracle 9i Release 2 verwenden, stellen Sie möglicherweise fest, dass Dokumente nicht verarbeitet werden und dass die Protokolle der Messaging-Steuerkomponente `BCGMAS` den folgenden Fehler enthalten:

```
J2CA0056I: The Connection Manager received a fatal connection error from the
Resource Adapter for resource datasources/bcgMASDS The exception received is
com.ibm.websphere.ce.cm.StaleConnectionException: No more data to read from socket:
java.sql.SQLException: No more data to read from socket.
```

Installieren Sie zur Lösung dieses Problems die Oracle-Version 10g auf dem JDBC-Treiber. Dies Treiber behebt bekannte Inkompatibilitäten zwischen Oracle 9i und der Messaging-Steuerkomponente von WebSphere Application Server.

Weitere Details finden Sie in den IBM Technischen Hinweisen für diese Ausgabe. Die IBM Technischen Hinweise finden Sie unter folgender Adresse:

1. Wechseln Sie zu http://www.ibm.com/support/us/.
2. Geben Sie im Suchfeld die Nummer 1239781 ein.
3. Wählen Sie in der Suchergebnisliste **Oracle 9i Thin driver running in cognizance with Service Integration Bus and Scheduler Service can result in J2C Connection Pool Exhaustion** aus.

Den JDBC-Treiber für Oracle 10g können Sie von der Oracle-Website unter http://www.oracle.com/technology/software/tech/java/sqlj_jdbc/index.html herunterladen.

Dokumentverarbeitung bei einem Ausfall der Datenbank

Fällt die Datenbank aus, während WebSphere Partner Gateway Dokumente verarbeitet, behalten die Dokumente den Status 'inprocess' bei und blockieren, und die Nachrichten werden in die Fehlerwarteschlange "datalogerrorQ" versetzt. Ist die Datenbank wieder aktiv, müssen Sie die Batchdatei **reprocessDbLoggingErrors.bat** (im Verzeichnis WPG_HOME/bin) ausführen, um die Nachrichten aus der Warteschlange "datalogerrorQ" zu versetzen und mit der Verarbeitung der Dokumente fortzufahren.

Fehler "java.lang.NoClassDefFoundError" bei Ausführung von "reprocessDbLoggingErrors.bat"

Der Fehler "java.lang.NoClassDefFoundError" kann aus dem folgenden Grund auftreten: Die Datei "reprocessDbLoggingErrors.bat" verwendet den Pfad zur Datei "ws_runtime.jar", die sich im folgenden Verzeichnis befindet:

```
<WAS_HOME>\deploytool\itp\plugins\com.ibm.websphere.v61_6.1.0.
```

Nach jedem Release eines Fixpacks wird jedoch der Name des Ordners "com.ibm-.websphere.v61_6.1.0" geändert, um die entsprechende Version des Fixpacks widerzuspiegeln. Daher kann die Batchdatei die Datei "ws_runtime.jar" nicht finden. Um diesen Fehler zu beheben, müssen Sie den Pfad für die Datei "ws_runtime.jar" festlegen. Gehen Sie hierzu wie folgt vor:

1. Wechseln Sie in das folgende Verzeichnis:
   ```
   <WAS_HOME>\deploytool\itp\plugins
   ```
2. Prüfen Sie den Pfad für "ws_runtime.jar".
3. Wechseln Sie in das folgende Verzeichnis:
   ```
   <WAS_HOME>\bin
   ```
4. Bearbeiten Sie das Dateiverzeichnis in der Datei **reprocessDbLoggingErrors.bat**.
5. Legen Sie den korrekten Pfad für die Datei "ws_runtime.jar" fest und führen Sie das Script erneut aus.

Wiederherstellungsprozess, wenn die Warteschlange oder Platte voll oder nicht verfügbar ist

Wenn das Nachrichtenübermittlungssystem oder das gemeinsame Dateisystem während der Verarbeitung voll oder nicht verfügbar ist, wird das Geschäftsdokumentobjekt (Business Document Object - BDO) vorübergehend im folgenden temporären Ordner des Empfängercomputers gespeichert: `WPG_HUB_INSTALL_HOME\Receiver\temp`. Tritt dieser Fall auf, löst der Hub das Ereignis 103205 mit der folgenden Beschreibung aus:

```
Receiver Processing halted, due to following reason failed to process target:
With Queue and File system unavailable/Full. Please make sure queue and disk
system are available for processing and start the receiver.
(Empfängerverarbeitung wurde gestoppt, da sie das Ziel aus dem folgenden Grund
nicht verarbeiten konnte: Warteschlange oder Dateisystem sind nicht verfügbar
oder voll. Stellen Sie sicher, dass die Warteschlange und das Plattensystem für
die Verarbeitung verfügbar sind, und starten Sie den Empfänger.)
```

Gehen Sie wie folgt vor, wenn eine Nachricht wie die oben beschriebene ausgegeben wird:

1. Stellen Sie sicher, dass die Warteschlange und die Platte für das gemeinsame Dateisystem für die Verarbeitung zur Verfügung stehen.
2. Starten Sie den Empfängerserver erneut.
3. Versetzen Sie das Geschäftsdokumentobjekt (BDO), das im temporären Ordner des Empfängers gespeichert wurde, in den Ordner **router_in** des gemeinsamen Dateisystems (d. h. des Hubs).

Laufzeitfehler im Workflow-Handler

Bei der Dokumentverarbeitung kann ein Fehler auftreten, und in der Dokumentanzeige wird die Nachricht 'Laufzeitfehler im Workflow-Handler' angezeigt. Prüfen Sie in diesem Fall, ob die WebSphere-Datei 'SystemErr.log' die folgenden Fehler enthält:

- Fehler 'java.net.ConnectException':

  Mögliche Lösung: Wenn Sie den WebSphere Transformation Extender-RMI-Server verwenden, müssen Sie sicherstellen, dass der Server aktiv ist und auf den in der Ausnahmebedingung genannten Hostnamen und Port zugreifen kann.
- Ausnahmebedingung 'com.ibm.websphere.dtx.dtxpi.rmi.MRmiApiException': Unknown error - Loading map failed - Native function: CMpiMapSet::CMpiMapSet:

  Mögliche Lösungen:
  - Stellen sie sicher, dass die Architektur von WebSphere Application Server ND und WebSphere Transformation Extender übereinstimmt. Wenn Sie beispielsweise die 32-Bit-Architektur von WebSphere Application Server ND verwenden, muss auch die 32-Bit-Architektur von WebSphere Transformation Extender installiert sein.
  - Stellen Sie sicher, dass das Systemverwaltungsattribut 'bcg.wtx.mapLocation' für WebSphere Transformation Extender korrekt konfiguriert ist und auf das Verzeichnis verweist, das die WebSphere Transformation Extender-Zuordnungen enthält.
  - Wenn Sie den WebSphere Transformation Extender-RMI-Server verwenden, müssen Sie sicherstellen, dass der Server auf das Verzeichnis zugreifen kann, das die WebSphere Transformation Extender-Zuordnung enthält.

Fehler beim Aufrufen der WebSphere Transformation Extender-Zuordnung

Wird beim Aufrufen der WebSphere Transformation Extender-Zuordnung der Fehler 'java.lang.NoClassDefFoundError' im WebSphere-Protokoll 'SystemOut.log' ausgegeben, müssen Sie sicherstellen, dass die Datei 'dtxpi.jar' für WebSphere Transformation Extender im Verzeichnis 'router/lib.userexits' installiert ist.

Plugin für IBM Support Assistant (ISA)

WebSphere Partner Gateway unterstützt IBM Support Assistant (ISA). Das ISA-Plugin für WebSphere Partner Gateway stellt Funktionen wie beispielsweise die Protokollerfassung für PMRs (Problem Management Reports) oder das Durchsuchen produktspezifischer Informationen bereit. Mit dem Tool ISA können Kunden die zum Analysieren eines Problems und zum Verwalten von Serviceanforderungen erforderlichen Informationen finden. Weitere Informationen zum ISA-Produktplugin für WebSphere Partner Gateway finden Sie unter http://www-01.ibm.com/software/integration/wspartnergateway. Weitere Informationen zu ISA finden Sie unter http://www.ibm.com/software/support/isa.

Mit ISA können Kunden Protokolle, Tracedateien und weitere Konfigurationsinformationen zusammenstellen, die von den Spezialisten der IBM Unterstützungsfunktion angefordert werden. Diese Informationen helfen der IBM Unterstützungsfunktion dabei, die zum schnelleren Analysieren und Beheben von PMRs des Kunden erforderlichen Informationen zu erfassen.

Dienstprogramm für die Partnermigration mit LDAP

Wenn LDAP für das Dienstprogramm für die Partnermigration in WebSphere Partner Gateway aktiviert ist, tritt ein Fehler auf, der besagt, dass der Benutzer nicht über ausreichende Berechtigungen verfügt.

Anmerkung: Der LDAP-Benutzer, der diese Operation ausführt, muss Mitglied der Hubadministratorgruppe sein.

1. Wählen Sie **Systemverwaltung** > **Gemeinsame Eigenschaften** aus.
2. Ändern Sie die Eigenschaft **bcg.ldap.containerauth** in *False*.
3. Melden Sie sich mit denselben Berechtigungsnachweisen, die Sie ohne LDAP verwendet haben, an der Konsole an.
4. Wählen Sie **Kontenadmin** > **Benutzer** aus und erstellen Sie einen Benutzer.
5. Führen Sie den LDAP-Benutzer nur zur Hubadministratorgruppe hinzu.
6. Wählen Sie **Systemverwaltung** > **Gemeinsame Eigenschaften** aus und setzen Sie die Eigenschaft **bcg.ldap.containerauth** auf *True*.
7. Melden Sie sich ab und melden Sie sich erneut an.

AS-Signaturfehler für den Inhaltstyp "interop"

Auf der Seite **Systemverwaltung** > **Gemeinsame Attribute** der Konsole kann die Eigenschaft **excludedContentTypesForCanonicalization** bearbeitet werden.

Beim Ausführen von AS2-Transaktionen enthält dieses Attribut alle Inhaltstypen, die von der Kanonisierung ausgeschlossen sind.

Um diesen Fehler zu beheben, müssen Sie den Inhaltstyp **application/pkcs7- mime** zur Eigenschaft **excludedContentTypesForCanonicalization** hinzufügen. Dies gilt nur für AS2-Transaktionen, da für RNIF-Transaktionen keine Unterstützung für die Kanonisierung bereitgestellt wird.

Einschränkung: Diese Eigenschaft **excludedContentTypesForCanonicalization** kann vom Hubadministrator oder von einem beliebigen Benutzer, der Mitglied der Hubadministratorgruppe (hubadmin) ist, geändert werden.

Hinweis: Starten Sie den Server neu, damit die Änderungen wirksam werden.

Anhang A - Empfehlungen zur Leistungsoptimierung

Dieser Anhang enthält Informationen zur Optimierung der Leistung in Ihrer jeweiligen Umgebung.

Warteschlangenüberlauf verwalten

Die Komponenten von WebSphere Partner Gateway verwenden eine JMS-Warteschlange, um sich gegenseitig asynchron aufzurufen. Wenn jedoch die Eingangsrate von Nachrichten in einer Warteschlange größer ist als die Verarbeitungsrate dieser Nachrichten, wird in der Warteschlange die maximal mögliche Anzahl an Nachrichten erreicht. Sobald die Länge der Warteschlange die für die Warteschlange konfigurierte maximale Länge erreicht hat, läuft die Warteschlange über. WebSphere Partner Gateway bietet einen Mechanismus, mit dem die eingehenden Dokumente oder Nachrichten für den Fall einer Warteschlangenüberlaufsituation trotzdem im Dateisystem bestehen bleiben können.

Anmerkung: Die maximale Länge der Warteschlange wird möglicherweise während Spitzenbelastungen oder während der Verarbeitung umfangreicher Dokumente erreicht. Überwachen Sie die Warteschlangen in solchen Zeiten, um sicherzustellen, dass die Warteschlangenlänge ausreichend ist, um einen Überlauf zu vermeiden.

In „Anhang C - Komponentenspezifische Systemattribute" auf Seite 253 finden Sie eine Liste der Attribute, mit denen der Warteschlangenüberlauf verwaltet werden kann.

Zusammenfassungsdaten generieren

WebSphere Partner Gateway fasst regelmäßig Daten über die Systemaktivität zusammen. Die Daten dieses Zusammenfassungsservices sind die Informationen, die Sie sehen, wenn Sie die Funktionen für Dokumentanalyseberichte oder Dokumentvolumenberichte verwenden.

Im Fenster **Merkmale für Zusammenfassungsservice** können Sie die Zusammenfassungsdaten anzeigen und festlegen, wie oft diese generiert werden sollen. In diesem Fenster finden Sie außerdem Datum und Uhrzeit der letzten Aktualisierung der Zusammenfassungsdaten.

Gehen Sie wie folgt vor, um das Zeitintervall zu ändern, in dem die Zusammenfassungsdaten generiert werden:

1. Klicken Sie auf **Systemverwaltung** > **DocMgr-Verwaltung** > **Andere** > **Zusammenfassungsengine**. In der Community Console wird das Fenster **Merkmale für Zusammenfassungsservice** geöffnet.
2. Klicken Sie auf das Symbol **Bearbeiten** neben **Verarbeitungsintervall (in Minuten)**.
3. Geben Sie einen Wert (zwischen 1 und 60) für die Anzahl der Minuten an, nach deren Ablauf die Daten erneut zusammengefasst werden sollen. Der Standardwert ist 15.
4. Klicken Sie auf **Speichern**.

Anahng B - Fehlgeschlagene Ereignisse

Wenn die Verarbeitung eines Dokuments fehlschlägt, generiert das WebSphere Partner Gateway-System ein Ereignis. Tabelle 43 enthält eine Auflistung der WebSphere Partner Gateway-Fehlerereignisse und ihrer zugehörigen Beschreibung. Tabelle 44 auf Seite 226 enthält eine Liste von Ereignissen, die von den EDI-Komponenten generiert werden können.

Anmerkung: Die HTTP-Empfängerkomponente gibt einen HTTP-Fehlercode zurück, wenn das Dokument nicht gespeichert werden kann. Bei allen anderen Empfängerkomponententypen wird der Dokumentinhalt zum Zeitpunkt des Fehlschlagens an der aktuellen Position gespeichert.

Tabelle 43. Fehlerereignisse

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG103001	Datenbankfehler	Datenbankfehler: {0} fehlgeschlagen in {1} mit Ausnahmebedingung {3}.	Kritisch	
BCG103101	Cache-Engine-Fehler	Cache-Engine-InstanceId {0} auf Host {1} wurde nicht initialisiert. Beheben Sie den Fehler, und starten Sie den Service erneut. Fehlerursache: {2}.	Kritisch	
BCG103201	Fehler in Hubeigner-Statusengine	Fehlerursache:{0}.	Fehler	Dieses Ereignis wird generiert, wenn ein nicht behebbarer Systemfehler auftritt, durch den die Verarbeitung eines Dokuments fehlschlägt. Beispiel: Ein Fehler beim Schreiben in die Datenbank.
BCG103203	Empfängerverarbeitungsfehler	Empfänger '{0},{1}' konnte Dokument nicht verarbeiten, Fehler: {2}.	Fehler	Dieses Ereignis wird generiert, wenn die Empfängerkomponente ein Dokument auf Grund von Dokument- oder Systemfehlern nicht verarbeiten kann.
BCG103205	Empfängerfehler	Empfänger '{0},{1}' konnte das Ziel nicht verarbeiten: {2}.	Fehler	
BCG106004	Kein Standardzielpaar	Verbindungserstellung fehlgeschlagen. Es ist kein Standardzielpaar zwischen den Partnern {0} und {1} vorhanden.	Fehler	

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG106005	Keine Aktion gefunden	Es konnte keine Verbindung für die B2B-Funktion erstellt werden, weil der Interaktion keine Aktionen zugeordnet sind.	Fehler	
BCG106600	Fehler beim Erstellen der Dokumentdefinition	Untergeordnete Ebene = {0} höher oder gleich übergeordneter Ebene = {1}.	Fehler	
BCG111001	Fehler beim Erstellen eines FTP-Kontos	FTP-Kontoerstellung für Partner {0} fehlgeschlagen. Fehlernachricht: {1}.	Fehler	
BCG112002	Verzeichnis konnte nicht erstellt werden	Verzeichnis konnte nicht erstellt werden: {0}.	Fehler	
BCG112002	Dokumentstammverzeichnis ist vorhanden	Dokumentstammverzeichnis {0} ist bereits vorhanden.	Fehler	
BCG200000	Kein Standardzielpaar	Verbindungserstellung fehlgeschlagen. Es ist kein Standardzielpaar zwischen den Partnern {0} und {1} vorhanden.	Fehler	
BCG200001	Abrufen des Geschäftsprozesses zur Protokollumsetzung fehlgeschlagen	Factory konnte keine Instanz des Geschäftsprozesses für Protokollumsetzung abrufen. Ursache: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn bei dem Versuch, eine Instanz des Geschäftsprozesses für Protokollumsetzung zu suchen, ein Systemausfall auftritt.
BCG200005	Dokumentumsetzungsfehler	Dokumentumsetzung fehlgeschlagen. Ursache: {0}.	Fehler	Dieses Ereignis wird auf Grund eines Fehlers während der Dokumentumsetzung generiert.
BCG200006	Fehler bei Eingabedatei für Protokollumsetzung	Fehler bei der Eingabedatei für Protokollumsetzung: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn in der Eingabedatei ein Fehler bei der Aktionsverarbeitung auftritt, z. B. wenn die Datei beschädigt ist.
BCG200007	Fehler bei Ausgabedatei für Protokollumsetzung	Fehler bei der Ausgabedatei für Protokollumsetzung: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn beim Schreiben in das Verzeichnis der Ausgabedatei ein Fehler auftritt.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG200009	Parsing des Dokuments fehlgeschlagen	Parsing fehlgeschlagen: {0}.	Fehler	Dieses Ereignis wird auf Grund eines Fehlers während des Parsings eines Dokuments generiert.
BCG200013	Fehler bei der vom internen Partner bereitgestellten RN-Prozessinstanz-ID	{0}.	Fehler	Dieses Ereignis wird generiert, wenn eine nicht verwendbare Prozessinstanz-ID empfangen wird und das Konfigurationsmerkmal angibt, dass das System keine neue Prozessinstanz-ID generieren wird.
BCG200015	Fehler bei dem vom internen Partner bereitgestellten RosettaNet-GlobalUsageCode	{0}.	Fehler	Dieses Ereignis wird generiert, wenn der x-aux-production-Headerwert nicht verwendbar ist und das Konfigurationsmerkmal angibt, dass das System bei einem Fehler nicht den Standardwert verwendet.
BCG210000	Kanalprüffehler	Kanalprüffehler	Fehler	Dieses Ereignis wird generiert, wenn ein Fehler bei der Kanalprüfung auftritt.
BCG210001	Kanalprüffehler	Kanalprüffehler	Fehler	Dieses Ereignis wird generiert, wenn die erforderlichen Daten zum Suchen einer Verbindung verfügbar sind, die entsprechende Verbindung aber nicht gefunden werden kann.
BCG210002	Verbindungssuchfunktion fehlgeschlagen	Verbindungssuchfunktion fehlgeschlagen: {0}.	Fehler	Dieses Ereignis wird generiert, wenn die erforderlichen Daten zum Suchen einer Verbindung nicht verfügbar sind.
BCG210007	Ausgehendes Dokument kann nicht gepackt werden	Fehler in Ausgangsprozessor.	Kritisch	Dieses Ereignis wird generiert, wenn für ein ausgehendes Dokument kein Packprogramm verfügbar ist.
BCG210008	Fehler bei der IP-Adressvalidierung	Die IP-Adresse des Absenders befindet sich nicht im Partnerprofil {0}.	Fehler	Dieses Ereignis wird generiert, wenn ein Dokument von einer für den Partner nicht genehmigten IP-Adresse gesendet wird.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG210009	Fehler bei der SSL-Zertifikatvalidierung	Der Name des Client-SSL-Zertifikats befindet sich nicht im Partnerprofil {0}.	Fehler	Dieses Ereignis wird generiert, wenn das SSL-Zertifikat, mit dem das Dokument gesendet wird, nicht in der Liste der für diesen Partner genehmigten Zertifikate enthalten ist.
BCG210010	Dokument zu groß	Dokument ist zu groß: {0} Byte.	Fehler	Dieses Ereignis wird generiert, wenn das empfangene Dokument für die Verarbeitung zu groß ist.
BCG210011	Fehler beim Entpacken durch den Transport des internen Partners	Nicht genügend Transportinformationen für den internen Partner angegeben: {0}.	Fehler	Dieses Ereignis wird generiert, wenn nicht ausreichende Transportinformationen angegeben wurden.
BCG210012	B2B-Funktion nicht gefunden	B2B-Funktion nicht gefunden: {0}.	Fehler	Dieses Ereignis wird generiert, wenn die erforderliche B2B-Funktion zum Weiterleiten des Dokuments nicht aktiviert ist.
BCG210013	Verbindung nicht vollständig konfiguriert	Verbindung ist nicht vollständig konfiguriert {0}.	Fehler	Dieses Ereignis wird generiert, wenn die Verbindung für das Dokument nicht vollständig konfiguriert wurde. Höchstwahrscheinlich verfügt die Zieladresse des Dokuments nicht über ein konfiguriertes Ziel.
BCG210014	Fehler bei Entpacken eines mehrteiligen MIME-Dokuments	Ein mehrteiliges MIME-Dokument konnte nicht entpackt werden: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das System ein mehrteiliges MIME-Dokument nicht entpacken konnte.
BCG210015	cXML-Packungsfehler	Ein cXML-Dokument konnte nicht verpackt werden: {0}.	Fehler	
BCG210016	cXML-Kanal-parsingfehler	cXML-Route-Informationen konnten nicht analysiert werden: {0}.	Fehler	
BCG210017	EDI-Verbindungs-parsingfehler	EDI-Route-Informationen konnten nicht analysiert werden: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das System EDI-Route-Informationen nicht analysieren konnte.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG210019	Synchronbetrieb über diese Verbindung nicht unterstützt	Synchronbetrieb über diese Verbindung nicht unterstützt.	Fehler	Dieses Ereignis wird generiert, wenn das Dokument Synchronbetrieb erfordert, die Verbindung den Synchronbetrieb jedoch nicht unterstützt.
BCG210031	Dokument kann nicht als unbestreitbares Dokument (Non-Rep) behandelt werden	Dokument kann nicht als unbestreitbares Dokument (Non-Rep) behandelt werden: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System das Dokument nicht als unbestreitbares Dokument behandeln kann. Stellen Sie sicher, dass das System über ausreichenden Plattenspeicherplatz verfügt, und dass die folgenden Verzeichnisse nur vom System erstellte Dateien enthalten: • `/<allgem_infoverz>/non_rep/` • `/<allgem_infoverz>/msg_store/` Wenn diese beiden Verzeichnisse benutzergenerierte Dateien enthalten, schlägt die Verarbeitung des Dokuments fehl.
BCG210032	Systemfehler im Eingangsprozessor	Systemfehler im Eingangsprozessor für Dokument: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System einen Fehler im Eingangsprozessor findet.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG210033	Nachrichten-speicherung fehlgeschlagen	Einfacher Dokumenttext kann nicht gespeichert werden.	Fehler	Dieses Ereignis wird generiert, wenn das System das Dokument nicht als einfachen Dokumenttext speichern kann. Stellen Sie sicher, dass das System über ausreichenden Plattenspeicherplatz verfügt, und dass die folgenden Verzeichnisse nur vom System erstellte Dateien enthalten: • /<*allgem_infoverz*>/non_rep/ • /<*allgem_infoverz*>/msg_store/ Wenn diese beiden Verzeichnisse benutzergenerierte Dateien enthalten, schlägt die Verarbeitung des Dokuments fehl.
BCG210034	Systemfehler in Document Manager	Systemfehler in Document Manager für Dokument: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System einen Fehler in Document Manager findet.
BCG210051	Duplikatverarbeitungsfehler	Systemfehler — Fehler im Duplikatprozess.	Kritisch	Dieses Ereignis wird generiert, wenn das System während des Duplikatprozesses keine Verbindung mit dem Datenbankserver herstellen kann.
BCG210052	Doppeltes Dokument empfangen	Dieses Dokument scheint ein Duplikat eines am {2} gesendeten Dokuments zu sein.	Fehler	Dieses Ereignis wird generiert, wenn ein empfangenes Dokument ein Duplikat ist und zurückgewiesen wird.
BCG210061	Zielparsingfehler	Fehler in Bestimmungsparsing.	Kritisch	Dieses Ereignis wird generiert, wenn das Bestimmungsparsing fehlschlägt. Ursache hierfür ist normalerweise ein Datenbankproblem.
BCG210063	Zielprozessfehler	Zielprozess fehlgeschlagen.	Kritisch	Dieses Ereignis wird generiert, wenn die Verarbeitung des Ziels fehlschlägt. Ursache hierfür ist normalerweise ein Datenbankproblem.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG210065	Zielermittlungsfehler	{0}.	Fehler	Dieses Ereignis wird generiert, wenn bei der Verarbeitung des Ziels einander widersprechende Eingaben vorhanden sind.
BCG210066	Paket- und Inhaltsgeschäfts-IDs sind verschiedenen Partnern zugeordnet	Absenderpartner-ID = {0}, Empfängerpartner-ID = {1}, Absenderpaket-Partner-ID = {2}, Empfängerpaket-Partner-ID = {3}.	Fehler	Dieses Ereignis wird generiert, wenn zwischen den Route-Informationen von Inhalt und Paket eine Abweichung besteht.
BCG210201	Fehler beim Laden des PIP während der DOCTYPE-Verarbeitung	Der PIP für ein Dokument kann bei der DOCTYPE-Verarbeitung nicht geladen werden.	Kritisch	Dieses Ereignis wird generiert, wenn für den PIP keine Spezifikation gefunden werden kann. Dieses Ereignis dürfte lediglich auftreten, wenn Konfigurationsprobleme bestehen.
BCG210202	Ausnahmebedingung in der DOCTYPE-Verarbeitung	Ausnahmebedingung bei der DOCTYPE-Verarbeitung: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System bei dem Versuch fehlschlägt, den DOCTYPE-Tag einzufügen.
BCG210203	DoctypeProcess-Fehler — Keine Aktion gefunden	DoctypeProcess-Fehler — Keine Aktion gefunden.	Kritisch	Dieses Ereignis wird generiert, wenn für den Dokumenttyp PIP keine Spezifikation gefunden werden kann.
BCG210205	Verarbeitung des Dokuments wurde abgebrochen	Verarbeitung des Dokuments wurde abgebrochen. Grund: Die Verarbeitung eines oder mehrerer Dokumente ist fehlgeschlagen.	Kritisch	Dieses Ereignis wird generiert, wenn die Dokumentverarbeitung abgebrochen wird, weil für das Attribut "Umschlag bei Fehlern löschen" der Wert "Ja" angegeben ist.
BCG230004	Interner Validierungsfehler	{0}.	Kritisch	Dieses Ereignis wird auf Grund eines internen Systemfehlers während der Durchführung der Validierung generiert.
BCG230006	Datenbankvalidierungsfehler	{0}.	Kritisch	Dieses Ereignis wird auf Grund eines Datenbankfehlers während der Validierungsverarbeitung generiert.
BCG230007	Validierungsfehler in Geschäftsprozessfactory	{0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System den Prozess nicht ermitteln kann, der an die Validierungsengine gesendet werden soll.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG230009	RosettaNet-Validierungsfehler	{0}.	Fehler	Dieses Ereignis wird generiert, wenn ein Dokument die RosettaNet-Prozessvalidierung nicht besteht.
BCG230010	Datenvalidierungsfehler	Dokument hat die Datenvalidierung nicht bestanden: {0}.	Fehler	Dieses Ereignis wird generiert, wenn ein Dokument die Datenvalidierung nicht besteht und zurückgewiesen wird.
BCG230012	AS-Folgevalidierungsfehler	{0}.	Fehler	Dieses Ereignis wird generiert, wenn ein Dokument die EDIINT-Prozessvalidierung nicht besteht.
BCG240003	RosettaNet-Entpackungsfehler	RosettaNet-Entpackungsfehler.	Fehler	Dieses Ereignis wird generiert, wenn das System während des Entpackens die RosettaNet-Präambel nicht analysieren kann.
BCG240005	Fehler des Parsers für RNPackager-Delivery-Header	Fehler in Parser für Delivery-Header: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das System während des Entpackens RosettaNet-Delivery-Header nicht analysieren kann.
BCG240007	RNPackager-Service-Header-Fehler	Fehler in Parser für Service-Header: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das System während des Entpackens RosettaNet-Service-Header nicht analysieren kann.
BCG240009	Fehler beim RNPackager-MIME-Parsing	MIME-Parsingfehler: {0}.	Fehler	Dieses Ereignis wird generiert, wenn während des Entpackens ein Mime-Parsingfehler bei der RosettaNet-Nachricht auftritt.
BCG240011	RNPackager-Signatur fehlgeschlagen	Validierung der digitalen Signatur fehlgeschlagen: {0}.	Fehler	Dieses Ereignis wird generiert, wenn die Validierung der digitalen Signatur während des Entpackens fehlschlägt.
BCG240012	Fehler beim Aktualisieren des RN-Entpackstatus	Datenbankzugriffsfehler: Der RosettaNet-Status konnte nicht aktualisiert werden.	Kritisch	Dieses Ereignis wird generiert, wenn das Entpackprogramm einen Datenbankkommunikationsfehler feststellt, während der RosettaNet-Status aktualisiert wird.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG240013	Partnerzertifikat stimmt nicht mit Unterzeichner überein	Name/Seriennummer auf Unterzeichnerzertifikat stimmte nicht mit Datenbankeintrag überein.	Fehler	Dieses Ereignis wird generiert, wenn die DUNS-Überprüfung des Zertifikats bei der digitalen Signatur fehlschlägt.
BCG240014	Fehlende Signatur in Dokument	Signatur im Dokument nicht gefunden.	Fehler	Dieses Ereignis wird generiert, wenn eine Signatur vom TPA gefordert, im Dokument aber nicht gefunden wird.
BCG240015	Fehler bei RosettaNet-Dokumenterstellung	{0}.	Kritisch	Dieses Ereignis wird generiert, wenn der Versuch, ein RosettaNet-Dokument zu erstellen, fehlschlägt.
BCG240016	Fehler in der RosettaNet-Unbestreitbarkeit	{0}.	Fehler	Dieses Ereignis wird generiert, wenn die Empfangsbestätigung keinen korrekten Auszug der vorherigen Nachricht enthält oder der Auszug fehlt.
BCG240017	Synchrone Empfangsbestätigung nicht empfangen	Synchrone Empfangsbestätigung ist erforderlich, wurde jedoch in der synchronen Antwort nicht empfangen.	Fehler	
BCG240025	Ausnahmebedingung bei der Initialisierung von WBIC Security Manager	Initialisierung von WBIC Security Manager ist fehlgeschlagen. Ausnahmebedingung: {1}.	Kritisch	
BCG240026	Das Zertifikat ist noch nicht gültig	Das Zertifikat ist noch nicht gültig. Seriennummer: {0}, registrierter Name des Zertifikatinhabers: {1}, registrierter Name des Zertifikatausstellers: {2}.	Kritisch	
BCG240027	Das Zertifikat ist abgelaufen	Das Zertifikat ist abgelaufen. Seriennummer: {0}, registrierter Name des Zertifikatinhabers: {1}, registrierter Name des Zertifikatausstellers: {2}.	Kritisch	
BCG240028	Das Zertifikat wurde widerrufen	Das Zertifikat wurde widerrufen. Seriennummer: {0}, registrierter Name des Zertifikatinhabers: {1}, registrierter Name des Zertifikatausstellers: {2}.	Kritisch	

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG240029	Das Zertifikat konnte nicht gefunden werden	Das Zertifikat konnte nicht gefunden werden.	Kritisch	
BCG240030	Kein gültiges Signaturzertifikat gefunden	Kein gültiges Signaturzertifikat gefunden.	Kritisch	
BCG240031	Packinstanzfehler	Fehler: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System kein Packprogramm für den gelieferten Dokumenttyp findet.
BCG240032	Kein gültiges Verschlüsselungszertifikat gefunden	Kein gültiges Verschlüsselungszertifikat gefunden.	Kritisch	Dieses Ereignis wird generiert, wenn kein gültiges Zertifikat gefunden werden kann. Wird dieses Ereignis ausgegeben, ist weder das primäre noch das sekundäre Zertifikat gültig. Die Zertifikate sind möglicherweise abgelaufen oder sie wurden widerrufen. Sind die Zertifikate abgelaufen oder wurden sie widerrufen, wird das entsprechende Ereignis (Zertifikat widerrufen oder abgelaufen) in der Ereignisanzeige ausgegeben.
BCG240033	Kein gültiges SSL-Clientzertifikat gefunden	Kein gültiges SSL-Clientzertifikat gefunden.	Kritisch	
BCG240036	Entpackinstanzfehler	Fehler: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das System kein Entpackprogramm für ein Dokument finden kann.
BCG240065	Verbindungsparsingfehler für XML-Nachricht	XML-Verbindungsparsing fehlgeschlagen: {0}.	Fehler	Dieses Ereignis wird generiert, wenn für eine XML-Nachricht keine Verbindungsinformationen gefunden werden können.
BCG240068	Verbindungsparserfehler in RosettaNet-Dokument	Verbindungsparsing für RosettaNet fehlgeschlagen.	Fehler	Dieses Ereignis wird generiert, wenn in einem RosettaNet-Dokument keine Verbindungsinformationen gefunden werden können.
BCG240070	Verbindungsparsingfehler für XML-Datei	XML-Verbindungsparsing fehlgeschlagen.	Fehler	Dieses Ereignis wird generiert, wenn das System keine Verbindungsinformationen für eine XML-Datei finden kann.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG240071	Verbindungsparsing-fehler für Flachdatei	Flachdateiverbindungs-parsing fehlgeschlagen: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das System keine Verbindungsinformationen für eine Flachdatei finden kann.
BCG240078	Verbindungsparsing für Web-Service fehlgeschlagen	Verbindungsparsing für Web-Service fehlgeschlagen.	Fehler	Dieses Ereignis wird generiert, wenn das System keine Verbindungsinformationen für eine SOAP-Nachricht finden kann.
BCG240409	AS-Entpack-programmfehler	AS-Entpackprogramm-fehler: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das AS-Entpackprogramm fehlschlägt.
BCG240411	AS-Signaturfehler	AS-Signaturvalidierungs-fehler: {0}.	Fehler	Dieses Ereignis wird generiert, wenn die AS-Signaturvalidierung fehlschlägt.
BCG240412	DB-Fehler in AS-Statusengine	AS-Statusenginefehler für DB: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn die AS-Statusenginedatenbank fehlschlägt.
BCG240415	AS-Packprogramm-fehler	AS-Packprogrammfehler: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn das AS-Packprogramm fehlschlägt.
BCG240416	Fehler in der AS-Unbestreitbarkeit	{0}.	Fehler	Dieses Ereignis wird generiert, wenn die AS-Unbestreitbarkeit fehlschlägt.
BCG240417	Entschlüsselung fehlgeschlagen	{0}.	Fehler	Dieses Ereignis wird generiert, wenn die Entschlüsselung fehlschlägt.
BCG240418	Nachrichtenauszug kann nicht generiert werden	{0}.	Fehler	Dieses Ereignis wird generiert, wenn das System keinen Nachrichtenauszug erstellen kann.
BCG240419	Nicht unterstütztes Signaturformat	{0}.	Fehler	Dieses Ereignis wird generiert, wenn das System ein nicht unterstütztes Signaturformat empfängt.
BCG240420	Nicht unterstützter Signaturalgorithmus	{0}.	Fehler	Dieses Ereignis wird generiert, wenn das System einen nicht unterstützten Signaturalgorithmus empfängt.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG240421	Unerwarteter Fehler	{0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System auf einen unerwarteten Fehler trifft.
BCG240422	AS-Dokument für diese MDN nicht gefunden	{0}.	Fehler	Dieses Ereignis wird generiert, wenn eine MDN empfangen wird und das System das entsprechende Dokument nicht finden kann.
BCG240423	Eingabedateifehler	Ungültige Eingabedatei im Dokument übergeben.	Fehler	Dieses Ereignis wird generiert, wenn das System auf eine nicht verwendbare Eingabedatei trifft.
BCG240424	Ungenügende Nachrichtensicherheit	{0}.	Fehler	Dieses Ereignis wird generiert, wenn das System ungenügende Nachrichtensicherheit vorfindet.
BCG240500	Fehler in RosettaNet-Statusengine	Fehler in RosettaNet-Statusengine.	Kritisch	Dieses Ereignis wird generiert, wenn die RosettaNet-Statusengine einen Systemfehler vorfindet.
BCG240550	POP3-Abfragefehler	Fehler beim Abfragen des POP3-Servers: {0}; zurückgewiesene Nachrichten-VUID: {1}.	Fehler	
BCG240600	AS-Statusenginefehler	AS-Statusenginefehler: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn die RosettaNet-Statusengine einen Systemfehler vorfindet.
BCG240601	AS-Wiederholungsfehler	Max. Wiederholungslimit für AS-Attribut erreicht.	Fehler	Dieses Ereignis wird generiert, wenn das System bei der AS-Wiederholung fehlschlägt. Möglicherweise wurde das maximale Wiederholungslimit erreicht.
BCG240606	Fehler beim Packen	Fehler beim Packen: {0}.	Fehler	
BCG240610	Fehler beim Entpacken	Fehler beim Entpacken: {0}.	Fehler	
BCG240615	Fehler beim Parsing des Protokolls	Fehler beim Parsing des Protokolls: {0}.	Fehler	

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG240701	Fehler bei der Protokollierung der Aktivitäten	Fehler beim Protokollieren der Aktivitätsdetails: {0}.	Fehler	Dieses Ereignis wird generiert, wenn die Suche nach der Aktivitäts-ID für eine bestimmte Dokument-ID eines Partners nicht erfolgreich war.
BCG250001	Dokumentzustellung fehlgeschlagen	Dokumentzustellung an Partnerziel ist fehlgeschlagen: {0}.	Fehler	Dieses Ereignis wird generiert, wenn die Dokumentzustellung an ein Partnerziel fehlschlägt und das Dokument in den Status "fehlgeschlagen" gesetzt wird.
BCG250002	Fehler im Zustellscheduler	Ein interner Fehler ist im Zustellscheduler aufgetreten: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn im Zustellmanager ein nicht kategorisierter interner Fehler aufgetreten ist, der auf fehlerhafte Ziel- oder Dokumentdaten und nicht auf eine fehlgeschlagene Zustellung zurückzuführen ist.
BCG250005	FTP-Zustellung fehlgeschlagen	FTP-Zustellung an Partnerziel ist fehlgeschlagen mit Ausnahmebedingung: {0}.	Fehler	Dieses Ereignis wird generiert, wenn die FTP-Zustellung des Protokolldokuments fehlschlägt, aber mehrere Wiederholungen möglich sind. Ein endgültiges Fehlschlagen generiert Ereignis 250001.
BCG260002	RosettaNet-Pass-Through-Protokollierung fehlgeschlagen	Protokollierung der RosettaNet-Pass-Through-Prozessansicht fehlgeschlagen: {0}.	Fehler	Dieses Ereignis wird generiert, wenn ein Dokument bei der RosettaNet-Pass-Through-Anmeldung fehlschlägt.
BCG280006	Fehler beim Verarbeiten des Dokuments	Inhalts-, Metadaten- und Header-Dateien konnten in {0}-Ordnern /reject und /oversize für Dokument {1} nicht gefunden werden.	Fehler	
BCG281002	Das Dokument für das erneute Versenden über die Konsole steht bereits in der Warteschlange	Das Dokument für das erneute Versenden über die Konsole steht bereits in der Warteschlange: {0}.	Kritisch	
BCG310002	EDI-Transaktion wurde mit einem Umschlag versehen	EDI-Transaktion wurde mit einem Umschlag versehen. Umschlagsaktivitäts-ID: {0}.	Fehler	Dieses Ereignis wird generiert, wenn das Dokument für die EDI-Transaktion in einen Umschlag eingefügt wird. Die Aktivitäts-ID des Umschlags stimmt mit der Aktivitäts-ID des neuen Umschlagdokuments überein.

Tabelle 43. Fehlerereignisse (Forts.)

Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCG310003	Die EDI-Transaktion konnte nicht mit einem Umschlag versehen werden	Die EDI-Transaktion konnte nicht mit einem Umschlag versehen werden.	Fehler	Dieses Ereignis wird generiert, wenn das Dokument für die EDI-Transaktion nicht in einen Umschlag eingefügt wird. Dieses Ereignis folgt auf ein Ereignis, in dem die Fehlerdetails aufgeführt sind.
BCG800000	Abrufen des Geschäftsprozesses für den internen Partner ist fehlgeschlagen	Es konnte keine Instanz des Geschäftsprozesses für den internen Partner abgerufen werden. Ursache: {0}.	Kritisch	Dieses Ereignis wird generiert, wenn das System die Aktion des internen Partners für Geschäftsprozesse nicht finden kann.
BCG800004	Geschäftsprozess für den internen Partner hat Datenbankfehler festgestellt	{0}.	Kritisch	Dieses Ereignis wird auf Grund eines Datenbankfehlers während der Verarbeitung der Aktion des internen Partners generiert.
BCG800005	Prozess für den internen Partner hat internen Fehler festgestellt	{0}.	Kritisch	Dieses Ereignis wird auf Grund eines internen Systemfehlers während der Verarbeitung der Aktion des internen Partners generiert.
BCG700002	Fehler bei einer Task der Archivierungsfunktion	Fehler bei Task {0} in der Archivierungsfunktion.	Fehler	Dieses Ereignis wird generiert, wenn die Ausführung einer Task der Task der Archivierungsfunktion fehlschlägt.
BCG700005	Wiederherstellung ist fehlgeschlagen	Wiederherstellung ist fehlgeschlagen. Fehlerursache: {1}	Fehler	Dieses Ereignis wird generiert, wenn die Wiederherstellung in der Archivierungsfunktion fehlschlägt.

Tabelle 44. EDI-Ereigniscodes und -Nachrichten

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDICM0001	Unerwartete Ausnahmebedingung aufgetreten	In Komponente {0} ist ein unerwarteter Fehler aufgetreten. Text der Ausnahmebedingung: {1}.	Fehler	
BCGEDICM0003	Erforderliche Eigenschaft fehlt	Ungültige Eingabe für Komponente {0}. Die erforderliche Eigenschaft {1} fehlt.	Fehler	
BCGEDICM0004	Ungültiger Eigenschaftswert	Ungültige Eingabe für Komponente {0}. Der Wert {1} ist für die Eigenschaft {2} ungültig.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDICM0005	Nicht unterstützter Zeichensatz	Ungültige Eingabe für Komponente {0}. Der in Eigenschaft {2} angegebene Zeichensatz {1} wird nicht unterstützt.	Fehler	
BCGEDICM0006	Ungültige Dokumentsyntax für die Komponente	Ungültige Eingabe für Komponente {0}. Die Dokumentsyntax {1} ist für diese Komponente nicht gültig.	Fehler	
BCGEDICM0010	E/A-Fehler aufgetreten	In Komponente {0} ist ein E/A-Fehler aufgetreten. Text der Ausnahmebedingung: {1}.	Fehler	
BCGEDICM0011	Öffnen der Datei ist fehlgeschlagen	Komponente {0} konnte die Datei {1} nicht öffnen.	Fehler	
BCGEDICM0012	Fehler beim Zugriff auf den Speicherpuffer	Komponente {0} konnte nicht auf den Speicherpuffer zugreifen.	Fehler	
BCGEDICM0013	Fehlende Eingabedatenquelle	Für Komponente {0} wurde keine Eingabedatenquelle angegeben.	Fehler	
BCGEDICM0014	Fehlende Ausgabedatenquelle	Für Komponente {0} wurde keine Ausgabedatenquelle angegeben.	Fehler	
BCGEDICM0020	Parsingfehler in der Komponente	Komponente {0} ist fehlgeschlagen. Fehler beim Parsing der Eingabedaten.	Fehler	
BCGEDICM0021	Datenbankfehler	Beim Zugreifen auf die Datenbank ist ein Fehler aufgetreten. Klassenname: {0}, Methode: {1}, Ausnahmebedingung: {2}.	Fehler	
BCGEDICM0022	Unerwartete Ausnahmebedingung in der Datenbank	Beim Zugreifen auf die Datenbank ist eine unerwartete Ausnahmebedingung aufgetreten. Klassenname: {0}, Methode: {1}, Ausnahmebedingung: {2}.	Fehler	
BCGEDICM0023	Keine Datenbankverbindung	Die Managerklasse {0} der Datenbankverbindung gab keine gültige Verbindung zurück.	Kritisch	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDICM0101	Fehlendes oder ungültiges Objekt für die Komponente	Ein interner Fehler ist aufgetreten. Das an die Komponente {0} übergebene Objekt fehlt oder ist ungültig.	Fehler	
BCGEDICM0102	Fehler beim Laden einer Klasse	Eine dynamisch konfigurierte Klasse konnte nicht geladen werden. Konfigurationsschlüssel {0}, Klassenname: {1}.	Kritisch	
BCGEDICM0103	Ungültiger Funktionsparameter	In Komponente {0} ist ein interner Fehler aufgetreten. Der ungültige Wert '{1}' wurde an die Funktion {2} übergeben.	Fehler	
BCGEDICM0104	Ungültiges Quellendokument	Das Quellendokument ist für die Komponente {0} nicht gültig.	Fehler	
BCGEDIEM0100	Inhalt der Aufzeichnungsdatei	Inhalt der Aufzeichnungsdatei {0}.	Fehler	
BCGEDIEM0101	Beim Abrufen der Zertifikate ist eine Ausnahmebedingung aufgetreten	Beim Abrufen der Zertifikate ist eine Ausnahmebedingung aufgetreten. Details: {0}.	Fehler	
BCGEDIEM0102	Beim Lesen der Aufzeichnungsdatei ist eine Ausnahmebedingung aufgetreten	Beim Lesen der Aufzeichnungsdatei ist eine Ausnahmebedingung aufgetreten. Details: {0}.	Fehler	
BCGEDIEM0103	Ein erforderliches Attribut ist leer	Ein erforderliches Attribut {0} ist leer.	Fehler	
BCGEDIEM0104	Beim Schreiben der zu sendenden Datei an eine temporäre Position ist eine Ausnahmebedingung aufgetreten	Beim Schreiben der zu sendenden Datei an eine temporäre Position ist eine Ausnahmebedingung aufgetreten. Details: {0}.	Fehler	
BCGEDIEM0105	Zertifikate müssen in das Zertifikatrepository hochgeladen werden	Zertifikate müssen in das Zertifikatrepository hochgeladen werden.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIEM0106	Die Datei mit dem privaten Schlüssel konnte nicht geladen werden. Aliasname nicht gefunden	Die Datei mit dem privaten Schlüssel konnte nicht geladen werden. Aliasname nicht gefunden.	Fehler	
BCGEDIEM0107	Validierung des Clientzertifikats (lokales Zertifikat) ist fehlgeschlagen. Möglicherweise ist das Zertifikat ungültig oder wurde widerrufen	Validierung des Clientzertifikats (lokales Zertifikat) ist fehlgeschlagen. Möglicherweise ist das Zertifikat ungültig oder wurde widerrufen.	Fehler	
BCGEDIEM0108	Sicherheitsausnahmebedingung	Sicherheitsausnahmebedingung. Details: {0}.	Fehler	
BCGEDIEM0109	Der für den Empfänger angegebene Wert für das temporäre Verzeichnis ist leer	Der für die Empfängerkomponente angegebene Wert für das temporäre Verzeichnis ist leer.	Fehler	
BCGEDIEM0110	Das übergebene 'BusinessDoucument'-Array ist leer	Das übergebene 'BusinessDoucument'-Array ist leer.	Fehler	
BCGEDIEM0111	Eingabedatei ist leer	Die Eingabedatei ist leer.	Fehler	
BCGEDIEM0112	Eine Verteilerausnahmebedingung wurde empfangen	Eine Ausnahmebedingung des Verteilers wurde empfangen. Details: {0}.	Fehler	
BCGEDIEM0113	Eine Verteilerausnahmebedingung wurde empfangen	Eine Ausnahmebedingung des Verteilers wurde empfangen. Details: {0}.	Fehler	
BCGEDIEM0114	Eingabeprogramm kann nicht gefunden werden	Eingabeprogramm kann nicht gefunden werden.	Fehler	
BCGEDIEM0118	Fehler bei der Zeichencodierung	Fehler beim Codieren von "{0}" in den Zeichensatz {1}.	Fehler	
BCGEDIEM0120	Fehler beim Initialisieren von 'RODScanner'	Fehler beim Initialisieren von 'RODScanner'. Details: {0}.	Fehler	
BCGEDIEM0128	Netzfehlernachricht von IBM VAN empfangen	Netzfehlernachricht von IBM VAN empfangen. Details: Nachrichten-ID = {0}, Nachrichtenbeschreibung = {1}, Fehlerklasse = {2}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIEM0150	Das übergebene Dokument gilt nicht für EDIAckHandler	Das übergebene Dokument gilt nicht für EDIAckHandler.	Fehler	
BCGEDIEM0151	Fehler beim Verarbeiten der EDI-Bestätigung	Fehler beim Verarbeiten der EDI-Bestätigung. Nachricht wurde in Fehlerterminal versetzt.	Fehler	
BCGEDIEM0152	Die Datenbankverbindung kann nicht aus dem Kontext abgerufen werden	Die Datenbankverbindung kann nicht aus dem Kontext abgerufen werden.	Fehler	
BCGEDIEM0200	Datenbankverbindungsfehler	Ungültiges oder fehlendes Datenbankverbindungsobjekt im Kontext.	Fehler	
BCGEDIEM0201	E/A-Fehler beim Schreiben in die Datei	Im Verzeichnis PROCESS DIR {0} kann keine Datei erstellt werden.	Fehler	
BCGEDIEM0202	'AbsDocument' kann nicht serialisiert werden	Ausnahmebedingung des Parsers beim Serialisieren von 'AbsDocument'.	Fehler	
BCGEDIEM0203	Beim Serialisieren von 'AbsDocument' ist eine Ausnahmebedingung aufgetreten	Ausnahmebedingung beim Serialisieren von 'AbsDocument'.	Fehler	
BCGEDIEM0204	Geschäftsdokument kann nicht eingeführt werden	Geschäftsdokument mit der ID {0} konnte nicht wieder in den Arbeitsablauf eingeführt werden.	Fehler	
BCGEDIEM0205	Statusinformationen können nicht gefunden werden	Die Statusinformationen im Status-Management-Service konnten nicht gefunden werden.	Fehler	
BCGEDIEV0003	Beginn des Austauschs nicht gefunden	Das Entfernen des Umschlags für eine Nachricht ist fehlgeschlagen, da kein gültiger Beginn des Austausch gefunden werden konnte.	Fehler	
BCGEDIEV0009	Suche des Kurznamens des Handelspartners fehlgeschlagen	Der Kurzname des Handelspartners konnte nicht gefunden werden: {0}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIEV0010	Interner Fehler für Funktion	Ein interner Fehler ist aufgetreten. Funktion: {0}, Rückkehrcode: {1}.	Fehler	
BCGEDIEV0011	Die Datenbanktransaktion ist fehlgeschlagen	Die Datenbanktransaktion ist fehlgeschlagen. SQL-Fehler: {0}.	Fehler	
BCGEDIEV0018	Umschlagssegment nicht gefunden	Das Programm zum Generieren oder Entfernen des Umschlags für {0} hat einen Fehler festgestellt: Segment {1} konnte nicht gefunden werden.	Fehler	
BCGEDIEV0050	Suche in der Konvertierungstabelle fehlgeschlagen	Die Suche in einer Umsetzungstabelle ist fehlgeschlagen, während eine Nachricht mit einem Umschlag versehen oder der Umschlag der Nachricht entfernt wurde. Umsetzungstabelle: {0}, Wert: {1}.	Fehler	
BCGEDIEV0051	Umschlagssegment nicht gefunden	Das Programm zum Entfernen eines Umschlags für {0} hat einen Fehler festgestellt: {1} wurde ohne {2} gefunden.	Fehler	
BCGEDIEV0052	Leere Nachricht soll mit Umschlag versehen werden	Das Programm zum Generieren eines Umschlags für {0} hat einen Fehler festgestellt: Eine leere Nachricht soll mit einem Umschlag versehen werden.	Fehler	
BCGEDIEV0053	Maximalzahl der Gruppen für die Kontrollnummernmaske überschritten	Das Programm zum Generieren eines Umschlags für {0} hat einen Fehler festgestellt: Die Gesamtzahl der Gruppen ist größer als die durch die Kontrollnummernmaske zulässige Anzahl.	Fehler	
BCGEDIEV0054	Mehrfache Fehler bei Austausch	Das Programm zum Entfernen eines Umschlags für {0} hat einen Fehler festgestellt: Mehrfacher nicht zulässiger Austausch wurde festgestellt.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIEV0055	Warnung bei Suche in der Konvertierungstabelle	Die Suche in der Konvertierungstabelle lieferte keinen Eintrag während des Einfügens einer Nachricht in einen Umschlag. Konvertierungstabelle: {0}, Wert: {1}.	Fehler	
BCGEDIEV0056	Warnung bei Suche in der Konvertierungstabelle	Die Suche in der Konvertierungstabelle lieferte keinen Eintrag während des Entfernens eines Umschlags von einer Nachricht. Konvertierungstabelle: {0}, Wert: {1}, Gruppen-/ Transaktionskontrollnummer {2}.	Fehler	
BCGEDIEV0057	Umschlag fehlgeschlagen	Fehler beim Einfügen einer Nachricht in einen Umschlag. Umschlagtyp: {0}.	Fehler	
BCGEDIEV0058	Entfernen des Umschlags fehlgeschlagen	Fehler beim Entfernen eines Umschlags von einer Nachricht.	Fehler	
BCGEDIFT0100	Erwartetes Argument fehlt	Syntaxfehler in Befehl '{0}'. Ein erwartetes Argument fehlte.	Fehler	
BCGEDIFT0110	FTP-Scriptverarbeitung gestoppt	Der Fehler führte dazu, dass die FTP-Scriptverarbeitung gestoppt wurde.	Fehler	
BCGEDIFT0111	Basisname der Datei fehlt	Für abgerufene Dateien wurde kein Basisname angegeben.	Fehler	
BCGEDIFT0112	Fehlendes oder ungültiges Objekt für die Komponente	Unbekanntes Objekt im Eingabeterminal.	Fehler	
BCGEDIFT0113	Unerwarteter Fehler beim Ausführen des Befehls	Unerwarteter Fehler bei der Ausführung des Befehls '{0}'.	Fehler	
BCGEDIFT0114	Unerwarteter Fehler beim Herunterladen der Datei	Unerwarteter Fehler beim Herunterladen der Datei '{0}'.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIFT0115	FTP-Scriptdatei konnte nicht gefunden werden	FTP-Scriptdatei nicht gefunden.	Fehler	
BCGEDIFT0116	E/A-Ausnahmebedingung beim Lesen der Datei	Beim Lesen des Scripts wurde eine E/A-Ausnahmebedingung abgefangen.	Fehler	
BCGEDIFT0117	Unerwartete Ausnahmebedingung bei der Syntaxanalyse des FTP-Scripts	Bei der Syntaxanalyse des Scripts wurde eine unerwartete Ausnahmebedingung abgefangen. Wenden Sie sich an den Systemadministrator. Weitere Informationen zu der Ausnahmebedingung sowie einen Stack-Trace finden Sie in der Tracedatei.	Fehler	
BCGEDIFT0118	Hochladen der Datei ist fehlgeschlagen	Die Datei kann nicht hochgeladen werden. Dateiname: {0}.	Fehler	
BCGEDIFT0119	Keine Datei für MPUT vorhanden	MPUT wurde abgesetzt, aber es wurde keine Datei zum Senden gefunden. Dateiname: {0}. Verzeichnis: {1}.	Fehler	
BCGEDIFT0120	Der FTP-Befehl hat das Zeitlimit überschritten	Der FTP-Befehl hat das Zeitlimit überschritten. Gesendeter Befehl: {0}.	Fehler	
BCGEDIFT0200	E/A-Ausnahmebedingung	Eine E/A-Ausnahmebedingung ist aufgetreten. Text der Ausnahmebedingung: {0}.	Fehler	
BCGEDIFT0201	Erstellen des Daten-Sockets ist fehlgeschlagen	Daten-Socket konnte nicht erstellt werden. Verbindung oder 'ControlSocket' ist leer.	Fehler	
BCGEDIFT0202	Antwortcodes sind leer	Ausnahmebedingung wegen Nullzeiger: 'StringBuffer' mit Antwortcodes für die Verarbeitung ist leer.	Fehler	
BCGEDIFT0203	Ungültige Argumentwerte	Ungültige Werte für die Argumente, oder einige oder alle Werte sind leer.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIFT0204	Steuer-Socket nicht erstellt	Steuer-Socket nicht erstellt.	Fehler	
BCGEDIFT0205	Erforderliche Datei nicht gefunden	Erforderliche Datei nicht gefunden.	Fehler	
BCGEDIFT0206	Ausnahmebedingung aufgetreten	Ausnahmebedingung aufgetreten.	Fehler	
BCGEDIFT0207	Aktiver Daten-Socket ist leer	Aktiver Daten-Socket ist leer.	Fehler	
BCGEDIFT0208	'SocketException' ist aufgetreten	'SocketException' ist aufgetreten.	Fehler	
BCGEDIFT0209	Passiver Daten-Socket ist leer	Passiver Daten-Socket ist leer.	Fehler	
BCGEDIFT0210	Daten-Socket ist leer	Daten-Socket ist leer.	Fehler	
BCGEDIFT0211	Laden des privaten Schlüssels ist fehlgeschlagen	Die Datei mit dem privaten Schlüssel konnte nicht aus der Datei—{0} geladen werden. Aliasname nicht gefunden.	Fehler	
BCGEDIFT0212	Validierung des Clientzertifikats ist fehlgeschlagen	Validierung des Clientzertifikats (lokales Zertifikat) ist fehlgeschlagen. Möglicherweise ist das Zertifikat ungültig oder wurde widerrufen	Fehler	
BCGEDIFT0220	Befehl OPEN ist fehlgeschlagen	Befehl OPEN ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0221	Befehl CWD ist fehlgeschlagen	Befehl CWD ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0222	Befehl DELE ist fehlgeschlagen	Befehl DELE ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0223	Befehl PUT ist fehlgeschlagen	Befehl PUT ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0224	Befehl GET ist fehlgeschlagen	Befehl GET ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0225	Befehl LIST ist fehlgeschlagen	Befehl LIST ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0226	Befehl QUIT ist fehlgeschlagen	Befehl QUIT ist fehlgeschlagen. Ursache: {0}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIFT0227	Befehl RMD ist fehlgeschlagen	Befehl RMD ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0228	Befehl MKD ist fehlgeschlagen	Befehl MKD ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0229	Befehl PASV ist fehlgeschlagen	Befehl PASV ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0230	Befehl GETDEL ist fehlgeschlagen	Befehl GETDEL ist fehlgeschlagen. Ursache: {0}.	Fehler	
BCGEDIFT0231	Befehl FTP ist fehlgeschlagen	Befehl FTP {0} ist fehlgeschlagen. Ursache: {1}.	Fehler	
BCGEDIFT0232	Keine Antwort vom FTP-Server	Keine Antwort vom FTP-Server.	Fehler	
BCGEDIMD0001	Unerwartete Ausnahmebedingung beim Lesen von Metadaten	Beim Lesen der Metadaten ist eine unerwartete Ausnahmebedingung aufgetreten. Syntax: {0}, Wörterverzeichnis: {1}, Dokument: {2}, Text der Ausnahmebedingung: {3}.	Fehler	
BCGEDIMD0002	Steuerzeichenfolge für Metadaten ist ungültig	Die Steuerzeichenfolge der Metadaten ist ungültig oder wurde für eine andere Version kompiliert. Syntax: {0}, Wörterverzeichnis: {1}, Dokument: {2}.	Fehler	
BCGEDIMD0003	Lesen der Steuerzeichenfolge für Metadaten ist fehlgeschlagen	Die Steuerzeichenfolge der Metadaten konnte nicht aus der Datenbank gelesen werden. Syntax: {0}, Wörterverzeichnis: {1}, Dokument: {2}.	Fehler	
BCGEDINK0001	Ungültige Netzbestätigung	Das an die IBM VAN-Komponente für die Netzbestätigung übergebene Dokument ist keine gültige Netzbestätigung.	Fehler	
BCGEDINK0002	Ungültiger Attributwert	Das Attribut {0} hat den ungültigen Wert {1}.	Fehler	
BCGEDISP0002	Codierung kann nicht ermittelt werden	Der XML-Verteiler konnte die Codierung der XML-Eingabedaten nicht ermitteln.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDISP0003	Ungültige XML-Daten	Die an den XML-Verteiler übergebenen Daten sind keine gültigen XML-Daten.	Fehler	
BCGEDISP0005	Austauschiterator ist leer	Ein interner Fehler ist aufgetreten. Der Austauschiterator wurde während eines vorherigen Aufrufs nicht definiert.	Fehler	
BCGEDISP0006	Ende der Eingabedaten	Der Verteiler hat das Ende der Eingabedaten erreicht.	Fehler	
BCGEDIUP0001	Schwer wiegender XML-Parsingfehler	Bei der Syntaxanalyse des XML-Dokuments {0} ist ein schwerwiegender Fehler aufgetreten. Zeile: {1}, Spalte: {2}. Nachrichtentext des Parsers: {3}.	Fehler	
BCGEDIUP0002	Schwerer XML-Parsingfehler	Bei der Syntaxanalyse des XML-Dokuments {0} ist ein schwerer Fehler aufgetreten. Zeile: {1}, Spalte: {2}. Nachrichtentext des Parsers: {3}.	Fehler	
BCGEDIUP0015	Lesen der Metadaten ist fehlgeschlagen	Das Abrufen der Metadaten für die Nachricht ist fehlgeschlagen.	Fehler	
BCGEDIUP0118	Fehler bei der Zeichencodierung	Fehler beim Codieren von "{0}" in den Zeichensatz {1}.	Fehler	
BCGEDIUP0021	Eingabedatensatz kann nicht identifiziert werden	Der Eingabedatensatz kann nicht identifiziert werden. Satznummer: {0}. Datenimage: {1}.	Fehler	
BCGEDIUP0023	Datensatz hat angegebene maximale Anzahl von Wiederholungen überschritten	Die empfangenen Daten haben die angegebenen maximalen Wiederholungen überschritten. Satznummer: {0}. Datenidentifikation: {1}. Maximale Anzahl Wiederholungen: {2}	Fehler	
BCGEDIUP0033	Fehlende Wörterverzeichnis- oder Dokumentwerte	Die für die Syntaxanalyse verwendeten Wörterverzeichnis- oder Dokumentwerte wurden nicht angegeben oder sind leer.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIUP0034	Ungültige Strukturverwendung	Durch Zeichen getrennte Daten ist für Datenformate, die Strukturen enthalten, keine unterstützte Option.	Fehler	
BCGEDIUP0038	Fehlender Satzbegrenzer	Das Ende des Datensatzes wurde erreicht, ohne dass ein Satzbegrenzer gefunden wurde. Erwarteter Satzbegrenzer: {0}. Satznummer: {1}. Satzname: {2}. Relative Byteadresse: {3}.	Fehler	
BCGEDIUP0039	Zeichenkonvertierung ist fehlgeschlagen	Die Konvertierung von Daten in Unicodezeichen ist fehlgeschlagen. Eingabedaten: {0}. Datenlänge {1}. Empfangener Fehler: {2}.	Fehler	
BCGEDIUP0040	Ungültige Daten für den Datentyp	Ungültige Daten gefunden beim Konvertieren von Daten des Typs {0}. Ungültige Daten: {1}.	Fehler	
BCGEDIUP0041	Nicht unterstützter Zeichensatz	Der für die ROD-Daten verwendete Zeichensatz wird nicht unterstützt. Zeichensatz: {0}.	Fehler	
BCGEDIUP0042	Nicht unterstützter Datensatz	Beim Verarbeiten von C- und D-Sätzen wurde ein nicht unterstützter Satz gefunden. Das Zeichen C, D oder Z wurde an der ersten Stelle erwartet. {0} wurde empfangen. Relative Byteadresse: {1}.	Fehler	
BCGEDIUP0052	Unerwartete Ausnahmebedingung bei der Serialisierung	Beim Serialisieren des Dokuments ist eine unerwartete Ausnahmebedingung aufgetreten. Text der Ausnahmebedingung: {0}.	Fehler	
BCGEDIUP0053	Erstellung der Parser- oder Serialisierungsmethode ist fehlgeschlagen	Für die Syntax {0} konnte kein Parser oder keine Serialisierungsmethode erstellt werden.	Fehler	
BCGEDIUP0055	Leeres Dokument für die Serialisierung	Das Dokument konnte nicht serialisiert werden, da es leer ist.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIUP0057	Ungültiges Dokument für die Serialisierung	Das Dokument konnte nicht serialisiert werden, da seine interne Struktur ungültig ist.	Fehler	
BCGEDIUP0099	Keine erkannten Eingabedaten	Der Parser fand keine erkennbaren Eingabedaten. Parserkomponente {0}.	Fehler	
BCGEDIUP0100	Details der Metadaten konnten nicht gefunden werden	Metadatendetails konnten im Dokument nicht gefunden werden. Wörterverzeichnis={0}, Dokument={1}, Syntax={2}.	Fehler	
BCGEDIUP0101	Steuerzeichenfolge für Metadaten konnte nicht gefunden werden	Steuerzeichenfolge für Metadaten konnte nicht gefunden werden. Wörterverzeichnis={0}, Dokument={1}, Syntax={2}.	Fehler	
BCGEDIUP0106	Ungültiges ROD-Datenformat	Ungültiges ROD-Datenformat. Im Satzknoten wurden keine untergeordneten Knoten (Strukturen oder Felder) gefunden. Satzname: {0}.	Fehler	
BCGEDIUP0107	Fehlender Satzname im Satz	Im Dokument für den D-Satz wurde ein leerer Satzname (NULL RecordName) gefunden.	Fehler	
BCGEDIUP0108	Unerwartete Knoten unterhalb des Stammknotens	Ungültiges ROD-Datenformat. Der ROD-Stammknoten {0} hat andere untergeordnete Knoten als 'Satz' und 'Schleife'.	Fehler	
BCGEDIUP0109	Fehlender Satzname im Knoten	Im Satzknoten wurde ein leerer Satzname gefunden.	Fehler	
BCGEDIUP0110	Fehler beim Abrufen der Metadateninformationen	'RODMetaDataElement' kann nicht aus den Metadaten für den folgenden Satz abgerufen werden: {0}.	Fehler	
BCGEDIUP0111	Leerer Datensatz	In 'MetaDataElement' {0} wurden keine untergeordneten Elemente gefunden. Elementtyp: Satz.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIUP0112	Unerwartete Knoten unterhalb des Satzknotens	Ungültiges ROD-Datenformat. Der ROD-Satzknoten {0} hat andere untergeordnete Knoten als 'Struktur' und 'Feld'.	Fehler	
BCGEDIUP0113	Unerwartete Knoten unterhalb des Schleifenknotens	Ungültiges ROD-Datenformat. Der ROD-Schleifenknoten {0} hat andere untergeordnete Knoten als 'Schleife' und 'Satz'.	Fehler	
BCGEDIUP0114	Unerwartete Knoten unterhalb des Strukturknotens	Ungültiges ROD-Datenformat. Der ROD-Strukturknoten {0} hat andere untergeordnete Knoten als 'Struktur' und 'Feld'.	Fehler	
BCGEDIUP0115	Leere Struktur	In 'MetaDataElement' {0} wurden keine untergeordneten Elemente gefunden. Elementtyp: Struktur.	Fehler	
BCGEDIUP0116	Ungültiges Zeichen im Datenformat	Im Datenformat {0} wurde ein ungültiges Zeichen gefunden. Zeichen: {1}.	Fehler	
BCGEDIUP0117	Fehler bei der Zeichendecodierung	Zeichendecodierfehler. Relative Adresse: {0}.	Fehler	
BCGEDIUP0118	Fehler bei der Zeichencodierung	Fehler beim Codieren von "{2}" in den Zeichensatz {3}.	Fehler	
BCGEDIUT0008	Name der aktuellen Zuordnung	Name der verarbeiteten Zuordnung: {0}.	Fehler	
BCGEDIUT0011	Anweisung der Steuerzeichenfolge ist fehlgeschlagen	Der Transformationsknoten (DTC) konnte eine Anweisung der Steuerzeichenfolge nicht verarbeiten. Anweisung der Steuerzeichenfolge: {0}, Relative Adresse des Anweisungsdatenstroms: {1}, Name der Zuordnung: {2}.	Fehler	
BCGEDIUT0023	Erstellen des Ausgabedokuments ist fehlgeschlagen	Das Erstellen eines Ausgabedokuments ist fehlgeschlagen. Name des Stammknotens: {0}, Syntax: {1}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIUT0033	Vom Benutzer angegebener Nachrichtentext	Text der vom Benutzer angegebenen Nachricht: {0}. Diese Nachricht wurde mit der Fehlerklasse {1} und dem Benutzercode {2} protokolliert.	Fehler	
BCGEDIUT0034	'HexDecode'-Zeichenfolgelänge ist ungültig	Die Transformationskomponente versuchte, eine Zeichenfolge mit 'HexDecode' zu decodieren; die Zeichenfolgelänge war jedoch ungültig. Die Anzahl der Zeichen in der zu decodierenden Zeichenfolge muss eine gerade Zahl sein.	Fehler	
BCGEDIUT0035	'HexDecode'-Zeichen ist ungültig	Die Transformationskomponente führte den Befehl 'HexDecode' aus. Ein Zeichenfolgewert, der nicht decodiert werden kann, wurde gefunden. Zeichenfolgewert: {0}.	Fehler	
BCGEDIUT0041	Suche in der Konvertierungstabelle fehlgeschlagen	Sucheintrag {0} der Konvertierungstabelle nicht in {1} gefunden. Zurückgegebener Standardwert: {2}.	Fehler	
BCGEDIUT0061	Ungültiger Wert für eingebettete Zuordnung	Für die eingebettete Zuordnung ist ein Byte-Array-Element erforderlich. Relative Adresse des Anweisungsdatenstroms: {1}, Name der Zuordnung: {2}.	Fehler	
BCGEDIUT0100	Benutzerexit nicht gefunden	Benutzerexit {0} konnte nicht gefunden werden.	Fehler	
BCGEDIUT0101	Unerwartete Ausnahmebedingung im Benutzerexit	Benutzerexit {0}: Unerwartete Ausnahmebedingung: {1}.	Fehler	
BCGEDIUT0401	Steuerzeichenfolge für Zuordnung konnte nicht gefunden werden	Die Steuerzeichenfolge für die Zuordnung {0} konnte nicht in der Datenbank gefunden werden.	Fehler	
BCGEDIUT0402	Steuerzeichenfolge für Zuordnung ist ungültig	Die Steuerzeichenfolge für die Zuordnung {0} ist ungültig oder wurde für eine andere Version kompiliert.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIUT0403	Globale Variable nicht gefunden	Die globale Variable {0} konnte nicht gefunden werden. Die Steuerzeichenfolge {1} für die Zuordnung konnte nicht geladen werden.	Fehler	
BCGEDIUT0404	Globale Variable hat einen ungültigen Anfangswert	Die globale Variable {0} hat einen ungültigen Anfangswert. Die Steuerzeichenfolge {1} für die Zuordnung konnte nicht geladen werden.	Fehler	
BCGEDIUT0405	Unerwartete Ausnahmebedingung beim Lesen der Steuerzeichenfolge für Zuordnung	Beim Lesen der Steuerzeichenfolge für die Zuordnung aus der Datenbank ist eine unerwartete Ausnahmebedingung aufgetreten. Name der Zuordnung: {0}, Text der Ausnahmebedingung: {1}.	Fehler	
BCGEDIUT0406	Unerwartete Ausnahmebedingung beim Lesen der globalen Variablen	Beim Lesen der globalen Variablen aus der Datenbank ist eine unerwartete Ausnahmebedingung aufgetreten. Name der Variablen: {0}, Name der Zuordnung: {1}, Text der Ausnahmebedingung: {2}.	Fehler	
BCGEDIUT0407	Datenbankfehler beim Lesen der Steuerzeichenfolge für Zuordnung	Die Steuerzeichenfolge für die Zuordnung {0} konnte wegen eines Datenbankfehlers nicht geladen werden.	Fehler	
BCGEDIUT0501	Eingabedokument für die Konvertierung ist leer	Das Eingabedokument für die Transformation ist leer.	Fehler	
BCGEDIVA0001	Obligatorisches Datenelement fehlt	Ein obligatorisches Datenelement fehlt. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0002	Datenelement ist zu lang	Datenelement ist zu lang. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}, effektive Länge = {10}, definierte maximale Länge = {11}.	Fehler	
BCGEDIVA0003	Datenelement ist zu kurz	Datenelement ist zu kurz. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}, effektive Länge = {10}, definierte minimale Länge = {11}.	Fehler	
BCGEDIVA0004	Codierter Wert konnte in der Validierungstabelle nicht gefunden werden	Codierter Wert konnte in der Validierungstabelle nicht gefunden werden. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}, Validierungstabelle = {10}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0010	Bedingung 'paarig' (P) wurde nicht erfüllt	Die Bedingung 'paarig' (P) wurde nicht erfüllt. Der Standard definiert die Elemente {0} als paarig; es ist aber nur Element {1} vorhanden. Segmentname = {2}, Segmentposition = {3}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {4}/{5}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {6}/{7}, Kontrollnummern = {8}.	Fehler	
BCGEDIVA0011	Bedingung 'erforderlich' (R) wurde nicht erfüllt	Die Bedingung 'erforderlich' (R) wurde nicht erfüllt. Der Standard definiert die Elemente {0} als erforderlich; alle Elemente fehlen jedoch. Segmentname = {2}, Segmentposition = {3}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {4}/{5}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {6}/{7}, Kontrollnummern = {8}.	Fehler	
BCGEDIVA0012	Bedingung 'ausschließend' (E) wurde nicht erfüllt	Die Bedingung 'ausschließend' (E) wurde nicht erfüllt. Der Standard definiert die Elemente {0} als sich gegenseitig ausschließend, die Elemente {1} sind jedoch vorhanden. Segmentname = {2}, Segmentposition = {3}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {4}/{5}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {6}/{7}, Kontrollnummern = {8}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0013	Bedingung 'bedingt' (C) wurde nicht erfüllt	Die Bedingung 'bedingt' (C) wurde nicht erfüllt. Der Standard definiert die Elemente {0} als bedingt erforderlich, aber nur {1} ist vorhanden. Ist das erste Element vorhanden, müssen alle anderen Elemente ebenfalls vorhanden sein. Segmentname = {2}, Segmentposition = {3}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {4}/{5}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {6}/{7}, Kontrollnummern = {8}.	Fehler	
BCGEDIVA0014	Bedingung 'bedingte Liste' (L) wurde nicht erfüllt	Die Bedingung 'bedingte Liste' (L) wurde nicht erfüllt. Der Standard definiert die Elemente {0} als bedingt paarig, aber nur {1} ist vorhanden. Ist das erste Element vorhanden, muss mindestens eines der anderen Elemente ebenfalls vorhanden sein. Segmentname = {2}, Segmentposition = {3}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {4}/{5}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {6}/{7}, Kontrollnummern = {8}.	Fehler	
BCGEDIVA0015	Obligatorisches zusammengesetztes Element fehlt	Ein obligatorisches zusammengesetztes Element fehlt. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0016	Maximale Wiederholungen für das zusammengesetzte Datenelement überschritten	Das zusammengesetzte Element wird häufiger wiederholt, als im Standard definiert. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Anzahl der Wiederholungen = {8}, maximal definierte Wiederholungen= {9}.	Fehler	
BCGEDIVA0025	Doppelte Transaktion oder Nachricht im Austausch oder in der Gruppe	Doppelte Transaktionsgruppe oder Nachricht im aktuellen Austausch oder in der aktuellen funktionalen Gruppe, Kontrollnummer der Transaktionsgruppe oder Nachricht = {0}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}, Kontrollnummern = {5}.	Fehler	
BCGEDIVA0030	Zeichensatzvalidierung für das Datenelement fehlgeschlagen	Zeichensatzvalidierung für Datenelement ist fehlgeschlagen. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}, Validierungstabelle = {10}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0031	Ungültiges numerisches Element	Ungültiges numerisches Element. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}.	Fehler	
BCGEDIVA0032	Ungültiges reelles numerisches Element	Ungültiges reelles numerisches Element. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}.	Fehler	
BCGEDIVA0033	Ungültiges Datumselement	Ungültiges Datumselement. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}.	Fehler	
BCGEDIVA0034	Ungültiges Zeitelement	Ungültiges Zeitelement. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Elementtyp = {8}, Wert = {9}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0035	Maximale Wiederholungen für das Datenelement überschritten	Das Element wird häufiger wiederholt, als im Standard definiert. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}. Anzahl der Wiederholungen = {8}, maximal definierte Wiederholungen= {9}.	Fehler	
BCGEDIVA0050	Zu viele Elemente oder unerwartetes Element im Segment	Zu viele Elemente oder nicht erwartetes Element im Segment. Elementname = {0}, Segmentname = {1}, Segmentposition = {2}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {3}/{4}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {5}/{6}, Kontrollnummern = {7}.	Fehler	
BCGEDIVA0051	Nicht erkannte Segment-ID	Nicht erkannte Segment-ID. Segmentname = {0}, Segmentposition = {1}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {2}/{3}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {4}/{5}, Kontrollnummern = {6}.	Fehler	
BCGEDIVA0052	Obligatorisches Segment fehlt	Obligatorisches Segment fehlt. Segmentname = {0}, Segmentposition = {1}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {2}/{3}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {4}/{5}, Kontrollnummern = {6}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0054	Schleife wiederholt öfter, als im Standard definiert	Schleife wiederholt häufiger, als im Standard definiert. Schleifenname = {0}, Segmentposition = {1}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {2}/{3}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {4}/{5}, Kontrollnummern = {6}. Anzahl der Wiederholungen = {7}, maximal definierte Wiederholungen= {8}.	Fehler	
BCGEDIVA0055	Segment wiederholt öfter, als im Standard definiert	Segment wiederholt häufiger, als im Standard definiert. Segmentname = {0}, Segmentposition = {1}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {2}/{3}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {4}/{5}, Kontrollnummern = {6}. Anzahl der Wiederholungen = {7}, maximal definierte Wiederholungen= {8}.	Fehler	
BCGEDIVA0101	Transaktionsgruppe oder Nachrichtenkontrollnummern stimmen nicht überein	Die Kontrollnummern der Transaktionsgruppe oder Nachricht im Header und Trailer stimmen nicht überein. Kontrollnummer des Gruppenheaders = {0}, Kontrollnummer des Gruppentrailers = {1}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {2}/{3}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {4}/{5}, Kontrollnummern = {6}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0102	Trailer der Transaktionsgruppe oder Nachricht fehlt oder ist ungültig	Trailer der Transaktionsgruppe oder Nachricht fehlt oder ist ungültig. Kontrollnummer = {0}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}, Kontrollnummern = {5}.	Fehler	
BCGEDIVA0103	Ungültige Anzahl von Trailern der Transaktionsgruppe oder Nachricht	Trailer der Transaktionsgruppe oder Nachricht enthält eine ungültige Anzahl an Segmenten. Kontrollnummer = {0}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}. Wert im Trailer = {5}, tatsächlich empfangene Anzahl = {6}.	Fehler	
BCGEDIVA0151	Kontrollnummern für die funktionale Gruppe stimmen nicht überein	Die Kontrollnummern der funktionalen Gruppe im Header und Trailer stimmen nicht überein. Kontrollnummer des Headers = {0}, Kontrollnummer des Trailers = {1}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {2}/{3}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {4}/{5}, Kontrollnummern = {6}.	Fehler	
BCGEDIVA0152	Trailer der funktionalen Gruppe fehlt oder ist ungültig	Trailer der funktionalen Gruppe fehlt oder ist ungültig. Funktionale Kontrollnummer = {0}, ID/ Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/ Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}, Kontrollnummern = {5}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0153	Ungültige Anzahl von Trailern der funktionalen Gruppe	Trailer der funktionalen Gruppe enthält eine ungültige Anzahl an Transaktionsgruppen oder Nachrichten. Funktionale Kontrollnummer = {0}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}, Kontrollnummern = {5}. Wert im Trailer = {6}, tatsächlich empfangene Anzahl = {7}.	Fehler	
BCGEDIVA0158	Doppelte Gruppe im Austausch	Doppelte Gruppe im aktuellen Austausch festgestellt. Gruppenkontrollnummer = {0}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}, Kontrollnummern = {5}.	Fehler	
BCGEDIVA0202	Austauschtrailer fehlt oder ist ungültig	Austauschtrailer fehlt oder ist ungültig. Kontrollnummer des Austauschheaders = {0}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}.	Fehler	
BCGEDIVA0203	Kontrollnummern des Austauschs stimmen nicht überein	Die Kontrollnummern des Austauschs im Header und Trailer stimmen nicht überein. Kontrollnummer des Austauschheaders = {0}, Kontrollnummer des Austauschtrailers = {1}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {2}/{3}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {4}/{5}.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0205	Ungültige Anzahl von Austauschtrailern	Austauschtrailer enthält eine ungültige Anzahl von Gruppen oder Nachrichten. Kontrollnummer des Austauschheaders = {0}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}. Wert im Trailer = {5}, tatsächlich empfangene Anzahl = {6}.	Fehler	
BCGEDIVA0211	Doppelter Austausch	Doppelter Austausch festgestellt. Kontrollnummer des Austauschheaders = {0}, ID/Qualifikationsmerkmal des sendenden Handelspartners = {1}/{2}, ID/Qualifikationsmerkmal des empfangenden Handelspartners = {3}/{4}.	Fehler	
BCGEDIVA0981	Vom Benutzer angegebene Validierungszuordnung konnte nicht gefunden werden	Vom Benutzer angegebene Validierungszuordnung {0} konnte nicht gefunden werden.	Fehler	
BCGEDIVA0982	Validierungszuordnung für das Servicesegment konnte nicht gefunden werden	Validierungszuordnung für das Servicesegment {0} konnte nicht gefunden werden.	Fehler	
BCGEDIVA0983	Validierung für das Servicesegment wird für die Dokumentsyntax nicht unterstützt	Validierung für das Servicesegment wird für die Dokumentsyntax nicht unterstützt.	Fehler	
BCGEDIVA0991	Erforderliche Eigenschaft oder erforderliches Inhaltselement nicht gefunden	Erforderliche Eigenschaft oder Inhaltselement {0} konnte nicht gefunden werden.	Fehler	
BCGEDIVA0992	Keine Nachrichteneigenschaften gefunden	Keine Nachrichteneigenschaften gefunden.	Fehler	

Tabelle 44. EDI-Ereigniscodes und -Nachrichten (Forts.)

EDI-Ereigniscode	Ereignisname	Interne Beschreibung	Wertigkeit	Detaillierte Beschreibung
BCGEDIVA0993	Metadaten nicht gefunden	Metadaten nicht gefunden. Wörterverzeichnis = {0}, Dokumenttyp = {1}, Syntax = {2}.	Fehler	
BCGEDIVA0994	Leere Transaktionsgruppe oder Nachricht	EDI-Transaktionsgruppe oder -Nachricht ist leer.	Fehler	
BCGEDIVA0995	Schwer wiegender Parserfehler	Schwer wiegender Parserfehler.	Fehler	
BCGEDIVA0997	Unbekannte Richtung des Ablaufs	Unbekannte Ablaufrichtung {0} angegeben.	Fehler	
BCGEDIVA0998	Nicht unterstützter Syntaxtyp	Nicht unterstützten Syntaxtyp {0} angegeben.	Fehler	
BCGEDIVA0999	Unbekanntes Objekt empfangen	Unbekanntes Objekt des Typs {0} empfangen.	Fehler	

Anhang C - Komponentenspezifische Systemattribute

Attribute als Umgebungsvariablen von WebSphere Application Server Network Deployment konfigurieren

Auf der Seite **Systemverwaltung** der WebSphere Partner Gateway-Konsole finden Sie die Konfigurationsattribute für bestimmte Unterkomponenten der WebSphere Partner Gateway-Laufzeit. Diese Attribute gelten für alle Instanzen der Unterkomponenten. Weitere Informationen zu den Attributen finden Sie in den Tabellen im Abschnitt „Attributtabellen" auf Seite 259. Es mag Situationen geben, in denen Sie die Werte eines Attributs für eine bestimmte Instanz ändern möchten. So kann es z. B. sinnvoll sein, die Anzahl der Threads zu erhöhen, wenn der Computer, auf dem die Instanz der Komponente ausgeführt wird, über eine höhere CPU-Kapazität verfügt. Gehen Sie wie folgt vor, um den in der WebSphere Partner Gateway-Konsole konfigurierten Wert eines Attributs für eine bestimmte Instanz einer Komponente zu ändern: Erstellen Sie über den Deployment Manager auf der Seite **Systemverwaltung** eine Umgebungsvariable für den Knoten und den Server, auf denen die Komponente ausgeführt wird. Der Wert der Umgebungsvariable hat gegenüber dem in der WebSphere Partner Gateway-Konsole konfigurierten Wert Vorrang. Ausführliche Informationen zu WebSphere-Umgebungsvariablen finden Sie in der Dokumentation zu WebSphere Application Server.

Gehen Sie wie folgt vor, um eine Umgebungsvariable für WebSphere Application Server Network Deployment zu konfigurieren:

1. Öffnen Sie die Administrationskonsole von WebSphere Application Server.
2. Navigieren Sie zu **Umgebung**> **WebSphere-Variablen**.
3. Wählen Sie im Menü den Knoten und den Server aus, für die Sie die Variable hinzufügen.
4. Klicken Sie auf **Neu**.
5. Geben Sie den Eigenschaftsnamen so an, wie er auf der Seite **Systemverwaltung** von WebSphere Partner Gateway angezeigt wird, und legen Sie den Wert fest.
6. Klicken Sie auf **OK**.
7. Speichern Sie die Masterkonfigurationen.

RosettaNet-Attributwerte bearbeiten

Wenn für einen PIP (Partner Interface Process) keine XPath-Abfragen zur Verfügung stehen, werden die in Tabelle 45 aufgelisteten Standard-XPath-Abfragen verwendet, um die entsprechenden Werte zu extrahieren:

Tabelle 45. Standard-XPath-Abfragen

Standard-XPath-Abfragen	Extrahierter Wert

`thisDocumentIdentifier[0]/ProprietaryDocumentIdentifier[0]`
 	
`thisMessageIdentifier[0]/ProprietaryMessageIdentifier[0]`
	Dokument-ID

`thisDocumentGenerationDateTime[0]/DateTimeStamp[0]`
 	
`theMessageDatetime[0]/DateTimeStamp[0]`
 	
`thisMessageDateTime[0]/DateTimeStamp[0]`
	Dokumenterstellungsdatum und Zeitmarke

Tabelle 45. Standard-XPath-Abfragen (Forts.)

Standard-XPath-Abfragen	Extrahierter Wert
`GlobalDocumentFunctionCode[0]`	GlobalFunctionCode

`requestingDocumentIdentifier[0]/ProprietaryDocumentIdentifier[0]`
 	
`WarrantyClaimConfirmData[0]/DocumentReference[0]/ ProprietaryDocumentIdentifier[0]`
 	
`receivedDocumentIdentifier[0]/ProprietaryDocumentIdentifier[0]`
 	
`ReturnProductResource[0]/DocumentReference[0]/ ProprietaryDocumentIdentifier[0]`
 	
`theOffendingDocumentIdentifier[0]/ ProprietaryDocumentIdentifier[0]`
	Kennung des Anforderungsdokuments

`fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/ GlobalPartnerClassificationCode[0]`	Klassifizierungscode des absendenden Partners
`fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/ BusinessDescription[0]/GlobalSupplyChainCode[0]`	Globaler Lieferkettencode des absendenden Partners

`fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/ BusinessDescription[0]/GlobalBusinessIdentifier[0]`
 	
`fromRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/ BusinessDescription[0]/BusinessIdentification[0]/ GlobalBusinessIdentifier[0]`
	Geschäfts-ID des absendenden Partners

`fromRole[0]/PartnerRoleDescription[0]/ GlobalPartnerRoleClassificationCode[0]`	Rolle des absendenden Partners
`toRole[0]/PartnerRoleDescription[0]/ GlobalPartnerRoleClassificationCode[0]`	Rolle des empfangenden Partners
`toRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/ BusinessDescription[0]/GlobalBusinessIdentifier[0]`	Geschäfts-ID des empfangenden Partners
`toRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/ GlobalPartnerClassificationCode[0]`	Klassifizierungscode des empfangenden Partners
`toRole[0]/PartnerRoleDescription[0]/PartnerDescription[0]/ BusinessDescription[0]/GlobalSupplyChainCode[0]`	Globaler Lieferkettencode des empfangenden Partners

Die XSD-basierten PIP-Pakete (XSD - XML Schema Definition Language) enthalten die zugehörigen XPath-Abfragen. Wenn Sie diese Werte anzeigen oder bearbeiten möchten, wählen Sie **Hubadmin** > **Hubkonfiguration** > **Dokumentdefinition** > **Dokumentdefinitionen verwalten** aus. Erweitern Sie auf dieser Seite das Paket "RNIF-Knoten", bis der Aktionsknoten eines PIP erreicht ist (Beispiel: 'Aktion: Benachrichtigungsaktion über aktualisierte Bestellung'). Auf dieser Seite können Sie XPath-Abfragen anzeigen, erstellen und bearbeiten.

Klicken Sie zum Bearbeiten der XPath-Abfrage auf das Symbol **RosettaNet-Attributwerte bearbeiten**, das in der zum PIP gehörenden Spalte **Aktionen** angezeigt wird. Dadurch wird das Fenster mit den RosettaNet-Attributen angezeigt, in dem Sie die XPath-Abfragen anzeigen, hinzufügen und bearbeiten können.

FTP-Verwaltung bearbeiten

Die FTP-Verwaltung verfügt über die folgenden Eigenschaften:

- Listenereigenschaften
- Verbindungseigenschaften
- IP Restrictor

- Ereigniseigenschaften
- Datenbankeigenschaften
- Andere Eigenschaften

Listenereigenschaften :

Der Listener ist die Komponente im FTP-Server, die die Clientverbindungen, die Befehlsausführung und ähnliches überwacht. Die Eigenschaften für diesen Listener gliedern sich in die Eigenschaften des Standardlisteners und die Clientauthentifizierung.

Tabelle 46. Eigenschaften des Standardlisteners

Name der Eigenschaft	Beschreibung
bcg.ftp.config.listeners.default.class	Die konkrete Implementierung des Listeners.
bcg.ftp.config.listeners.default.address	Die IP-Adresse oder der Hostname des Hosts, auf dem der FTP-Server ausgeführt wird.
bcg.ftp.config.listeners.default.port	Der Port des FTP-Servers. Dieser Port gilt für den Standardlistener.
bcg.ftp.config.listeners.default.implicit-ssl	Anstelle von SSL wird FTP verwendet.
bcg.ftp.config.listeners.default.ssl.class	Die Klasse, die SSL verarbeitet.
bcg.ftp.config.listeners.default.ssl.ssl-protocol	Das standardmäßige SSL-Protokoll. Zulässige Werte sind "TLSv1", "SSLv3" und "SSL_TLS".
bcg.config.listeners.default.ssl.client-authentication	Gibt an, ob die Clientauthentifizierung erforderlich ist.
bcg.ftp.config.listeners.default.data -connection.class	Die Klasse, die Datenverbindung verarbeitet.
bcg.ftp.config.listeners.default.data -connection.idle-time	Leerlaufzeit der Verbindung in Sekunden.
bcg.ftp.config.listeners.default.data -connection.active.enable	Gibt an, ob die aktive Verbindung für diesen Listener aktiviert ist.
bcg.ftp.config.listeners.default.data -connection.active.local-address	Die lokale Adresse, die in aktiven Verbindungen überwacht werden soll.
bcg.config.listeners.default.data -connection.active.local-port	Der lokale Port, der für aktive Verbindungen überwacht werden soll.
bcg.ftp.config.listeners.default.data -connection.passive.address	Die Adresse für passives FTP. Dies ist dieselbe Adresse wie die IP-Adresse, an der der FTP-Server ausgeführt wird.
bcg.ftp.config.listeners.default.data -connection.passive.ports	Passive Ports.
bcg.ftp.config.listeners.default.data -connection.ssl.class	Die für SSL verwendete Klasse.

Tabelle 47. Clientauthentifizierung

Name der Eigenschaft	Beschreibung
bcg.ftp.config.listeners.clientauth.class	Die konkrete Implementierung des Listeners.
bcg.ftp.config.listeners.clientauth.address	Die IP-Adresse oder der Hostname des Hosts, auf dem der FTP-Server ausgeführt wird.
bcg.ftp.config.listeners.clientauth.port	Der Port des FTP-Servers. Dieser Port gilt für den Standardlistener.
bcg.ftp.config.listeners.clientauth.implicit-ssl	Anstelle von SSL wird FTP verwendet.
bcg.ftp.config.listeners.clientauth.ssl.class	Die Klasse, die SSL verarbeitet.
bcg.ftp.config.listeners.clientauth.ssl.ssl-protocol	Das standardmäßige SSL-Protokoll. Zulässige Werte sind "TLSv1", "SSLv3" und "SSL_TLS". **Anmerkung:** Im FIPS-Modus kann optional 'TLSv1' als Wert für die Eigenschaft 'bcg.ftp.config.listeners.default.ssl.ssl-protocol' gesetzt werden, um Unklarheiten zu vermeiden. Verwenden Sie dazu die folgenden Schritte: Wählen Sie in WebSphere Partner Gateway Console **Systemverwaltung** > **FTP-Verwaltung** > **Listenereigenschaften** > **Standard** aus. Im Nicht-FIPS-Modus kann der Wert auf “SSL_TLS” gesetzt werden, wodurch die SSLv3- und die TLSv1-Unterstützung aktiviert wird.
bcg.config.listeners.clientauth.ssl.client-authentication	Gibt an, ob die Clientauthentifizierung erforderlich ist.
bcg.ftp.config.listeners.clientauth.data-connection.class	Die Klasse, die Datenverbindung verarbeitet.
bcg.ftp.config.listeners.clientauth.data-connection.idle-time	Leerlaufzeit der Verbindung in Sekunden.
bcg.ftp.config.listeners.clientauth.data-connection.active.enable	Gibt an, ob die aktive Verbindung für diesen Listener aktiviert ist.
bcg.ftp.config.listeners.clientauth.data-connection.active.local-address	Die lokale Adresse, die in aktiven Verbindungen überwacht werden soll.
bcg.config.listeners.clientauth.data-connection.active.local-port	Der lokale Port, der für aktive Verbindungen überwacht werden soll.
bcg.ftp.config.listeners.clientauth.data-connection.passive.address	Die PASV-Adresse (Adresse für passives FTP).
bcg.ftp.config.listeners.clientauth.data-connection.passive.ports	Passive Ports.
bcg.ftp.config.listeners.clientauth.data-connection.ssl.class	Die für SSL verwendete Klasse.

Verbindungseigenschaften:

Alle Verbindungseigenschaften können bearbeitet werden.

Tabelle 48. Verbindungseigenschaften

Name der Eigenschaft	Beschreibung
bcg.ftp.config.connection-manager.max-connection	Die maximal zulässige Anzahl der Verbindungen.
bcg.ftp.config.connection-manager.max-login	Die maximal zulässige Anzahl der Anmeldungen.
bcg.ftp.config.connection-manager.default-idle-time	Die standardmäßige Leerlaufzeit in Sekunden, nach deren Ablauf eine hergestellte Verbindung getrennt werden soll.
bcg.ftp.config.connection-manager.timeout-poll-interval	Das Intervall für Zeitlimits, in dem der Sendeaufrufthread ausgeführt werden soll, der Verbindungen im Leerlauf erfasst.

Eigenschaften von IP Restrictor:

Diese Eigenschaften enthalten eine Liste mit IP-Adressen, deren Zugriff eingeschränkt ist.

Tabelle 49. Eigenschaften von IP Restrictor

Name der Eigenschaft	Beschreibung
IP Pattern	Eine gültige IP-Adresse muss im Format x.x.x.x angegeben werden. Alternativ hierzu kann auch ein Platzhalterzeichen (*) angegeben werden.
Permission	Die dieser IP-Adresse zugeordnete Berechtigung.

Ereigniseigenschaften

Tabelle 50. Ereigniseigenschaften

Name der Eigenschaft	Beschreibung
bcg.config.ftpserver.FTPSerializeFileInterval	Das Intervall in Millisekunden, nach dessen Ablauf die aufgelaufenen Ereignisse in das Dateisystem serialisiert werden.
bcg.config.ftpserver.eventPersistThreads	Diese Eigenschaft gibt die Anzahl der Threads im Thread-Pool an, die zum Ausführen der Datenbankaktualisierungen verwendet werden sollen.
bcg.config.ftpserver.FTPEventThreshold	Die maximale Anzahl der FTP-Ereignisse, die gesammelt werden können, bevor sie in der Datenbank oder im Dateisystem gespeichert werden.
bcg.config.ftpserver.FTPEventStoreInterval	Das Intervall, nach dem FTP-Ereignisse in der Datenbank oder im Dateisystem gespeichert werden.

Tabelle 50. Ereigniseigenschaften (Forts.)

Name der Eigenschaft	Beschreibung
bcg.config.ftpserver.FTPEventLoggingLevel	Diese Eigenschaft hat den Wert 0,1,2 oder 3. Der Wert entspricht den Ereignisstufen ("Debugging/Information", "Warnung", "Fehler" und "Kritisch"). Der Standardwert für diese Eigenschaft ist 2. Dies bedeutet, dass standardmäßig alle Fehler und kritischen Ereignisse protokolliert werden. Diese Werte werden verwendet, um die Stufe der FTP-Ereignisse festzulegen, die protokolliert werden sollen.

Datenbankeigenschaften:

Tabelle 51. Datenbankeigenschaften

Name der Eigenschaft	Beschreibung
Hostname	Der Host, auf dem die Datenbank installiert ist.
User / Password	Der Benutzername und das Kennwort zum Herstellen der Verbindung zur Datenbank.
Port	Der Port an dem der Datenbankserver empfangsbereit ist.

Andere Eigenschaften:

Tabelle 52. Andere Eigenschaften

Name der Eigenschaft	Beschreibung
bcg.ftp.config.rootdirectory	Dies ist das FTP-Stammverzeichnis. Wenn ein Benutzer erstellt und ein Verzeichnis zugeordnet wird, wird das Benutzerverzeichnis in diesem Stammverzeichnis erstellt.

SFTP-Verwaltung bearbeiten

Die SFTP-Verwaltung verfügt über die folgenden Eigenschaften:

Tabelle 53. SFTP-Eigenschaften

Name der Eigenschaft	Beschreibung
bcg.sftp.port	Der Port, an dem der SFTP-Server gestartet wird.
max-auth-requests	Die maximal zulässige Anzahl der Anmeldeversuche am SFTP-Server.

Tabelle 53. SFTP-Eigenschaften (Forts.)

Name der Eigenschaft	Beschreibung
auth-timeout	Die zulässige Leerlaufzeit bei der Anmeldung am SFTP Server.

Attributtabellen

- Attribute, die von einer oder von mehreren Komponenten gemeinsam genutzt werden - Tabelle 54 auf Seite 260.
- Attribute für die Verarbeitung von EDI-Dokumenten - Tabelle 55 auf Seite 264.
- Attribute zur Konfiguration der Konsolenkomponente - Tabelle 56 auf Seite 266.
- Attribute zur Konfiguration von JMS für die Konsolenkomponente - Tabelle 57 auf Seite 268.
- Attribute zur Konfiguration des RosettaNet-Simulators - Tabelle 58 auf Seite 269.
- Attribute zur Konfiguration der Alertengine - Tabelle 59 auf Seite 270.
- Attribute zur Konfiguration der AS-Statusengine - Tabelle 60 auf Seite 271
- Attribute zur Konfiguration der BPE - Tabelle 61 auf Seite 272.
- Attribute zur Konfiguration der Signalverarbeitung - Tabelle 62 auf Seite 273.
- Attribute zur Konfiguration der synchronen Verarbeitung durch die BPE und die DAE - Tabelle 63 auf Seite 273.
- Attribute zur Konfiguration des Zustellmanagers - Tabelle 64 auf Seite 274.
- Attribute zur Konfiguration von JMS für die Document Manager-Komponente - Tabelle 65 auf Seite 275.
- Attribute zur Konfiguration des Document Manager-Paketierungsprozesses - Tabelle 66 auf Seite 277.
- Attribute zur Konfiguration der RosettaNet-Verarbeitung durch Document Manager - Tabelle 67 auf Seite 278.
- Attribute zur Konfiguration der Sicherheit in Document Manager - Tabelle 68 auf Seite 280.
- Attribute zur Konfiguration von JMS für die Empfängerkomponente - Tabelle 69 auf Seite 280.
- Attribute zur Konfiguration der Verarbeitung synchroner Antworten durch die Empfängerkomponente - Tabelle 70 auf Seite 281.
- Attribute zur Konfiguration der von der Empfängerkomponente verwendeten Verzeichnisnamen - Tabelle 71 auf Seite 281.
- Attribute zur Konfiguration verschiedener Aspekte der Empfängerkomponente - Tabelle 72 auf Seite 282.
- Attribute zur Konfiguration der Zusammenfassungssteuerkomponente als Unterkomponente von Document Manager - Tabelle 73 auf Seite 282.
- Attribute zur Konfiguration der Projektträgersteuerkomponente als Unterkomponente von Document Manager - Tabelle 74 auf Seite 282.
- Attribute zur Konfiguration der Archivierungsfunktion als Unterkomponente von Document Manager - Tabelle 75 auf Seite 283.
- Attribute zur Konfiguration der Verarbeitung von ebMS-Dokumenten - Tabelle 76 auf Seite 283.
- Attribute zur Konfiguration des zuverlässige Nachrichtenaustauschs (RM) als Unterkomponente von Document Manager - Tabelle 77 auf Seite 284.

- Attribute zur Konfiguration der Ereignisengine als Unterkomponente von Document Manager - Tabelle 78 auf Seite 284.
- Attribute zur Konfiguration des Archivierungs- und Bereinigungsprozesses - Tabelle 80 auf Seite 285.
- Erforderliche Attribute für die Konfiguration von WebSphere Transformation Extender - Tabelle 81 auf Seite 285

Tabelle 54. Attribute, die von einer oder von mehreren Komponenten gemeinsam genutzt werden

Eintrag	Standardwert	Mögliche Einstellungen	Beschreibung
bcg.ldap.containerauth	False	Boolescher Wert "True" oder "False"	Wenn dieser boolesche Wert auf "True" gesetzt ist, gibt dies an, dass die Benutzer mithilfe der lokalen Datenbank von WebSphere Partner Gateway authentifiziert werden. Ist dieser boolesche Wert auf "False" gesetzt, wird mithilfe von JAAS auf ein Unternehmensbenutzerregister zugegriffen.
bcg.ldap.jaaslogin	WSLogin	Zeichenfolge, die die Anmelde-ID enthält	Gibt den Namen der Anmeldekonfiguration des JAAS-Systems oder der Anwendung an.
bcg.receiver.persistpath	*<hub-install-stammverz>*/common/router_in/	Dateisystempfad	Hier speichert der Empfänger eingehende Dokumente, damit sie von der DAE übernommen werden können.
bcg.receiver.sync.persistpath	*<hub-install-stammverz>*/common/sync_in	Dateisystempfad	Hier speichert der Empfänger synchrone Dokumente, damit sie von der DAE (Document Acquisition Engine - Dokumentübernahme-Engine) übernommen werden können.
bcg.receiver.signal.persistpath	*<hub-install-stammverz>*/common/signal_in	Dateisystempfad	Hier speichert der Empfänger RosettaNet-Signale.
bcg.vms_inbound_directory.main	*<hub-install-stammverz>*/common/router_in	Dateisystempfad	Eingangsverzeichnis des Hauptrouters.
bcg.bpe_temp_directory.main	*<hub-install-stammverz>*/common/data	Dateisystempfad	Datenverzeichnis des Hauptrouters.
bcg.vms_inbound_directory.signal	*<hub-install-stammverz>*/common/signal_in	Dateisystempfad	Eingangsverzeichnis des Signalrouters.
bcg.bpe_temp_directory.signal	*<hub-install-stammverz>*/common/data	Dateisystempfad	Datenverzeichnis des Signalrouters.

Tabelle 54. Attribute, die von einer oder von mehreren Komponenten gemeinsam genutzt werden (Forts.)

Eintrag	Standardwert	Mögliche Einstellungen	Beschreibung
bcg.vms_inbound_directory.synchronous	*<hub-install-stammverz>*/common/sync_in	Dateisystempfad	Eingangsverzeichnis des synchronen Routers.
bcg.bpe_temp_directory.synchronous	*<hub-install-stammverz>*/common/data	Dateisystempfad	Datenverzeichnis des synchronen Routers.
bcg.scheduler_initial_pool_size	10	Positive ganze Zahl	Dieser Wert gibt die Anfangsgröße des Pools der Threads an. Dies ist eine Eigenschaft des Schedulermanagers.
bcg.scheduler_max_pool_size	50	Positive ganze Zahl	Dieser Wert gibt die maximale Größe des Pools der Threads an. Dies ist eine Eigenschaft des Schedulermanagers.
bcg.global.common.introduce.document.transport	JMS	Zeichenfolge, die entweder 'FileSystem' oder 'JMS' enthält	Legt den Dokumentweiterleitungstransport zum internen Verschieben von Dokumenten vom Empfänger an Document Manager fest.
bcg.global.common.introduce.document.transport.unavailable.timeout	60000	Positive ganze Zahl	Falls JMS-Transport für die interne Weiterleitung zwischen dem Empfänger und Document Manager verwendet wird, ist dies der Zeitlimitwert, mit dem festgestellt wird, ob bei der Verwendung dieses Transports ein Fehler aufgetreten ist.
bcg.global.common.deletetempfiles	Yes	Yes oder No	Wenn der Eigenschaftswert bcg.global.common.deletetempfiles auf **Yes** gesetzt wurde, werden temporäre Dateien, die von WebSphere Partner Gateway erstellt wurden, gelöscht. Wenn der Wert auf **No** gesetzt wurde, löscht das System die temporäre Dateien nicht.
bcg.messagestore.threshold	100000	Dateigröße in Byte	Der Wert des Attributs bcg.messagestore.threshold gibt den Schwellenwert für die Inhaltsdateigröße in Byte an. Wird dieser Wert überschritten, wird keine Nachrichtenspeicheroperation ausgeführt.
bcg.event_log_exclude	Kein Standardwert	Zeichenfolge	Listet die durch Kommata getrennten Ereigniscodes auf, die nicht verarbeitet werden müssen.

Tabelle 54. Attribute, die von einer oder von mehreren Komponenten gemeinsam genutzt werden (Forts.)

Eintrag	Standardwert	Mögliche Einstellungen	Beschreibung
bcg.CRLDir	*<hub-install-stammverz>*/common/security/crl/	Zeichenfolge mit einem Verzeichnispfad	Pfad des Verzeichnisses, in dem die Dateien der Zertifikats-widerrufslisten (CRLs) gespeichert sind.
bcg.checkRevocationStatus	TRUE	Zeichenfolge, boolescher Wert TRUE oder FALSE	Der Wert "TRUE" führt dazu, dass die CRL geprüft wird, bevor beim Senden des Dokuments oder beim Herstellen der Verbindung zum SSL-Server über den FTP-Scripting-Empfänger das Dokument signiert oder die Signatur, die Verschlüsselung, die Entschlüsselung, das SSL-Clientzertifikat oder das Serverzertifikat überprüft wird.
bcg.http.SSLDebug	FALSE	Zeichenfolge, boolescher Wert TRUE oder FALSE	Für dieses Attribut generiert der Wert "TRUE" SSL-Debugprotokolle. Die Debuginformationen werden in die Datei SystemOut.log in das Verzeichnis *<hub-install-stammverz>*/wasND/Profiles/bcgprofile/logs/*<profilname>* gestellt.
bcg.rosettanet.encrypt.CertDbRefreshInterval	60000	Ganze Zahl	CRLs und VTP-Zertifikate (VTP Virtual Test Partner) werden nach diesem Intervall periodisch geladen; das Intervall ist in Millisekunden angegeben. Obwohl im Namen "Rosettanet" enthalten ist, gilt dieses Attribut für alle Protokolle.
bcg.certs.vtp.CertificateDir	*<hub-install-stammverz>*/common/security/vtp	Zeichenfolge mit einem Dateiverzeichnispfad	Verzeichnis, das Zertifikate für die VTP-Signaturvalidierung und -Verschlüsselung enthält. Der Wert sollte dem Wert in bcg.console.certs.vtp.CertificateDir entsprechen, der in den allgemeinen Attributeinstellungen der Konsole festgelegt wird.

Tabelle 54. Attribute, die von einer oder von mehreren Komponenten gemeinsam genutzt werden (Forts.)

Eintrag	Standardwert	Mögliche Einstellungen	Beschreibung
bcg.build_complete_certpath	true	Zeichenfolge, boolescher Wert TRUE oder FALSE	"TRUE" bedeutet, dass im Falle einer Kette von Zertifikaten der Zertifizierungspfad bis zum Root-Zertifikat erstellt wird. Dadurch werden sämtliche Zertifikate in der Kette geprüft. Der Wert "False" bedeutet, dass der Zertifikatspfad nur bis zum Ausstellerzertifikat erstellt und überprüft wird. Es wird empfohlen, diesen Wert auf "True" zu setzen, da Sie auch die CA-Zertifikate widerrufen können. **Anmerkung:** Sie können das CA-Zertifikat nur widerrufen, wenn Sie es für die Handelsgemeinschaft erstellt haben.

Tabelle 55. Attribute für die Verarbeitung von EDI-Dokumenten

Eintrag	Standardwert	Mögliche Einstellungen	Beschreibung
`traceLevel.All`	0	Ganze Zahl zwischen 0 und 2	Dieses bestimmte Attribut (All) betrifft alle Traceerstellungen. Wenn Sie ein fokussiertes Trace wünschen, richten Sie die einzelnen Traces für die gewünschten Funktionen ein. 0 bedeutet, dass keine Protokolle für die zugehörige Funktionalität geschrieben werden sollen. 1 bedeutet, dass nur Fehlerprotokolle in die Tracedatei geschrieben werden sollen. 2 bedeutet, dass alle Protokolle (Fehler und Debugging) in die Tracedatei geschrieben werden sollen. Beispiel: traceLevel.Transformation = 1 bedeutet, dass nur die Fehler, die während der EDI-Transformation generiert wurden, in die Traceprotokolle geschrieben werden sollen. Die Traceprotokolle befinden sich in *<hub-install-stammverz>*`/wasND/Profiles/bcgprofile/logs/bcgdocmgr/`. Der Standardname der Tracedatei ist `bcg_router.log`.
`traceLevel.Transformation`	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu `traceLevel.All`.
`traceLevel.Validation`	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu `traceLevel.All`.
`traceLevel.Enveloper`	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu `traceLevel.All`.
`traceLevel.Deenveloper`	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu `traceLevel.All`.
`traceLevel.EDI-Parser`	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu `traceLevel.All`.
`traceLevel.XML-Parser`	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu `traceLevel.All`.
`traceLevel.ROD-Parser`	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu `traceLevel.All`.

Tabelle 55. Attribute für die Verarbeitung von EDI-Dokumenten (Forts.)

Eintrag	Standardwert	Mögliche Einstellungen	Beschreibung
traceLevel.EDI-Serializer	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.XML-Serializer	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.ROD-Serializer	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.EDI-Splitter	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.XML-Splitter	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.ROD-Splitter	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.ROD-Scanner	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.FTP-Scripting	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.IBMVanAckProcessor	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.EDIAckProcessor	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
traceLevel.Utility	0	Ganze Zahl zwischen 0 und 2	Siehe Beschreibung zu traceLevel.All.
transcript.file.option	N	Y oder N	Wenn die Option Y ausgewählt ist, werden die Aufzeichnungsdateien im aktuellen Arbeitsverzeichnis generiert, das im Ordner "transcripts" angegeben ist.
database.encoding	UTF-8	Eine Dateicodierung	Die in der Datenbank für DB2 verwendete Codierung. Der Wert muss "UTF-8" sein, da der in DB2 verwendete codierte Zeichensatz UTF-8 ist.

Tabelle 56. Attribute zur Konfiguration der Konsolenkomponente

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
`bcg.console.outbound.gatewayDirectory`	*<hub-install-stammverz>*`/common/gateways`	Dateisystempfad	Stammverzeichnis im gemeinsamen Dateisystem, unter dem sich die Unterverzeichnisse für die Verwaltung der Ziele (Gateways) befinden.
`bcg.console.db.debugLevel`	0	Boolesche 0 oder 1	Eine binäre Einstellung, bei der 0 und 1 zum Aktivieren (1) oder Inaktivieren (0) des Debug-Trace der Datenbank verwendet werden.
`bcg.console.appserver.mgmt.pool.maxsize`	20	Ganze Zahl	Interne Einstellung, nur für IBM.
`bcg.console.EAIDocDir`	Dokumente	Gültiger Verzeichnisname	Der Name des Unterverzeichnisses, das im Stammverzeichnis erstellt wird, welches Sie für die Empfängerinstanz eines Dateisystems angeben.
`bcg.console.specialChars`	`!#:;\\& /?.,`	Zeichenliste	Eine bestimmte Gruppe von Zeichen, die in einigen über die Konsole konfigurierten Feldern nicht verwendet werden können. Sie werden für die Validierung der Anmeldedaten des Partners sowie der Daten des Empfängers und des Ziels (des Gateways) verwendet, die über die Konsole eingegeben werden. **Anmerkung:** Es kann sinnvoll sein, diese Werte für die Internationalisierung zu ändern, je nach der Sprache des Betriebssystems und den Vorgaben für Verzeichnisnamen.

Tabelle 56. Attribute zur Konfiguration der Konsolenkomponente (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.console.specialCharsDir	!#;& ?.,	Zeichenliste	Eine bestimmte Gruppe von Zeichen, die in einigen Verzeichnisnamen, die in der Konsole angegeben werden, nicht verwendet werden können. **Anmerkung:** Es kann sinnvoll sein, diese Werte für die Internationalisierung zu ändern, je nach der Sprache des Betriebssystems und den Vorgaben für Verzeichnisnamen.
bcg.console.file.encodings	us-ascii|ascii|646|iso_646.irv:1983|ansi_x3.4-1968| iso646-us|default|ascii7| utf-8|utf8| unicode-1-1-utf-8|utf-16|utf16|unicode|sjis|\u30B7\u30D5\u30C8\u7B26\u53F7\u5316\u8868\u73FE|pck|gb18030|big5| windows-1255|windows-1256|ISO8859-8|IBM856|ISO8869-6|IBM1046	Liste der IANA-Dateicodierungsnamen (IANA - Internet Assigned Numbers Authority), die von der Klasse sun.io.CharacterEncoding unterstützt werden Namen werden durch ein vertikales Balkenzeichen getrennt	Die Dokumentanzeige generiert eine Liste der Java-Aliasnamen, die den IANA-Codierungen entspricht und zeigt diese Liste an. Der Benutzer kann die Dateicodierungen für die Verarbeitung der Dateien festlegen. Beachten Sie, dass ein Java-Aliasname auf mehrere IANA-Namen angewendet werden kann. Die Standardeinstellung umfasst IANA-Werte für viele der am häufigsten verwendeten Codierungen.
bcg.console.help.host	localhost	Hostname oder IP-Adresse	Der Hostname oder die IP-Adresse des Hilfesystemservers, der von der Konsole verwendet wird.
bcg.console.help.port	58080	Ganzzahlige Portnummer	Der Port des Hilfesystemservers, über den Hilfe angefordert wird.
bcg.console.version	Version 6.2.0.0.273	Zeichenfolgewert	Eine Zeichenfolge, die die Version der verwendeten Konsole angibt.

Tabelle 57. Attribute zur Konfiguration von JMS für die Konsolenkomponente

Eintrag	Standardwert	Mögliche Einstellungen	Beschreibung
bcg.jms.queue.factory	jms/bcg/cf/CONCF	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.topic.factory	jms/bcg/cf/CONCF	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.jndi_factory	com.ibm.websphere.naming.WsnInitialContextFactory	Klassenname	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.context_url	corbaloc:iiop:localhost:58809	URL	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.topic.name	jms/bcg/topic/reloadCacheT	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.retry_connect_interval	300000	Ganze Zahl	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.console.jmsPosterInstance	com.ibm.bcg.shared-.event.MQSeriesPoster	Klassenname	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.reloadCache.name	Kein Standardwert	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.oaq_log_q	jms/bcg/queue/datalogQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.

Tabelle 58. Attribute zur Konfiguration des RosettaNet-Simulators

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
`bcg.console.certs.vtp.Certificate-Dir`	*<hub-install-stammverz>*`/common/security/vtp`	Lokaler Dateisystempfad	Vollständiger Pfad des Verzeichnisses, in dem die Dateien `.p8` und `.der` für den RosettaNet-Simulator enthalten sind. Wenn der Pfad oder die Namen der Zertifikatsdatei und der Datei für den privaten Schlüssel nicht korrekt sind, wird ein Fehler in der Protokolldatei `SystemErr.log` in der Konsole angezeigt. Dieser Fehler hat keine negativen Auswirkungen auf den Betrieb des Hubs und kann als Warnung eingestuft werden. Der Wert dieses Attributs sollte mit den Einstellungen des Attributs "bcg.certs.vtp.CertificateDir" übereinstimmen, das in den Sicherheitseinstellungen von Document Manager festgelegt wird.
`bcg.console.certs.vtp.Certificate`	Kein Standardwert	Dateiname	Der Name der Zertifikatsdatei (DER, Binärformat), die einen vom Simulator verwendeten öffentlichen Schlüssel enthält. Der Name muss die Dateierweiterung enthalten.
`bcg.console.certs.vtp.PrivateKey`	Kein Standardwert	Dateiname	Der Name der Datei für den privaten Schlüssel (PKCS8, Binärformat), die vom Simulator verwendet wird. Der Name muss die Dateierweiterung enthalten.
`bcg.console.certs.vtp.Passwd`	Kein Standardwert	Dateiname	Das Kennwort, mit dem auf den Schlüssel in der Datei PKCS8 zugegriffen wird
`bcg.console.certs.vtp.VerifySig`	FALSE	TRUE | FALSE	Boolescher Wert, mit dem angegeben wird, ob die Signaturprüfung ausgeführt wird, wenn der Simulator verwendet wird.
`bcg.console.vtp.RouterIn`	*<hub-install-stammverz>*`/common/router_in`	Dateisystempfad	Das Verzeichnis im gemeinsamen Dateisystem, das für die Weitergabe von Dokumenten an Document Manager verwendet wird.

Tabelle 59. Attribute zur Konfiguration der Alertengine

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.alertQReceiver.maxRetries	100	Ganze Zahl	Maximale Anzahl der vom Alertempfänger versuchten Wiederholungen.
bcg.alertQReceiver.retryInterval	60000	Ganze Zahl	Intervall in Millisekunden zwischen den einzelnen Wiederholungen.
bcg.volumeAlertScheduler.allowanceForProcessingReceivedDocInMins	10	Ganze Zahl	Zeit in Minuten nach der Endzeit des Volumenalerts für das Aufzeichnen von Dokumenten, die empfangen wurden, bevor der Volumenalert ausgewertet wurde. Dadurch wird sichergestellt, dass alle während des Intervalls empfangenen Dokumente berücksichtigt werden.
bcg.alertNotifications.maxNotificationsInInterval	10	Ganze Zahl	Zur Vermeidung exzessiver E-Mail-Benachrichtigungen werden verschiedene Eigenschaften verwendet. Wenn für denselben Alert mehr Benachrichtigungen (maxNotificationsInInterval) im festgelegten Zeitintervall (maxNotificationIntervalInMins) vorhanden sind, werden Alerts in die Warteschliefe gestellt und nach einer bestimmten Minutenanzahl (heldAlertsBatchTimeInMins) stapelorientiert verarbeitet, bis für das Attribut minNotificationQuietIntervalInMins keine Alerts dieses Typs mehr empfangen werden.
bcg.alertNotifications.maxNotificationIntervalInMins	30	Ganze Zahl	Siehe Beschreibung für maxNotificationsInInterval.
bcg.alertNotifications.minNotificationQuietIntervalInMins	30	Ganze Zahl	Siehe Beschreibung für maxNotificationsInInterval.
bcg.alertNotifications.heldAlertsBatchTimeInMins	30	Ganze Zahl	Siehe Beschreibung für maxNotificationsInInterval.
bcg.alertNotifications.mailHost	unknown	Das Wort "unknown" (unbekannt), eine IP-Adresse oder ein Hostname	Die IP-Adresse oder der Hostname des SMTP-Mailhosts, über den Alertbenachrichtigungen gesendet werden.

Tabelle 59. Attribute zur Konfiguration der Alertengine (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.alertNotifications.mailFrom	unknown@ unknown.com	E-Mail-Adresse	Die E-Mail-Adresse, die für den Absender von Alertbenachrichtigungen verwendet wird.
bcg.alertNotifications.mailReplyTo	unknown@ unknown.com	E-Mail-Adresse	Die E-Mail-Adresse, die als Antwortadresse für Alertbenachrichtigungen verwendet wird.
bcg.alertNotifications. mailEnvelopeFrom	unknown@ unknown.com	E-Mail-Adresse	Die E-Mail-Adresse, die für Antworten im Falle falscher E-Mail-Adressen verwendet werden soll.
bcg.alert.eventGenerator.schedule	13 1 CertificateExpiration	Minuten (in ganzen Zahlen) Stunden (in ganzen Zahlen) Alertname	Mehrere Datensätze sollten durch das Zeichen "|" getrennt werden. Die Einträge der einzelnen Datensätze bestehen aus (erste ganze Zahl) Minuten, (zweite ganze Zahl) Stunden und (Zeichenfolge) dem Alertnamen. Diese Einträge müssen durch mindestens ein Leerzeichen voneinander getrennt werden.
bcg.VolumeAlertScheduler.scheduleTime	10	Ganze Zahl	Nach der jeweils angegebenen Anzahl von Sekunden generiert der Volumenalertgenerator die Volumenalerts.
bcg.BatchAlertScheduler.scheduleTime	10	Ganze Zahl	Nach der jeweils angegebenen Anzahl von Sekunden generiert der Batch-Alertgenerator die Batch-Alerts.
bcg.NotificationAlertScheduler- .scheduleTime	10	Ganze Zahl	Nach der jeweils angegebenen Anzahl von Sekunden generiert der Benachrichtigungsalertgenerator die Benachrichtigungsalerts.

Tabelle 60. Attribute zur Konfiguration der AS-Statusengine

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.asstate.thread_count	1	Ganze Zahl	Anzahl Threads, die von der AS-Statusengine verwendet werden.

Tabelle 60. Attribute zur Konfiguration der AS-Statusengine (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.asstate.batchSize	1	Ganze Zahl	Die Batchgröße ist immer auf 1 gesetzt. Die Änderung dieses Attributs hat keinerlei Auswirkungen, und das Attribut ist für künftige Zwecke reserviert. Es kann als Anzahl von Zeilen interpretiert werden, die beim Auslösen der Statusengine zurückgegeben werden.
bcg.asstate.runinterval	60000	Ganze Zahl	Zeitintervall in Millisekunden, mit dem festgelegt wird, wie oft die AS-Statusengine Anforderungen verarbeitet.

Tabelle 61. Attribute zur Konfiguration der BPE

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.dae.main.maxLockAge	180000	Ganze Zahl	Maximale Sperrendauer für den Hauptordner in Millisekunden.
bcg.dae.main.maxfiles.perPass	5	Ganze Zahl	Maximale Anzahl zu verarbeitender Dateien pro Abfrageintervall für den Hauptordner.
bcg.docmgr.channelCache.maxSize	20	Ganze Zahl	Wenn ein Dokument verarbeitet wird, wird nach einer Partnerverbindung für das Dokument gesucht. Die Konfigurationsdaten dieser Partnerverbindung werden in der Laufzeitumgebung zwischengespeichert. Dieses Attribut bestimmt die maximale Anzahl der Partnerverbindungen, die jeweils zwischengespeichert werden können. Sobald die maximale Anzahl erreicht ist, werden ältere Daten gelöscht und die neueren Partnerverbindungsdaten hinzugefügt.
bcg.in_thread_count.main	2	Ganze Zahl	Anzahl Threads für die Hauptrouterverarbeitung eingehender Nachrichten.
bcg.inbound_poll_interval.main	1000	Ganze Zahl	Zeit in Millisekunden zwischen zwei Verzeichnisüberprüfungen.
bcg.bpe_max_file_size	0	Ganze Zahl	Maximale Dateigröße in Byte. Der Wert Null (0) bedeutet, dass kein Grenzwert zwingend ist.

Tabelle 61. Attribute zur Konfiguration der BPE (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.inbound_files_per _pass.main	5	Ganze Zahl	Maximale Anzahl zu berücksichtigender Dateien pro Überprüfung.
bcg.duplicate.DupField1 bis bcg.duplicate.DupField10	x-aux-system-msg-id (Dies ist der Standardwert für 'DupField1').	Zeichenfolge	Der Name eines Nachrichtenheaders, dessen Wert die eindeutige Identität einer Nachricht darstellt. Er kann mit anderen Headerwerten kombiniert werden, um eine Nachricht eindeutig zu identifizieren.

Tabelle 62. Attribute zur Konfiguration der Signalverarbeitung

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.dae.signal.maxLockAge	180000	Ganze Zahl	Maximale Sperrendauer für den Ordner für Signalnachrichten in Millisekunden.
bcg.dae.signal.maxfiles.perPass	5	Ganze Zahl	Maximale Anzahl zu verarbeitender Dateien pro Abfrageintervall für den Ordner für Signalnachrichten.
bcg.inbound_poll_interval.signal	1000	Ganze Zahl	Zeit in Millisekunden zwischen zwei Verzeichnisüberprüfungen.
bcg.in_thread_count.signal	2	Ganze Zahl	Anzahl der eingehenden Threads für den Signalrouter.
bcg.inbound_files_per_pass.signal	5	Ganze Zahl	Maximale Anzahl zu berücksichtigender Dateien pro Überprüfung.

Tabelle 63. Attribute zur Konfiguration der synchronen Verarbeitung durch die BPE und die DAE

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.dae.synchronous.maxLockAge	180000	Ganze Zahl	Maximale Sperrendauer für den Ordner für synchrone Nachrichten in Millisekunden.
bcg.dae.synchronous.maxfiles-.perPass	5	Ganze Zahl	Maximale Anzahl zu verarbeitender Dateien pro Abfrageintervall für den Ordner für synchrone Nachrichten.
bcg.inbound_poll_interval. synchronous	1000	Ganze Zahl	Zeit in Millisekunden zwischen zwei Verzeichnisüberprüfungen.

Tabelle 63. Attribute zur Konfiguration der synchronen Verarbeitung durch die BPE und die DAE (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.in_thread_count.synchronous	2	Ganze Zahl	Anzahl der eingehenden Threads für den synchronen Router.
bcg.inbound_files_per_pass. synchronous	5	Ganze Zahl	Maximale Anzahl zu berücksichtigender Dateien pro Überprüfung.

Tabelle 64. Attribute zur Konfiguration des Zustellmanagers

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.delivery.gatewayDirectory	*<hub-install-stammverz>*/common/gateways	Zeichenfolge	Stammverzeichnis, unter dem sich die Dateien und Unterverzeichnisse befinden, mit denen Ziele verwaltet werden.
bcg.delivery.smtpHost	$ROUTER.DM. SMTP_RELAY$	IP-Adresse/ Hostname	Host, der verwendet wird, wenn Dokumente mit SMTP übergeben werden.
bcg.delivery.smtpHostPort	$ROUTER.DM. SMTP_RELAY.PORT$	Ganze Zahl	Der verwendete Port auf dem SMTP-Mail-Host.
bcg.delivery.responseDir	*<hub-install-stammverz>*/common/sync_in	Zeichenfolge, die einen Verzeichnispfad enthält	Die Position des Verzeichnisses der synchronen Antwort.
bcg.delivery.msMaxFileLockLife	180000	Ganze Zahl	Maximale Zeit in Millisekunden zum Sperren einer Datei.
bcg.delivery.threadPoolMaxThreads	50	Ganze Zahl	Maximale Größe des Thread-Pools, der vom Zustellmanager verwendet wird.
bcg.delivery.gatewayMaxThreads	20	Ganze Zahl	Maximale Anzahl von Zielthreads.
bcg.delivery. gwTransportMaxRetries	3	Ganze Zahl	Anzahl der vom Zustellmanager-Framework für jede Wiederholung auf der Zielebene versuchten Wiederholungen. Dies ist eine globale Einstellung, die für alle Ziele gilt. Außerdem wird jedes Ziel mit einer eigenen Wiederholungsanzahl konfiguriert, die immer dann zum Einsatz kommt, wenn das Framework eine Wiederholung versucht.

Tabelle 64. Attribute zur Konfiguration des Zustellmanagers (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.delivery. gwTransportRetryInterval	3000	Ganze Zahl	Intervall in Millisekunden zwischen zwei Wiederholungsversuchen des Zustellmanagers.
bcg.delivery.numberOfLoggers	10	Ganze Zahl	—
bcg.delivery.jmstimeout	60000	Ganze Zahl	Wenn der JMS-Transport zur Übergabe von Dokumenten verwendet wird, wird über dieses Zeitlimit (angegeben in Millisekunden) festgestellt, ob ein Konnektivitätsproblem besteht oder nicht.
bcg.http.socketTimeout	120000	Ganze Zahl	Zeitlimit für HTTP-Socket in Millisekunden.
bcg.http.version	1.1	Zeichenfolge	HTTP-Version, die vom Zustellmanager verwendet wird.
bcg.router.ipv6.address	Kein Standardwert	Zeichenfolge	Wenn der Computer, auf dem Document Manager installiert ist, mit IPv6 konfiguriert wurde und die Dokumente über ein Gateway gesendet werden, das auf der Internetprotokollversion 6 (IPv6) basiert, muss die IPv6-Adresse des Computers hier angegeben werden.
bcg.delivery.loggerTimeOut	10000	Ganze Zahl	—

Tabelle 65. Attribute zur Konfiguration von JMS für die Document Manager-Komponente

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.jms.queue.factory	jms/bcg/cf/DOCMGRCF	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.topic.factory	jms/bcg/cf/DOCMGRCF	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.jndi_factory	com.ibm.websphere. naming. WsnInitialContextFactory	Klassenname	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.

Tabelle 65. Attribute zur Konfiguration von JMS für die Document Manager-Komponente (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.jms.context_url	corbaloc:iiop: localhost:58809	URL	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM. Port 58809 ist der Standardport für die Installation im einfachen Modus. Ihre Installation ist möglicherweise anders.
bcg.oaq_bpe_in.main	jms/bcg/queue/ main_InboundQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.oaq_bpe_out.main	jms/bcg/queue/ deliveryManagerQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.oaq_bpe_in.signal	jms/bcg/queue/ signal_InboundQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.oaq_bpe_out.signal	jms/bcg/queue/ deliveryManagerQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.oaq_bpe_in.synchronous	jms/bcg/queue/ sync_InboundQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.oaq_bpe_out.synchronous	jms/bcg/queue/ deliveryManagerQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.delivery.queue	jms/bcg/queue/ deliveryManagerQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.alertQueue.queue	jms/bcg/queue/alertQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.eventAlertQReceiver.queue	jms/bcg/queue/ alertEventQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.syncdelivery.queue	jms/bcg/queue/ syncDeliveryManagerQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.logReceiver.queue	jms/bcg/queue/datalogQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.

Tabelle 65. Attribute zur Konfiguration von JMS für die Document Manager-Komponente (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.dberrors.queue	jms/bcg/queue/ datalogErrorQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.retry_connect_interval	300000	Ganze Zahl	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.connect_pool_elements	2	Ganze Zahl	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.connect_max_pool_elements	100	Ganze Zahl	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.

Tabelle 66. Attribute zur Konfiguration des Document Manager-Paketierungsprozesses

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
Wbipackaging_version	1	1.0 und 1.1	Wird verwendet für das Erstellen des XML-Transportumschlags für Back-End-Integration. Version 1.0 ist für Version 4.2.2 FP1 und älter. Version 1.1 ist für 4.2.2 FP2 und neuer. Version 1.1 enthält die Inhalt-ID, die den Anhängen zugeordnet ist.
DBProcDebug	1	Ganze Zahl: entweder 0 oder 1	Eine binäre Einstellung, bei der 0 und 1 zum Aktivieren (1) oder Inaktivieren (0) des Datenbank-Debugging verwendet werden. In den Debugging-Protokollen werden der Prozedurname und die an ihn übermittelten Parameter angezeigt.
GlobalStateEngInstanceId	Bcg	Zeichenfolge	Eingehende und ausgehende AS-Dokumente werden in der Datenbank mit GlobalStateEngInstanceId protokolliert. Die AS-Statusengine ruft die Datenbank auf, um die letzte Detailzeile der ältesten Headerzeile abzurufen, die verarbeitet werden muss. Dafür verwendet sie GlobalStateEngInstanceId und generiert die MDN (Message Disposition Notification). Dieser Parameter wird auch für Wiederholungen verwendet.

Tabelle 66. Attribute zur Konfiguration des Document Manager-Paketierungsprozesses (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.ediint.reportingUA	WPG	Zeichenfolge	Mit "Reporting UA" ist der Benutzeragent gemeint, der die MDN angibt.
bcg.ediint.retryWaitTmMS	5000	Ganze Zahl	Wenn bei ausgehenden AS-Nachrichten (mit asynchroner MDN) die MDN nicht empfangen wurde, wiederholt die AS-Engine den Versuch nach dieser Anzahl an Millisekunden.
bcg.maxBatchSize	1000	Ganze Zahl	Maximale Anzahl zu berücksichtigender und zu verarbeitender Dateien als Batch durch ein Gateway.

Tabelle 67. Attribute zur Konfiguration der RosettaNet-Verarbeitung durch Document Manager

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.rosettanet.retryWaitTmMS	5000	Ganze Zahl	Wiederholungsintervall in Millisekunden.
bcg.rosettanet.strictBoundaryParse	FALSE	Zeichenfolge, boolescher Wert TRUE oder FALSE	Gibt an, ob die Grenzwerte von MIME-Multipartnachrichten (Rosettanet) strikt syntaktisch analysiert werden sollen. Der Standardwert ist "TRUE".
bcg.rosettanet.mimeBoundaryValidate	FALSE	Zeichenfolge, boolescher Wert TRUE oder FALSE	Wenn dieser Wert auf TRUE gesetzt wurde, erfolgt eine strukturelle Auswertung der MIME-Multipartnachricht (Rosettanet). Der Standardwert ist "FALSE".
bcg.rosettanet.globalUsageCode	Literal	Zeichenfolgewert von “Literal” oder Sonstigem	Wenn dieser Wert "Literal" ist, müsste der HTTP-Header von x-aux-production wörtlich "Production" oder "Test" sein. Wenn der Wert nicht "Literal" ist (z. B. wenn Sie ihn auf einen Leerwert setzen), müsste der HTTP-Header von x-aux-production "TRUE" oder "FALSE" sein. Bei allen Werten muss die Groß-/Kleinschreibung nicht beachtet werden.

Tabelle 67. Attribute zur Konfiguration der RosettaNet-Verarbeitung durch Document Manager (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.rosettanet.defaultUsageCdOnErr	1	Zeichenfolgewert 1 oder 0, der als boolescher Wert interpretiert wird	Wenn der HTTP-Header von x-aux-production nicht "Production", "Test", "True" oder "False" lautet und wenn diese Eigenschaft auf “1” gesetzt wurde, wird standardmäßig der im Attribut bcg.rosettanet.defaultGlbUsageCd festgelegte Wert angenommen.
bcg.rosettanet.defaultGlbUsageCd	Test	Zeichenfolge	Globaler Standardverwendungscode.
bcg.rosettanet. useBuilderProcessInstanceId	1	Zeichenfolgewert 1 oder 0, der als boolescher Wert interpretiert wird	Wenn dieser Wert gleich 1 ist, sollte das Erstellungsprogramm eine ID im HTTP-Header von x-aux-process-instance-id bereitstellen, die als Prozessinstanz-ID für eine ausgehende Anforderung verwendet wird.
bcg.rosettanet. genProcessInstanceIdOnError	1	Zeichenfolgewert 1 oder 0, der als boolescher Wert interpretiert wird	Wenn die vom Erstellungsprogramm bereitgestellte Prozessinstanz-ID aus irgendeinem Grund falsch ist, generieren Sie eine neue Prozessinstanz-ID, wenn dieser Wert 1 ist.
bcg.rne.inbound_poll_interval	10000	Ganze Zahl	Abfrageintervall in Millisekunden der RosettaNet-Engine.
bcg.rne.in_thread_count	2	Ganze Zahl	Anzahl der Threads, die von der RosettaNet-Engine zur Verarbeitung eingehender Dokumente verwendet wird.
bcg.rne.work_size	50	Ganze Zahl	Die Anzahl der PIP-Nachrichten, die pro Abfrageintervall verarbeitet wird.
bcg.0A1.fromContactName	$ROUTER. CONTACT_NAME$	Zeichenfolge	Name des 0A1-Kontakts.
bcg.0A1.fromEMailAddr	$ROUTER. CONTACT. MAIL_FROM$	Zeichenfolge	E-Mail des 0A1-Kontakts.
bcg.0A1.fromPhoneNbr	$ROUTER. CONTACT. PHONE_NO$	Zeichenfolge	Telefonnummer des 0A1-Kontakts.
bcg.0A1.fromFaxNbr	$ROUTER. CONTACT.FAX_NO$	Zeichenfolge	Faxnummer des 0A1-Kontakts.

Tabelle 67. Attribute zur Konfiguration der RosettaNet-Verarbeitung durch Document Manager (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.rnif.pip.twoaction.correlation	documentid	Zeichenfolge	Der Wert dieser Eigenschaft fungiert als Korrelationsparameter zwischen der 1-Aktion und der 2-Aktion eines PIPs mit zwei Aktionen.

Tabelle 68. Attribute zur Konfiguration der Sicherheit in Document Manager

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.rosettanet.signature. DigestAlgorithm	SHA1	SHA1 oder MD5	Dieser Algorithmus wird verwendet, um Nachrichtenauszüge zu generieren. Obwohl im Namen "rosettanet" enthalten ist, wird dieses Attribut für RNIF und AS verwendet. Es wird nicht für ebMS verwendet. Es gilt für alle Flüsse, die PKCS7 zum Signieren von Dokumenten verwenden. ebMS verwendet keine PKCS7-Signaturen.
bcg.rosettanet.signature. RejectIfFailVal	TRUE	Zeichenfolge, boolescher Wert TRUE oder FALSE	Der Wert "TRUE" bedeutet, dass ein Dokument abgelehnt wird, wenn die Signaturprüfung fehlschlägt.
bcg.rosettanet.signature. VerifySigner	TRUE	Zeichenfolge, boolescher Wert TRUE oder FALSE	Der Wert "TRUE" bedeutet, dass der Unterzeichner geprüft wird, sobald die Signatur geprüft worden ist. "FALSE" bedeutet, dass der Unterzeichner nicht geprüft wird.
bcg.rosettanet.encrypt.Algorithm	3des	3des oder des oder aes oder rc2-40	Verschlüsselungsalgorithmus, der für RosettaNet-Nachrichten verwendet wird. Diese Eigenschaft ist für alle Protokolle gültig.

Tabelle 69. Attribute zur Konfiguration von JMS für die Empfängerkomponente

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.jms.queue.factory	jms/bcg/cf/RCVRCF	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.topic.factory	jms/bcg/cf/RCVRCF	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.jndi_factory	com.ibm.websphere. naming. WsnInitialContextFactory	Klassenname	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.

Tabelle 69. Attribute zur Konfiguration von JMS für die Empfängerkomponente (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.jms.context_url	corbaloc:iiop:localhost:58809	URL	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM. Port 58809 ist der Standardport für die Installation im einfachen Modus. Ihre Installation ist möglicherweise anders.
bcg.oaq_log_q	jms/bcg/queue/datalogQ	JNDI-Name	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.retry_connect_interval	300000	Ganze Zahl	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.connect_pool_elements	2	Ganze Zahl	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.
bcg.jms.connect_max_pool_elements	100	Ganze Zahl	Interne Einstellung, die die Kommunikation zwischen Komponenten betrifft. Nur für IBM.

Tabelle 70. Attribute zur Konfiguration der Verarbeitung synchroner Antworten durch die Empfängerkomponente

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.receiver.sync.responseURL	/bcgsyncreceiver/SyncResponse	URI	Interne Empfänger-URI für die Übergabe von synchronen Antworten.
bcg.receiver.sync.responseURL.port	58081	Ganze Zahl	Portnummer, die für die synchrone Antwort-URI verwendet wird.

Tabelle 71. Attribute zur Konfiguration der von der Empfängerkomponente verwendeten Verzeichnisnamen

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.receiver.configpath	*<hub-install-stammverz>*/common/receiver/config	Zeichenfolge mit einem Verzeichnispfad	Adresse der XML-Konfigurationsdatei des Empfängers, die verwendet wird, wenn die Datenbank nicht verfügbar ist.
bcg.vms_receiver_reject_dir	*<hub-install-stammverz>*/common/receiver/reject	Zeichenfolge mit einem Verzeichnispfad	Verzeichnis 'reject' des Empfängers.

Tabelle 71. Attribute zur Konfiguration der von der Empfängerkomponente verwendeten Verzeichnisnamen (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.vms_receiver_tmp_dir	*<hub-install-stammverz>*/common/receiver/tmp	Zeichenfolge mit einem Verzeichnispfad	Temporäres Speicherverzeichnis des Empfängers. Empfänger, die andere Transportmethoden wie JMS, POP3 und HTTP anstelle von Dateitransporten verwenden, stellen die Inhaltsdateien mit der Erweiterung ".vcd" an diese Position. Nur für IBM.

Tabelle 72. Attribute zur Konfiguration verschiedener Aspekte der Empfängerkomponente

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.receiver.ipv6	Kein Standardwert	IPv6-Adresse	Die von den Empfängern verwendete IPv6-Adresse. Sie wird benötigt, wenn der Computer, der der Host für die Empfängerkomponente ist, IPv6 verwendet.

Tabelle 73. Attribute zur Konfiguration der Zusammenfassungssteuerkomponente als Unterkomponente von Document Manager

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.summary.processingInterval	15	Ganze Zahl	Zeitintervall in Minuten, mit dem festgelegt wird, wie oft die Verarbeitung der Ereigniszusammenfassung erfolgen soll.
bcg.summaryEng.thread_count	1	Ganze Zahl	Die Anzahl der Threads, die die Ereigniszusammenfassung vorbereiten.

Tabelle 74. Attribute zur Konfiguration der Projektträgersteuerkomponente als Unterkomponente von Document Manager

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.sponsor.inbound_poll_interval	10000	Ganze Zahl	Legt das Intervall in Millisekunden für die Abfrage der Tabelle fest, mit der Ereignisbenachrichtigungsdokumente generiert werden (hauptsächlich XML-Ereignisse). Weitere Informationen zu XML-Ereignissen finden Sie im *Abschnitt "XML-Ereignis (XMLEvent)" des Handbuchs Unternehmensintegration*.

Tabelle 74. Attribute zur Konfiguration der Projektträgersteuerkomponente als Unterkomponente von Document Manager (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.sponsor.in_thread_count	1	Ganze Zahl	Anzahl der vom Projektträger verwendeten Threads für die Generierung von Ereignisbenachrichtigungsdokumenten.
bcg.sponsor.work_size	10	Ganze Zahl	Anzahl der pro Arbeitsgang aus der Datenbank abgerufenen Zeilen für die Generierung von Ereignisbenachrichtigungsdokumenten.

Tabelle 75. Attribute zur Konfiguration der Archivierungsfunktion als Unterkomponente von Document Manager

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.archiver.maxSubVolFiles	70000	Ganze Zahl	Maximale Anzahl der Unterdatenträger unter einem Datenträger.
bcg.archiver.runinterval	600	Ganze Zahl	Zeitintervall in Sekunden, mit dem festgelegt wird, wie oft die Verarbeitung des Archivierungsfunktionsdienstes erfolgt.

Tabelle 76. Attribute zur Konfiguration der Verarbeitung von ebMS-Dokumenten

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.ebXML.language	en-US	Zeichenfolge	Die in ebXML-SOAP-Nachrichten verwendete Sprache.
bcg.AddKeyInfo	true	Boolescher Wert TRUE oder FALSE	Dieses Attribut gilt nur während der Signatur einer ebXML-Nachricht. Wenn der Wert dieses Attributs "FALSE" ist, enthält das Signaturelement nicht das KeyInfo-Element. Das Element 'KeyInfo' enthält den öffentlichen Schlüssel, der für die Signatur verwendet wird.
bcg.ebXML.version	2.0	Zeichenfolge	Die ebXML-Version, mit der Nutzdaten als ebXML-Nachricht verpackt werden. Derzeit wird nur die Version 2.0 unterstützt.

Tabelle 76. Attribute zur Konfiguration der Verarbeitung von ebMS-Dokumenten (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.ebms.xsd.schemaName	ebXMLSchema.xsd	Zeichenfolge mit Dateiname	Der XSD-Name für die Validierung einer eingehenden ebXML-Nachricht. Der XSD-Name wird bei der Installation in der Datenbank mit dem Standardnamen vorausgefüllt. Wenn der Benutzer die XSD-Datei ändert und sie unter einem anderen Namen in die Datenbank hochlädt, sollte dieser Name auch als Wert für das Attribut verwendet werden.
bcg.ebms.validate	False	Boolescher Wert TRUE oder FALSE	Dieses Attribut legt fest, ob eine ebXML-SOAP-Nachricht mit dem XSD-Namen abgeglichen werden soll, der vom Attribut 'schemaName' bestimmt wurde. Der Wert "TRUE" bedeutet, dass alle eingehenden ebXML-Nachrichten validiert werden.

Tabelle 77. Attribute zur Konfiguration des zuverlässigen Nachrichtenaustauschs (RM) als Unterkomponente von Document Manager

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.rm.pollInterval	300000	Ganze Zahl	Zeitintervall in Millisekunden, mit dem festgelegt wird, wie oft die Verarbeitung des zuverlässigen Nachrichtenaustausches erfolgen soll.
bcg.rm.thread_count	3	Ganze Zahl	Die Anzahl der Threads, die vom zuverlässigen Nachrichtenaustausch verwendet wird.

Tabelle 78. Attribute zur Konfiguration der Ereignisengine als Unterkomponente von Document Manager

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.eventeng.alertscache.size	100	Ganze Zahl	Die Größe des Alert-Cache.

Tabelle 79. Sonstige EDI-Eigenschaften

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
transcript.file.option	N	Y oder N	Wenn die Option "Y" (ja) ausgewählt ist, werden die Aufzeichnungsdateien im aktuellen Arbeitsverzeichnis generiert, das im Ordner 'transcripts' angegeben ist.
PageThreshold	1000	0–n	Diese Eigenschaft steuert die Auslagerung sich wiederholender Nachrichtenstrukturen in den EDI-Komponenten. Setzen Sie sie auf null, um die Auslagerung zu inaktivieren. Andere Werte als null geben die maximale Anzahl der Vorkommen eines Elements an, bevor die Auslagerung erfolgen soll. Die Auslagerung reduziert die Speicherbelegung, erhöht allerdings die Verarbeitungszeit.

Tabelle 80. Attribute zur Konfiguration des Archivierungs- und Bereinigungsprozesses

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
bcg.archive.maxThreads	4	Ganze Zahl	Die Archivierung von Dateien erfolgt als Multithreadoperation. In WebSphere Partner Gateway 6.2.1 wird die neue Eigenschaft "bcg.archive.maxThreads" mit dem Standardwert 4 eingeführt. Mit diesem Wert wird die maximale Anzahl der Threads angegeben, die für die Archivierung zulässig sind.

Tabelle 81. Attribute zur Konfiguration der Eigenschaften von WebSphere Transformation Extender

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
wtx.rmihostname	localhost	Ganze Zahl	Die IP-Adresse oder der Hostname des WebSphere Transformation Extender-Servers.
wtx.rmiport	2500	Ganze Zahl	Die Nummer des RMI-Ports für WebSphere Transformation Extender.
rmiuseserver	No	Boolescher Wert: 'Yes' (Ja) oder 'No' (Nein)	Dieses Attribut wird auf 'Yes' gesetzt, wenn der Innovationsstil der erforderlichen WebSphere Transformation Extender-Zuordnung 'RMI' ist.

Tabelle 81. Attribute zur Konfiguration der Eigenschaften von WebSphere Transformation Extender (Forts.)

Eintrag	Standardwert	Mögliche Einstellung	Beschreibung
`bcg.wtx.mapLocation`	<hub-install-stammverz>/bcghub-distrib/common/maps	Ganze Zahl	Die Standardposition der Zuordnung.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder andere Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Burlingame Laboratory Director
IBM Burlingame Laboratory

577 Airport Blvd., Suite 800
Burlingame, CA 94010
USA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Dokument aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Die oben genannten Erklärungen bezüglich der Produktstrategien und Absichtserklärungen von IBM stellen die gegenwärtige Absicht von IBM dar, unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ

Diese Veröffentlichung enthält Musteranwendungsprogramme, die in Quellensprache geschrieben sind und Programmiertechniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Musterprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der

Anwendungsprogrammierschnittstelle konform sind, für die diese Musterprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

Informationen zu Programmierschnittstellen

Die ggf. bereitgestellten Informationen zu Programmierschnittstellen sollen Ihnen bei der Erstellung von Anwendungssoftware unter Verwendung dieses Programms helfen. Mit allgemeinen Programmierschnittstellen können Sie Anwendungssoftware schreiben, die die Services aus den Tools dieses Programms abrufen. Diese Informationen können jedoch auch Angaben über Diagnose, Bearbeitung und Optimierung enthalten. Die Informationen zu Diagnose, Bearbeitung und Optimierung sollten Ihnen bei der Fehlerbehebung für die Anwendungssoftware helfen.

Achtung: Verwenden Sie diese Informationen zu Diagnose, Bearbeitung und Optimierung nicht als Programmierschnittstelle, da Änderungen vorbehalten sind.

Marken und Servicemarken

Folgende Namen sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern:

IBM	DB2	i5/OS	MQIntegrator	Informix
Das IBM Logo	DB2 Universal Database	IMS	OS/400	MVS
AIX	Domino	iSeries	Passport Advantage	WebSphere
CICS	IBMLink	Lotus	SupportPac	z/OS
CrossWorlds		Lotus Notes	Tivoli	

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

MMX, Pentium und ProShare sind Marken oder eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern.

Solaris, Java und alle auf Java basierenden Marken und Logos sind Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

WebSphere Partner Gateway Enterprise Edition und Advanced Edition enthalten Software, die vom Eclipse Project (www.eclipse.org) entwickelt wurde.

Index

E

F

G

H

I

J

K

L

N

P

Q

R

S

T

U

V

W

X

Z