IBM Cúram Social Program Management

Cúram Portlet Deployment Guide For WebSphere Portal Server

Version 6.0.5

IBM Cúram Social Program Management

Cúram Portlet Deployment Guide For WebSphere Portal Server

Version 6.0.5

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen in „Bemerkungen" auf Seite 21 gelesen werden.

Überarbeitung: Mai 2013

Diese Ausgabe bezieht sich auf IBM Cúram Social Program Management v6.0.5 und alle nachfolgenden Releases, sofern nicht anderweitig in neuen Auusgaben angegeben.

Licensed Materials - Property of IBM.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellen

Kapitel 1. Einführung

1.1 Einführung

In diesem Handbuch wird der Prozess der Konfiguration von Cúram-Portlets sowie die Implementierung dieser Portlets auf einer Portalseite beschrieben, die sich auf einem Portalserver befindet.

1.2 Voraussetzungen

Zur erfolgreichen Implementierung und Verwaltung von Cúram-Portlets müssen die folgenden Voraussetzungen erfüllt sein:

- Der Benutzer muss mit der Konfiguration von IBM® WebSphere Application Server und/oder IBM WebSphere Portal Server vertraut sein.
- Der Benutzer muss das Dokument *Cúram Third-Party Tools Installation Guide for Windows* gelesen haben, um zu wissen, welche Software zum Konfigurieren von Cúram-Portlets erforderlich ist.
- Grundlegende Kenntnisse im Umgang mit der Cúram-Anwendung und der Cúram-Anwendungsentwicklung.

1.3 Zielgruppe

Das vorliegende Dokument ist ein technisches Handbuch für Benutzer, die für die Verwaltung von Ressourcen auf einem Anwendungsserver und/oder Portalserver verantwortlich sind.

1.4 Kapitel in diesem Handbuch

In der folgenden Liste werden die Kapitel dieses Handbuchs beschrieben:

Übersicht über Cúram-Portlets
Dieses Kapitel enthält eine Übersicht über den Aufbau von Cúram-Portlets.

Portlet-WAR-Datei erstellen
In diesem Kapitel wird beschrieben, wie die Cúram-Portlets konfiguriert werden und die Datei `CuramPortlets.war` erstellt wird, bevor die Cúram-Portlets implementiert werden können.

Cúram-Portlets implementieren
In diesem Kapitel wird beschrieben, wie der Inhalt der Cúram-Portlets konfiguriert und die Cúram-Portlets implementiert werden.

Konfiguration von SSO-Cúram-Portlets
In diesem Anhang wird beschrieben, wie der Portalserver manuell konfiguriert und die Cúram-Anwendung manuell implementiert wird, damit der Benutzer SSO-Portlets (SSO - Single Sign-on) aktivieren kann.

Kapitel 2. Übersicht über Cúram-Portlets

2.1 Cúram-Portlets

Cúram-Portlets sind Portlets, die Informationen zu einer Cúram-Anwendung anzeigen. Es besteht - mit einigen geringfügigen Unterschieden - eine Eins-zu-Eins-Zuordnung zwischen den Inhalten bestimmter Cúram-Pods und Cúram-Portlets. Deshalb gibt es eine enge Beziehung zwischen den in Cúram-Portlets und Cúram-Pods angezeigten Inhalten. Weitere Informationen zu Pods finden Sie im Handbuch *Cúram Pod Developers Guide*. Cúram-Portlets wurden in Übereinstimmung mit der JSR 286-Spezifikation entwickelt. Das heißt allerdings nicht, dass Cúram-Portlets momentan über alle JSR 286-Features wie beispielsweise die Interportletkommunikation verfügen.

Es ist wichtig zu beachten, dass Cúram-Portlets nicht sofort implementiert werden können. Es gibt einige wichtige Schritte, die ausgeführt werden müssen, bevor Cúram-Portlets auf einer Portalseite implementiert werden können. Diese Schritte werden in den nachfolgenden Kapiteln beschrieben. Wenn die Cúram-Portlets darüber hinaus SSO-konform sein müssen (siehe 2.2, „Zugriffssteuerung für Cúram-Portlets"), sind die unter „Konfiguration von SSO-Cúram-Portlets", auf Seite 9 beschriebenen Anweisungen zu befolgen.

2.2 Zugriffssteuerung für Cúram-Portlets

Es gibt derzeit zwei Möglichkeiten, wie der Zugriff auf Cúram-Portlets gesteuert werden kann:

- **SSO-Cúram-Portlets**

  Lesen Sie die Informationen unter Single Sign On, um weitere Details zur SSO-Spezifikation zu erfahren. Wenn der Benutzer hier eine neue Portalsitzung startet (durch Anmeldung), muss er sich *nicht* an jedem Cúram-Portlet auf einer Portalseite anmelden, nachdem die Portalseite mit Cúram-Portlets zum ersten Mal geladen wurde.
- **Nicht-SSO-Cúram-Portlets**

  Hier *muss* sich der Benutzer beim Start einer neuen Portalsitzung (durch Anmeldung) an jedem Cúram-Portlet auf einer Portalseite anmelden, nachdem die Seite zum ersten Mal für die Verwendung der Portlets geladen wurde. Dabei wird vorausgesetzt, dass der Benutzer innerhalb derselben Browsersitzung noch nicht an der Cúram-Anwendung angemeldet ist. Weitere Informationen zu Browsersitzungen und zum Sitzungsmanagement der Cúram-Anwendung finden Sie im Kapitel zum Sitzungsmanagement im Handbuch *Cúram Web Client Reference Manual*.

2.3 Derzeitige Einschränkungen für Cúram-Portlets

Für Cúram-Portlets gelten momentan die folgenden Einschränkungen:

- **Lokalisierung**

  Cúram-Portlets werden momentan nur in englischer Sprache unterstützt.
- **Unterstützung für Web-Browser**

  Cúram-Portlets werden momentan von den Web-Browsern unterstützt, die von der Cúram-Anwendung unterstützt werden. Informationen darüber, welche Versionen dieser Browser unterstützt werden, finden Sie im Dokument *Cúram v6 Supported Prerequisites*.

Kapitel 3. Portlet-WAR-Datei erstellen

3.1 Cúram-Portlets konfigurieren

SSO-Cúram-Portlets konfigurieren: Wenn SSO-Cúram-Portlets erforderlich sind, muss die Cúram-Anwendung (IBM Cúram Social Program Management) manuell konfiguriert und auf dem Portalserver implementiert werden. Anweisungen hierzu finden Sie unter „Konfiguration von SSO-Cúram-Portlets", auf Seite 9. In allen anderen Fällen ist eine auf einem Anwendungsserver implementierte Cúram-Anwendung ausreichend. Weitere Einzelheiten hierzu finden Sie im Kapitel zur *Implementierung* im Handbuch *Cúram Deployment Guide for WebSphere Application Server*.

Die Cúram-Portlets müssen konfiguriert werden, bevor die Datei `CuramPortlets.war` erstellt wird. Die Portlets können durch Aktualisierung der entsprechenden Eigenschaftendateien in der Client-Kernkomponente konfiguriert werden.[1]

3.1.1 Cúram-Portlets konfigurieren

Anhand des Werts für den Eigenschaftsschlüssel 'portlet.ids' in der Datei `PortletConfig.properties` wird konfiguriert, welche Portlets in der Datei `CuramPortlets.war` gepackt werden. Der Wert dieser Eigenschaft muss so formatiert werden, dass die folgenden Bedingungen erfüllt sind:

- **Der Wert muss eine durch Kommas begrenzte Zeichenfolge sein.**

  Es muss sich um eine durch Kommas begrenzte Zeichenfolge handeln, wobei jeder Abschnitt der Zeichenfolge der ID (Kennung) eines Cúram-Pods entspricht.
- **Die zugehörigen durch Kommas begrenzten Unterzeichenfolgen müssen einer Eigenschaftendatei zugeordnet sein.**

  Die Werte der einzelnen durch Kommas begrenzten Unterzeichenfolgen werden einer Eigenschaftendatei im Verzeichnis `PortletConfig/resources` zugeordnet.

Wenn der Wert der Eigenschaft 'portlet.ids' diese Bedingungen nicht erfüllt, tritt bei der Erstellung der Datei `CuramPortlets.war` ein Fehler auf. Der Wert dieser Eigenschaft umfasst standardmäßig die vollständige Liste der unterstützten Cúram-Portlets. Es wird empfohlen, den Standardwert dieser Eigenschaft nicht zu aktualisieren. Ferner wird empfohlen, die Eigenschaftendateien im Verzeichnis `resources` in der Installation unverändert zu belassen, auch wenn der Wert der Eigenschaft 'portlet.ids' geändert wird.

3.1.2 Basis-URL in Cúram-Portlets konfigurieren

Die Basis-URL ist Teil der absoluten URL (Uniform Resource Locator), die von den einzelnen Portlets für den Zugriff auf die Seiten in der Cúram-Anwendung verwendet wird. Die Basis-URL ist für alle Cúram-Portlets gleich. Weitere Informationen zur URL-Spezifikation finden Sie in RFC 3986. Anhand des Werts für den Eigenschaftsschlüssel 'base.url' in der Datei `PortletConfig.properties` wird die Basis-URL für Cúram-Portlets konfiguriert.

Der Standardwert für den Eigenschaftsschlüssel 'base.url' ist **https://localhost:9044/Curam/**. Die Basis-URL für Cúram-Portlets kann wie folgt konfiguriert werden:

- **Schema/Protokoll**

  Dies ist der erste Teil des Eigenschaftswerts. Damit wird das Protokoll konfiguriert, das für den Zugriff auf Seiten in der Anwendung über ein Cúram-Portlet verwendet wird. Aus dem Standardwert geht

1. Derzeit müssen zum Konfigurieren von Cúram-Portlets die Eigenschaftendateien im Verzeichnis webclient/components/core/PortletConfig aktualisiert werden. Beachten Sie, dass die Aktualisierung der Eigenschaftendateien auf diese Weise in Konflikt mit der Strategie hinsichtlich der Anpassung von Dateien in der angepassten Komponente stehen. Dies ist eine Einschränkung, die in einem zukünftigen Release behoben wird.

hervor, dass der Wert **https** enthalten ist, der ein Portlet durch Verwendung von Hypertext Transfer Protocol über Secure Sockets Layer (HTTPS) für den sicheren Zugriff auf die Cúram-Anwendung konfiguriert. Es wird dringend empfohlen, diesen Wert nicht zu ändern.

- **Domäne**

  Mit der Domäne wird der Hostname oder die IP-Adresse des Servers konfiguriert, auf dem das WebSphere-System ausgeführt wird und die Cúram-Anwendung implementiert wurde. Die Standarddomäne ist „localhost" (siehe oben). Die Domäne sollte vollständig qualifiziert sein, wenn der Standardwert nicht verwendet wird (z. B. server1.xxx.com).

- **Portnummer**

  Die Portnummer muss mit der Portnummer des Hosts für die Cúram-Anwendung übereinstimmen. Wenn dieser Teil der URL nicht in den konfigurierten Eigenschaftswert einbezogen wird, wird die Standardportnummer `80` verwendet.

- **Anwendungsname**

  Dieser Teil der Basis-URL stellt die Anwendung gemäß dem Kontextstammverzeichnis der Anwendung bei der Implementierung der Cúram-Anwendung auf einem Host dar.

3.1.3 Anzeigemerkmale der einzelnen Cúram-Portlets konfigurieren

Jede Eigenschaftendatei im Verzeichnis `PortletConfig/resources` wird jedem der Cúram-Portlets zugeordnet, die in der WAR-Datei gepackt sind. Daher kann mithilfe der Eigenschaften in diesen Eigenschaftendateien die Art und Weise konfiguriert werden, wie ein bestimmtes Cúram-Portlet angezeigt wird. Die Eigenschaftsschlüssel, die mit „javax" beginnen, werden zum Konfigurieren von Titeltext und Bezeichnungen für das Portlet verwendet und in der Portletspezifikation angegeben. Weitere Informationen finden Sie in JSR 286. Über den Wert des Eigenschaftsschlüssels 'portlet.height' wird die Höhe des Cúram-Portlets konfiguriert. Alle Eigenschaften in den einzelnen Eigenschaftendateien im Verzeichnis `PortletConfig/resources` sind obligatorisch.

3.2 WAR-Datei erstellen

Erstellen Sie die Datei `CuramPortlets.war`, indem Sie **`build portlet-war`** im Verzeichnis `installationsverzeichnis/webclient` ausführen.

Die Datei `CuramPortlets.war` wird im Verzeichnis `installationsverzeichnis/webclient/build/CuramPortlets` generiert.

Kapitel 4. Cúram-Portlets implementieren

4.1 Inhalt des Cúram-Portlets konfigurieren

Nachdem die Datei `CuramPortlets.war` generiert wurde, muss der Inhalt der Cúram-Portlets konfiguriert werden, bevor die Implementierung erfolgen kann.

In den folgenden Schritten wird beschrieben, wie der Inhalt eines Cúram-Portlets konfiguriert werden kann:

1. Melden Sie sich an der Verwaltungsanwendung an.
2. **Navigieren Sie zu 'Personalisierte Pod-Seiten'.**

   Wählen Sie den Link „Personalisierte Pod-Seiten" aus der Kategorie „Benutzerschnittstelle" im Verknüpfungsbereich aus.
3. **Konfigurieren Sie eine persönliche Seite.**

   Wählen Sie die Aktionsschaltfläche „Neue personalisierte Seite" für die Seite aus. Daraufhin wird eine Modaldialogseite mit einem Fortschrittsbalken des Assistenten angezeigt.

   Für den Fortschrittsbalken des Assistenten auf der Modaldialogseite muss eine Reihe von Schritten wie folgt ausgeführt werden:

   - **Seiten-ID**

     Geben Sie im ersten Schritt des Assistenten die Seiten-ID ein, die für das zu konfigurierende Cúram-Portlet angegeben wurde. Wenn beispielsweise der Inhalt des Portlets `QuickLinksPortlet` konfiguriert wird (gemäß dem Wert des Eigenschaftsschlüssels 'portlet.ids' in der Datei `PortletConfig.properties`), muss in das bereitgestellte Texteingabefeld „QuickLinksPortlet" eingegeben werden. Siehe Liste der Cúram-Portlet-IDs in Tabelle 1.
   - **Benutzerrolle**

     Wählen Sie im zweiten Schritt des Assistenten über das Optionsfeld die Option „SUPERROLE" aus.
   - **Verfügbare Pods**

     Im dritten Schritt des Assistenten müssen Sie den entsprechenden Pod aus einer Liste auswählen (durch Aktivierung des entsprechenden Kontrollkästchens), damit der korrekte Podinhalt in einem bestimmten Cúram-Portlet angezeigt wird. In der folgenden Tabelle wird beschrieben, welcher Pod-Name basierend auf dem zu konfigurierenden Cúram-Portlet (nach ID) ausgewählt werden muss:

Tabelle 1. Auswahl von Cúram-Pod

Cúram-Portlet-ID	Cúram-Pod-Name
MyTasksPortlet	Meine Aufgaben
QuickLinksPortlet	Quick Links
MyAppointmentsPortlet	Eigene Termine
WorkQueuesPortlet	Gruppenpostfächer
RecentNotiPortlet	Letzte Benachrichtigungen
OrgSummaryPortlet	Zusammenfassung – Organisation
MyCurrentCasesPortlet	Meine aktuellen Fälle
MyTasksChartPortlet	Diagramm 'Eigene Aufgaben'
CaseloadSummaryPortlet	Meine Fallzusammenfassung

   - **Standardpods**

     Wählen Sie im vierten Schritt des Assistenten die angezeigte Option durch Aktivierung des Kontrollkästchens aus.

- **Seitenlayout**

  Geben Sie im letzten Schritt des Assistenten den Wert 1 in das Texteingabefeld ein und klicken Sie auf die Schaltfläche „Speichern", um die Konfiguration für das Portlet abzuschließen.

  Layoutprobleme: Wenn ein anderer Text als 1 in das Texteingabefeld eingegeben wird, treten bei der Implementierung der Cúram-Portlets Layoutprobleme auf.

4.2 Benutzer und Gruppen für Portalressourcen definieren

Der Administrator des Portalservers sollte Benutzer und Benutzergruppen so erstellen, dass Zugriff auf Cúram-spezifische Portalressourcen erteilt wird (z. B. Portalseiten mit Cúram-Portlets). Ferner sollte eine direkte Zuordnung zwischen den Benutzern der Portalressourcen und den Benutzern der Cúram-Anwendung (IBM Cúram Social Program Management) bestehen, d. h. die Benutzer `Admin` und `Fallbearbeiter`. Weitere Informationen zur Erstellung von Benutzern und Benutzergruppen finden Sie im Abschnitt **Verwalten** > **Benutzer und Gruppen** > **Neue Benutzer und Gruppen erstellen** in der WebSphere Portal Server-Dokumentation. Die Benutzer können zur Gruppe `Alle authentifizierten Portalbenutzer` oder zu einer neuen Gruppe hinzugefügt werden, die hervorhebt, dass die Gruppe aus Benutzern von Cúram-Portlets besteht.

Anmerkung: Die `Benutzer-ID` und das `Kennwort` für diese Benutzer müssen mit dem `Benutzernamen` und dem `Kennwort` für die Benutzer der Cúram-Anwendung übereinstimmen.

4.3 Portlets auf Portalseiten implementieren

Die Implementierung eines Cúram-Portlets auf einer Portalseite besteht grundsätzlich aus zwei Schritten, die im Abschnitt **Verwalten** > **Portlets und Portletanwendungen verwalten** > **Portlet installieren** in der WebSphere Portal Server-Dokumentation beschrieben werden:

- Installation der Datei `CuramPortlets.war` mit den Cúram-Portlets im Repository für Webmodule auf dem Portalserver.
- Erstellung einer Instanz eines Cúram-Portlets auf einer Portalseite.

Der entsprechende Benutzer kann eine Portalseite mit Cúram-Portlets öffnen, indem er eine Instanz eines Web-Browsers öffnet und über `http://domain:WpsHostPort/WpsContextRoot/MyPortalPage"/>` auf diese Seite verweist.

Beispiel: Wenn die Standardwerte für die Portalserverinstallation und die Standardwerte der Cúram-Portletkonfiguration verwendet werden (und eine Portalseite mit dem Namen `MyPortalPage` erstellt wurde, die Cúram-Portlets enthält), sollte der Browser auf `http://localhost:10039/wps/myportal/MyPortalPage"/>` verweisen.

Anhang. Konfiguration von SSO-Cúram-Portlets

A.1 Einführung

In den Abschnitten dieses Anhangs werden die manuellen Schritte beschrieben, die zum Konfigurieren von Cúram-SSO-Portlets auf einem Portalserver erforderlich sind. Zuerst muss der Portalserver manuell konfiguriert werden. Danach müssen die EAR-Dateien für die Anwendung manuell auf dem Server implementiert werden.

A.2 WebSphere Portal Server manuell konfigurieren

A.2.1 Portalserver starten

Zum Starten von `WebSphere_Portal` wird die Datei `startServer.bat` im Verzeichnis `wp_profile/bin` der WebSphere-Installation verwendet:

`<WEBSPHERE PORTAL-INSTALLATIONSVERZ>/wp_profile/bin/startServer WebSphere_Portal`. Der Standardprofilname während der Installation ist „wp_profile". Wenn Sie den Profilnamen angepasst haben, müssen Sie anstelle von „wp_profile" diesen Namen verwenden.

Alternativ kann die Administrationskonsole über **Start** > **Programme** > **IBM WebSphere** > **Portal Server** *Version* > **Server starten** gestartet werden.

A.2.2 Administrationskonsole

Um die Administrationskonsole zu öffnen, sollte der Web-Browser auf die folgende Adresse verweisen:
`https://domain:10032/ibm/console"/>`

Alternativ kann die Administrationskonsole über **Start** > **Programme** > **IBM WebSphere** > **Application Server Network Deployment** *Version* > **Profile** > **wp_profile** > **Administrationskonsole** gestartet werden. Die Befehle **Server starten** und **Server stoppen** können auch über dieses Menü zum Starten und Stoppen der Server verwendet werden.

Bei jedem Öffnen der Administrationskonsole wird für die Anmeldung nach einem Benutzernamen und einem Kennwort gefragt. Dies sind die Berechtigungsnachweise, die bei der Installation des Portalservers verwendet wurden. Die Administrationskonsole ist in zwei Sektionen unterteilt. Die linke Seite enthält eine Baumhierarchie zum Navigieren durch die Konsole. Die rechte Seite zeigt die Informationen an, die sich auf den aktuell im Baum ausgewählten Knoten beziehen. Auf den Befehl `Navigate to` hin sollte die Baumhierarchie zu dem entsprechenden Knoten traversieren.

A.2.3 Datenquellen-Anmeldealias erstellen

Die Administrationskonsole kann dazu verwendet werden, einen Anmeldealias sowohl für die DB2- als auch für die Datenquellen wie folgt zu konfigurieren:

1. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
2. Erweitern Sie die Option **Java Authentication and Authorization Service** im Abschnitt **Authentifizierung** und wählen Sie die Option **J2C-Authentifizierungsdaten**.
3. Klicken Sie auf **Neu**, um die Konfigurationsanzeige zu öffnen.
4. Definieren Sie die folgenden Felder:

   Alias = dbadmin

   Benutzer-ID = *<database username>*

   Kennwort = *<database password>*

Beschreibung = Alias für Datenbanksicherheit

Wobei <*database username*> und <*database password*> auf den Benutzernamen und das Kennwort gesetzt sind, die für die Anmeldung bei der Datenbank verwendet werden.

5. Klicken Sie auf **OK**, um die Änderungen zu bestätigen.

A.2.4 DB2-Datenquellen konfigurieren

A.2.4.1 DB2-Umgebungsvariable einrichten

1. Navigieren Sie zu **Umgebung** > **WebSphere-Variablen**.
2. Wählen Sie den Link 'DB2UNIVERSAL_JDBC_DRIVER_PATH' aus der Liste von Umgebungsvariablen aus. Damit wird die Konfigurationsanzeige für diese Variable geöffnet.
3. Richten Sie das Feld **Wert** so ein, dass es auf das Verzeichnis verweist, das die Typ-4- bzw. Typ-2-Treiber enthält. Normalerweise ist dies das Verzeichnis `Treiber` unter der SDEJ-Installation, z.B. `D:\Curam\CuramSDEJ\drivers`.
4. Klicken Sie auf **OK**, um die Änderungen zu bestätigen.

A.2.4.2 Anbieter für Datenbanktreiber einrichten

1. Navigieren Sie zu **Ressourcen** > **JDBC** > **JDBC-Provider**.
2. *Hinweis:* An dieser Stelle sollte der entsprechende Bereich ausgewählt werden, in dem die Datenquelle definiert werden soll.
3. Klicken Sie auf **Neu**, um einen neuen Treiber hinzuzufügen. Damit öffnet sich eine Konfigurationsanzeige.
4. Wählen Sie **DB2** aus der Drop-down-Liste **Datenbanktyp**.
5. Wählen Sie **DB2 Universal JDBC Driver Provider** aus der Drop-down-Liste **Anbietertyp**.
6. Wählen Sie die **XA-Datenquelle** aus der Drop-down-Liste **Implementierungstyp**.
7. Klicken Sie auf **Weiter**, um fortzufahren.
8. Überprüfen Sie die Eigenschaften in der Konfigurationsanzeige, die geöffnet wird. Es wird vermutlich nicht notwendig sein, eine von ihnen zu ändern, sofern Sie nicht planen, eine Verbindung zu einer **zOS**-Datenbank herzustellen. In diesem Fall überprüfen Sie, ob das Feld `${DB2UNIVERSAL_JDBC_DRIVER_PATH}` auf das richtige Verzeichnis für Ihr System verweist. Es sollte beispielsweise auf das Verzeichnis verweisen, das die DB2 Connect-Lizenz-JAR-Datei `db2jcc_license_cisuz.jar` enthält, die von IBM für die **zOS**-Konnektivität zur Verfügung gestellt wird.
9. Klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**, um die Änderungen zu bestätigen.

A.2.4.3 Datenquelle für den Datenbanktreiber einrichten

Die folgenden Schritte sollten für jede der Anwendungsdatenquellen wiederholt werden, wobei `curamdb`, `curamsibdb` und `curamtimerdb` für <*DatasourceName*> (ohne spitze Klammern) eingesetzt werden:

1. Wählen Sie den `DB2 Universeller JDBC-Treiberanbieter (XA)`, der jetzt in der Liste **JDBC-Provider** angezeigt wird. Damit wird die Konfigurationsanzeige für den Anbieter geöffnet.
2. Wählen Sie den Link **Datenquellen** unter **Weitere Eigenschaften**.
3. Klicken Sie auf **Neu**, um eine neue Datenquelle hinzuzufügen.
4. Setzen Sie die Felder wie folgt:

   Datenquellenname : <*DatasourceName*>

   JNDI-Name : *jdbc/*<*DatasourceName*>
5. Klicken Sie auf **Weiter**, um fortzufahren.
6. Setzen Sie die Felder wie folgt:

   Treibertyp : 2 oder 4 je nach Erforderlichkeit,

   Datenbankname : Der Name der DB2-Datenbank. (Dieser Name entspricht der Eigenschaft 'curam.db.name' in der Datei `Bootstrap.properties`.)

Servername : Der Name des DB2-Datenbankservers. (Dieser Name entspricht der Eigenschaft 'curam.db.servername' in der Datei `Bootstrap.properties`.)

Portnummer : Der DB2-Datenbankserverport. (Dieser Name entspricht der Eigenschaft 'curam.db.serverport' in der Datei `Bootstrap.properties`.)

Lassen Sie alle anderen Felder unverändert, solange keine bestimmte Änderung erforderlich ist. Klicken Sie auf **Weiter**.

7. Setzen Sie den Wert aus der Dropdown-Liste für **Komponentengesteuerter Authentifizierungsalias** auf <*valid for database*>.

   Setzen Sie den Wert aus der Drop-down-Liste für den **Alias für Konfigurationszuordnung** auf: DefaultPrinicipalMapping

   Setzen Sie **Containergesteuerter Authentifizierungsalias** auf: <*valid for database*>.

   Wobei der verwendete Alias <*valid for database*> der ist, der unter A.2.3, „Datenquellen-Anmeldealias erstellen", auf Seite 9 eingerichtet wird.

   Lassen Sie alle anderen Felder unverändert, soweit keine bestimmte Änderung erforderlich ist. Klicken Sie auf **Weiter**, um fortzufahren.
8. Klicken Sie auf **Fertigstellen**, um die Änderungen zu bestätigen, und fahren Sie fort.
9. Wählen Sie die neu erstellte Datenquelle *DatasourceName* aus der angezeigten Liste.
10. Wählen Sie den Link **Angepasste Eigenschaften** unter **Weitere Eigenschaften**.
11. Wählen Sie den Eintrag `fullyMaterializeLobData`.
12. Setzen Sie den `Wert` auf `false`.
13. Klicken Sie auf **OK**, um die Änderung zu bestätigen.

A.2.5 Masterkonfiguration speichern

Das *Speichern* wird durch Klicken auf den Link **Speichern** im Nachrichtenfenster **Nachricht(en)** ausgeführt. Dieses Fenster wird nur nach dem Vornehmen der Konfigurationsänderungen angezeigt.

A.2.6 Verwaltungssicherheit konfigurieren

Von der Anwendung wird standardmäßig die dateibasierte WebSphere-Benutzerregistry verwendet.

1. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
2. Setzen Sie **Verfügbare Realmdefinitionen** auf **Eingebundene Repositorys** und klicken Sie auf die Schaltfläche **Konfigurieren**.
3. Setzen Sie **Primärer administrativer Benutzername** auf `websphere`.
4. Wählen Sie das Optionsfeld **Automatisch generierte Server-ID**.
5. Wählen Sie **Groß-/Kleinschreibung für Berechtigung ignorieren** und klicken Sie auf **OK**.
6. Geben Sie das Kennwort für den Standardbenutzer mit Verwaltungsaufgaben, z.B. `websphere`, geben Sie die Bestätigung ein und klicken Sie auf **OK**, um die Änderungen zu bestätigen.
7. Setzen Sie **Verfügbare Realmdefinitionen** auf **Eingebundene Repositorys** und klicken Sie auf die Schaltfläche **Als aktuelles Repository festlegen**.
8. Wählen Sie **Verwaltungssicherheit aktivieren**.
9. Wählen Sie **Anwendungssicherheit aktivieren**.
10. Wählen Sie **Java-2-Sicherheit verwenden, um den Anwendungszugriff auf lokale Ressourcen zu beschränken** und **Warnen, wenn Anwendungen angepasste Berechtigungen erteilt werden**.
11. Klicken Sie auf die Schaltfläche **Anwenden**, um die Änderungen zu bestätigen.
12. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
13. Wählen Sie den Link **Angepasste Eigenschaften** aus.
14. Klicken Sie auf **Neu** und setzen Sie Namen und Wert wie folgt:

    Name= `com.ibm.ws.security.web.logoutOnHTTPSessionExpire`

    Wert = `true`

15. Klicken Sie auf **OK**, um die neue Eigenschaft hinzuzufügen.
16. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
17. Wählen Sie **Web- und SIP-Sicherheit** > **Single Sign-on (SSO)**.
18. Stellen Sie sicher, dass das Kontrollkästchen **Erfordert SSL** inaktiviert ist.
19. Stellen Sie sicher, dass der Wert des Felds **Domänenname** auf den vollständig qualifizierten Domänennamen für den Zugriff auf die Anwendung gesetzt ist (z. B. xxx.com). Die Konfiguration sollte der unter 3.1.2, „Basis-URL in Cúram-Portlets konfigurieren", auf Seite 5 angegebenen Konfiguration entsprechen.
20. Klicken Sie auf **OK**, um die Änderung zu bestätigen.
21. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
22. Wählen Sie **Angepasste Eigenschaften**.
23. Fügen Sie die Eigenschaft 'com.ibm.ws.security.addHttpOnlyAttributeToCookies' mit dem Wert `true` hinzu.
24. Klicken Sie auf **OK**, um die Änderung zu bestätigen.
25. Speichern Sie die Änderungen in der Masterkonfiguration.

A.2.7 Benutzer konfigurieren

Die konfigurierte WebSphere Portal Server-Benutzerregistry wird für die Authentifizierung von Benutzern mit Verwaltungsaufgaben und Datenbankbenutzern verwendet. Die WebSphere Portal Server-Benutzer mit Verwaltungsaufgaben und Datenbankbenutzer müssen der Benutzerregistry wie folgt manuell hinzugefügt werden:

- Navigieren Sie zu **Benutzer und Gruppen** > **Benutzer verwalten**.
- Klicken Sie auf die Schaltfläche **Erstellen**.
- Geben Sie die Einzeldaten für den Portalserverbenutzer mit Verwaltungsaufgaben ein und klicken Sie auf die Schaltfläche **Erstellen**.
- Wiederholen Sie diese Schritte für den Datenbankbenutzer.
- Für jeden Benutzer einer Cúram-Anwendung (z. B. Verwaltungsanwendung) sollte der entsprechende Benutzer als Portalserverbenutzer definiert werden. Geben Sie mindestens die Benutzer 'Admin' und 'Fallbearbeiter' an. Der Admin-Benutzer wird wie folgt definiert:
  - Der Wert des Felds `Benutzer-ID` muss auf `Admin` gesetzt werden.
  - Der Wert des Felds `Vorname` kann auf `Admin` gesetzt werden.
  - Der Wert des Felds `Vorname` kann auf `Bearbeiter` gesetzt werden.
  - Der Wert der Felder `Kennwort` und `Kennwort bestätigen` muss auf den Wert des Kennworts gesetzt werden, das für den Zugriff auf die Verwaltungsanwendung verwendet wird.

Hinweis: Wenn die Verwaltungssicherheit für den Portalserver während der Profilerstellung aktiviert war, ist der Benutzer mit Verwaltungsaufgaben möglicherweise bereits in der Registry definiert.

A.2.8 Cross-Cluster-Authentifizierung inaktivieren

Diese Eigenschaft bestimmt das Verhalten einer LTPA-Token2-Anmeldung mit Single Sign-on. Die Eigenschaft 'com.ibm.ws.security.webChallengeIfCustomSubjectNotFound' ist auf 'false' (falsch) gesetzt, um sicherzustellen, dass Websitzungen nahtlos zwischen den zwei Servern eines Clusters übertragen werden können (z.B. in einem Übernahmeszenario), ohne dass der Benutzer zur Eingabe von Sicherheitsberechtigungsnachweisen aufgefordert wird.

1. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
2. Klicken Sie auf **Angepasste Eigenschaften** und wählen Sie die Eigenschaft **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** aus der Liste verfügbarer Eigenschaften.
3. Ändern Sie unter 'General Properties' den Wert der Eigenschaft **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** in *false*.

4. Klicken Sie auf **OK**, um die Hinzufügung zu bestätigen.

A.2.9 Änderungen speichern

Speichern Sie die Änderungen in der Masterkonfiguration wie unter A.2.5, „Masterkonfiguration speichern”, auf Seite 11 beschrieben.

A.3 Konfiguration eines bestimmten Servers

In diesem Abschnitt wird beschrieben, wie das entsprechende Ziel hinsichtlich des Servergeltungsbereichs (d. h. WebSphere_Portal) konfiguriert wird.

A.3.1 Port für JNDI-Suche konfigurieren

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus, z. B. 'WebSphere_Portal'.
3. Erweitern Sie im Abschnitt **Kommunikation** die Option **Ports** und klicken Sie auf die Schaltfläche **Details**.
4. Wählen Sie den Eintrag **BOOTSTRAP_ADDRESS** aus und setzen Sie **Port** auf den Wert der Eigenschaft 'curam.server.port' in ihrer `AppServer.properties`-Datei.
5. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.
6. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

A.3.2 Pass-by-Reference für Object-Request-Broker konfigurieren

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus, z. B. 'WebSphere_Portal'.
3. Erweitern Sie im Abschnitt **Containereinstellungen** die Option **Containerservices** und klicken Sie auf den Link **ORB-Service**.
4. Wählen Sie die Option **Durch Referenz übergeben** aus dem Abschnitt **Allgemeine Eigenschaften**.
5. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.
6. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

A.3.3 Java Virtual Machine konfigurieren

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus (d. h. WebSphere_Portal).
3. Erweitern Sie im Abschnitt **ServerinfrastrukturJava- und Prozessverwaltung and Process Management**.
4. Wählen Sie den Link **Prozessdefinition** aus.
5. Wählen Sie im Abschnitt **Weitere Eigenschaften** den Link **Java Virtual Machine** aus.
6. Setzen Sie die Felder wie folgt:

   Anfangsgröße des Heapspeichers :`512`

   Maximale Größe des Heapspeichers :`1024`

   Klicken Sie auf **Anwenden**, um die Werte festzulegen.
7. Im Abschnitt **Weitere Eigenschaften** wählen Sie den Link **Angepasste Eigenschaften** aus.
8. Klicken Sie auf **Neu** und definieren Sie dann die Eigenschaften wie folgt:

   Name : `com.ibm.websphere.security.util.authCacheCustomKeySupport`

   Wert : `false`

   Klicken Sie auf **OK**, um die Eigenschaft hinzuzufügen.
9. *Der folgende Schritt ist nur für Plattformen, die keine Windows-Plattformen sind, erforderlich.*

Klicken Sie auf **Neu** und definieren Sie dann die Eigenschaften wie folgt:

Name : `java.awt.headless`

Wert : `true`

Klicken Sie auf **OK**, um die Eigenschaft hinzuzufügen.

10. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

A.3.4 Zeitgeberservice konfigurieren

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus (d. h. WebSphere_Portal).
3. Erweitern Sie im Abschnitt **ContainereinstellungenEJB-Containereinstellungen**.
4. Wählen Sie den Link **Einstellungen des EJB-Zeitgeberservice** aus.
5. Im Fenster **Schedulertyp** wählen Sie die Option **Interne Scheduler-Instanz für EJB-Zeitgeberservice verwenden** aus.
6. Setzen Sie die Felder wie folgt:

   JNDI-Name der Datenquelle :`jdbc/curamtimerdb`

   Datenquellenalias : *<valid for database>*

   Wobei der verwendete Alias der ist, der unter A.2.3, „Datenquellen-Anmeldealias erstellen", auf Seite 9 eingerichtet wird.
7. Klicken Sie auf **OK**, um die Änderungen zu bestätigen.
8. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

A.3.5 Portzugriff einrichten

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus (d. h. WebSphere_Portal).
3. Wählen Sie im Abschnitt **Kommunikation** den Link **Ports** aus.
4. Klicken Sie auf die Schaltfläche **Details**.
5. Klicken Sie auf **Neu** und setzen Sie für den Client-TCP/IP-Port die folgenden Felder:

   Name des benutzerdefinierten Ports : `CuramClientEndPoint`

   Host : `*`

   Port : `9044`

   Klicken Sie auf **OK**, damit die Änderungen Anwendung finden.
6. Klicken Sie auf **Neu** und setzen Sie für den Web-Services-TCP/IP-Port die folgenden Felder:

   Name des benutzerdefinierten Ports : `CuramWebServicesEndPoint`

   Host : `*`

   Port : `9082`

   Klicken Sie auf **OK**, damit die Änderungen Anwendung finden.
7. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
8. Wählen Sie den entsprechenden Server aus der Liste aus (d. h. WebSphere_Portal).
9. Erweitern Sie in der Verzweigung **Einstellungen des Webcontainers** den Abschnitt **Containereinstellungen**.
10. Wählen Sie den Link **Transportketten für Webcontainer** aus.
11. Klicken Sie auf **Neu** und setzen Sie für die Client-Transportketten die folgenden Felder:

    Name : `CuramClientChain`

    Transportkettenschablone : WebContainer-Secure

    Klicken Sie auf **Weiter**.

    Vorhandenen Port verwenden : CuramClientEndPoint

Klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**.

12. Klicken Sie auf **Neu** und setzen Sie für die WebServices-Transportkette die folgenden Felder:

    Name : `CuramWebServicesChain`

    Transportkettenschablone : WebContainer

    Klicken Sie auf **Weiter**.

    Vorhandenen Port verwenden : CuramWebServicesEndPoint

    Klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**.
13. Wählen Sie die neu erstellte **CuramClientChain** aus.
14. Wählen Sie den Link **HTTP Inbound Channel** aus.
15. Stellen Sie sicher, dass das Kontrollkästchen **Persistente (Keep-Alive-) Verbindungen verwenden** aktiviert ist.
16. Klicken Sie auf **OK**, um die Hinzufügung zu bestätigen.
17. Navigieren Sie zu **Umgebung** > **Virtuelle Hosts**.
18. Klicken Sie auf **Neu**, um durch Setzen der folgenden Felder `Virtueller Host` neu hinzuzufügen.

    Name = *client_host*

    Wiederholen Sie diesen Schritt und ersetzen Sie dabei *client_host* durch *webservices_host*.
19. Wählen Sie den Link **client_host** aus der Liste virtueller Hosts aus.

    Wählen Sie den Link **Hostalias** im Abschnitt **Weitere Eigenschaften**.

    Klicken Sie auf **Neu**, um durch Setzen der folgenden Felder einen neuen `Alias` hinzuzufügen.

    Hostname = *

    Port = *9044*

    Wobei *9044* der Port ist, der in Schritt 5 verwendet wurde. Wiederholen Sie diesen Schritt für den anderen verwendeten virtuellen Host und Port (z.B. webservices_host, 9082).
20. Klicken Sie auf **OK**, um die Hinzufügung zu bestätigen.
21. Speichern Sie die Änderungen in der Masterkonfiguration wie unter A.2.5, „Masterkonfiguration speichern", auf Seite 11 beschrieben.

A.3.6 Sicherheitsintegration für Sitzungen konfigurieren

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus (d. h. WebSphere_Portal).
3. Klicken Sie im Abschnitt **Containereinstellungen** auf **Sitzungsverwaltung**.
4. Wählen Sie **Sicherheitsintegration** und *inaktivieren* Sie sie. *Hinweis: Achten Sie darauf, dass die Sicherheitsintegration inaktiviert ist.*
5. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.
6. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.
7.

   Anmerkung: Die obige Einstellung wird für Webanwendungen benötigt.

A.4 Buskonfiguration

A.4.1 Service Integration Bus einrichten

1. Navigieren Sie zu **Serviceintegration** > **Busse**.
2. Klicken Sie auf **Neu** setzen Sie in **Schritt 1** das folgende Feld:

   Name : CuramBus

   Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **Weiter**.

3. Rufen Sie den Assistenten **Bussicherheit konfigurieren**, Schritt 1.1, auf und klicken Sie auf **Weiter**.

   In **Schritt 1.2** des Assistenten **Bussicherheit konfigurieren** übernehmen Sie die Standardeinstellung und klicken Sie auf **Weiter**.

   In **Schritt 1.3** des Assistenten **Bussicherheit konfigurieren** übernehmen Sie die Standardeinstellungen, sofern sie passen, und klicken Sie auf **Weiter**.

   In **Schrittt 1.4** des Assistenten **Bussicherheit konfigurieren** überprüfen Sie Ihre Einstellungen und klicken Sie auf **Weiter**.
4. In Schritt 2 klicken Sie auf **Fertigstellen**, damit die Änderungen wirksam werden.
5. Wählen Sie den **CuramBus** aus der Liste mit Bussen aus, die jetzt angezeigt wird. Damit öffnet sich die Konfigurationsanzeige.
6. Wählen Sie **Bus-Member** im Abschnitt **Topologie** aus.
7. Klicken Sie auf **Hinzufügen**, woraufhin der Assistent **Neues Bus-Member hinzufügen** geöffnet wird.
8. Wählen Sie den Server aus, der dem Bus hinzugefügt werden soll, und klicken Sie auf **Weiter**.
9. Wählen Sie **Datenspeicher** aus und klicken Sie auf **Weiter**.
10. Wählen Sie die Option **Vorhandene Datenquelle verwenden** aus und setzen Sie die Optionen wie folgt:

    JNDI-Name der Datenquelle = jdbc/curamsibdb

    Schemaname = *username*

    Wobei *username* der Benutzername für die Datenbank ist.

    Heben Sie die Auswahl der Option **Tabellen erstellen** auf.

    Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **Weiter**.
11. Übernehmen Sie die Standard-Optimierungsparameter als angemessene Werte und klicken Sie auf **Weiter**.
12. Klicken Sie auf **Fertigstellen**, um den Vorgang zu beenden und den Assistenten zu verlassen.
13. Navigieren Sie zu **Serviceintegration** > **Busse**.
14. Wählen Sie den **CuramBus** aus der Liste mit Bussen aus, die jetzt angezeigt wird. Damit öffnet sich die Konfigurationsanzeige.
15. Wählen Sie im Abschnitt **Weitere Eigenschaften Sicherheit** aus.
16. Wählen Sie im Abschnitt **Berechtigungsrichtlinie Benutzer und Gruppen in der Rolle Bus-Connector** aus.
17. Klicken Sie auf **Neu**, um den **Assistent für SIB-Sicherheitsressourcen** zu öffnen.
18. Wählen Sie das Optionsfeld **Integrierte Sondergruppen** aus und klicken Sie auf **Weiter**.
19. Aktivieren Sie die Kontrollkästchen **Server** und **AllAuthenticated** und klicken Sie auf **Weiter**.
20. Klicken Sie auf **Fertigstellen**, um den Vorgang zu beenden und den Assistenten zu verlassen.
21. Speichern Sie die Änderungen in der Masterkonfiguration wie unter A.2.5, „Masterkonfiguration speichern”, auf Seite 11 beschrieben.

A.5 JMS(Java Message Service)-Konfiguration

A.5.1 JMS-Verbindungsfactorys einrichten

1. Navigieren Sie zu **Ressourcen** > **JMS** > **JMS-Provider**.
2. *Hinweis:* An dieser Stelle sollte der entsprechende Bereich ausgewählt werden, in dem die JMS-Ressourcen definiert werden sollen.
3. Wählen Sie den Link **Standard-Messaging-Provider** aus.
4. Wählen Sie im Abschnitt **Weitere Eigenschaften** den Link **Verbindungsfactorys** aus.
5. Klicken Sie auf **Neu** und setzen Sie die folgenden Felder:

Name : CuramQueueConnectionFactory

JNDI-Name : jms/CuramQueueConnectionFactory

Beschreibung : Die Factory für alle Verbindungen zu Anwendungswarteschlangen.

Busname : CuramBus

Authentifizierungsalias für XA-Wiederherstellung : Gleicher Wert wie für die Datenquelle `jdbc/curamdb` (z.B. <*SERVERNAME*> /dbadmin)

Alias für Konfigurationszuordnung : DefaultPrinicipalMapping

Container-managed authentication alias : Gleicher Wert wie für den Authentifizierungsalias für die XA-Wiederherstellung.

Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **OK**, damit die Änderungen Anwendung finden.

6. Klicken Sie auf **Neu** und setzen Sie die folgenden Felder:

   Name : CuramTopicConnectionFactory

   JNDI-Name : jms/CuramTopicConnectionFactory

   Beschreibung : Die Factory für alle Verbindungen zu Anwendungswarteschlangen.

   Busname : CuramBus

   Authentifizierungsalias für XA-Wiederherstellung : Gleicher Wert wie für die Datenquelle `jdbc/curamdb` (z.B. <*SERVERNAME*> /dbadmin)

   Alias für Konfigurationszuordnung : DefaultPrinicipalMapping

   Containergesteuerter Authentifizierungsalias : Gleicher Wert wie für die Datenquelle `jdbc/curamdb` (z.B. <*SERVERNAME*> /dbadmin)

   Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **OK**, damit die Änderungen Anwendung finden.

7. Speichern Sie die Änderungen in der Masterkonfiguration wie unter A.2.5, „Masterkonfiguration speichern”, auf Seite 11 beschrieben.

A.5.2 Anwendungswarteschlangen einrichten

Führen Sie die folgenden Schritte durch, indem Sie <*QueueName*> (ohne spitze Klammern) durch jeden der folgenden Warteschlangennamen ersetzen: DPEnactment, DPError, CuramDeadMessageQueue, WorkflowActivity, WorkflowEnactment und WorkflowError.

1. Navigieren Sie zu **Serviceintegration** > **Busse** > **CuramBus**.
2. Wählen Sie im Abschnitt **Zielressourcen** den Link **Ziele** aus.
3. Klicken Sie auf **Neu**, um den Assistenten „Neues Ziel erstellen” zu öffnen.
4. Wählen Sie **Warteschlange** als Zieltyp aus und klicken Sie auf **Weiter**.
5. Setzen Sie die folgenden Warteschlangenattribute:

   ID : SIB_ <*QueueName*>

   Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **Weiter**.
6. Verwenden Sie **Ausgewähltes Bus-Member** und klicken Sie auf **Weiter**.
7. Klicken Sie auf **Fertigstellen**, um die Erstellung der Warteschlange zu bestätigen.
8. Wählen Sie die neu hinzugefügte Warteschlange SIB_ <*QueueName*> aus, die jetzt in der Liste vorhandener Anbieter angezeigt wird. Damit öffnet sich wieder die Konfigurationsanzeige.
9. Verwenden Sie die folgende Tabelle, um über das Optionsfeld **Angeben** und das zugehörige Textfeld das Ausnahmeziel festzulegen.

Tabelle 2. Einstellungen für Ausnahmeziele

Name der Warteschlange	Ausnahmeziel
SIB_CuramDeadMessageQueue	System

Tabelle 2. Einstellungen für Ausnahmeziele (Forts.)

Name der Warteschlange	Ausnahmeziel
SIB_DPEnactment	SIB_DPError
SIB_DPError	SIB_CuramDeadMessageQueue
SIB_WorkflowActivity	SIB_WorkflowError
SIB_WorkflowEnactment	SIB_WorkflowError
SIB_WorkflowError	SIB_CuramDeadMessageQueue

10. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.
11. Navigieren Sie zu **Ressourcen** > **JMS** > **JMS-Provider**.
12. Wählen Sie den Link **Standard-Messaging-Provider** aus.
13. Wählen Sie im Abschnitt **Weitere Eigenschaften** den Link **Warteschlangen** aus.
14. Klicken Sie auf **Neu** und setzen Sie die folgenden Felder:

    Name : <*QueueName*>

    JNDI-Name : jms/ <*QueueName*>

    Busname : CuramBus

    Name der Warteschlange : SIB_ <*QueueName*>

    Übermittlungsmodus : Persistent

    Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **OK**, damit die Änderungen Anwendung finden.

Speichern Sie die Änderungen in der Masterkonfiguration wie unter A.2.5, „Masterkonfiguration speichern", auf Seite 11 beschrieben.

A.5.3 Anwendungsthemen einrichten

1. Navigieren Sie zu **Ressourcen** > **JMS** > **JMS-Provider**.
2. Wählen Sie den Link **Standard-Messaging-Provider** aus.
3. Wählen Sie im Abschnitt **Weitere Eigenschaften** den Link **Thema** aus.
4. Klicken Sie auf **Neu** und setzen Sie die folgenden Felder:

   Name : CuramCacheInvalidationTopic

   JNDI-Name : jms/CuramCacheInvalidationTopic

   Beschreibung : Cache Invalidation Topic

   Busname : CuramBus

   Topicbereich : Default.Topic.Space

   JMS-Übermittlungsmodus : Persistent

   Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **OK**, damit die Änderungen Anwendung finden.
5. Speichern Sie die Änderungen in der Masterkonfiguration wie unter A.2.5, „Masterkonfiguration speichern", auf Seite 11 beschrieben.

A.5.4 Aufzubewahrende Protokolldateien konfigurieren

Dies ist ein optionaler Schritt. Es besteht die Möglichkeit, die maximale Anzahl an aufzubewahrenden Protokolldateien zu konfigurieren, die von einem bestimmten Server verwaltet werden sollen. Gehen Sie dazu wie folgt vor:

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste von Servern.
3. Wählen Sie **Protokollierung und Traceerstellung** aus dem Abschnitt **Fehlerbehebung**.

4. Wählen Sie **JVM-Protokolle** aus der Liste **Allgemeine Eigenschaften**.
5. Ändern Sie den Wert im Feld **Maximale Anzahl aufzubewahrender Protokolldateien** in '30', sowohl für die Datei `System.out` als auch für die Datei `System.err`.
6. Klicken Sie auf **OK**, damit die Änderungen Anwendung finden.
7. Speichern Sie die Änderungen in der Masterkonfiguration.

A.5.5 Fertigstellung

Der Portalserver ist nun konfiguriert und steht für die Installation einer Anwendung bereit. Melden Sie sich von der Administrationskonsole ab und führen Sie einen Neustart für den Portalserver durch.

A.6 Portalserver zur Wiederverwendung von JSESSIONID konfigurieren

Zur Aktivierung von SSO zwischen der Cúram-Anwendung und Cúram-Portlets müssen die Informationen von `JSESSIONID` beibehalten werden. Führen Sie dazu die folgenden Schritte aus:

- Navigieren Sie zu **Server** > **Servertypen** > **WebSphere Application Server** > **WebSphere_Portal** > **Serverinfrastruktur** > **Java- und Prozessverwaltung** > **Prozessdefinition** > **Java Virtual Machine** > **Benutzerdefinierte Merkmale** > **Neu**.
- Geben Sie `HttpSessionIdReuse` als Wert für das Feld `Name` und `true` als Wert für das Feld `Wert` an.
- Klicken Sie erneut auf **OK**, um die Änderungen anzuwenden.
- Speichern Sie die Änderungen in der Masterkonfiguration.

A.7 Manuelle Anwendungsimplementierung

Für das Installieren einer Unternehmensanwendung in WebSphere kann die Administrationskonsole verwendet werden. Mit den unten aufgeführten Schritten wird beschrieben, wie mithilfe der Administrationskonsole eine Anwendung, EJB-Komponente oder ein Webmodul installiert werden kann.

Anmerkung: Ist die Installation einmal gestartet, so muss zum Abbrechen der Installation der Anwendung die Schaltfläche **Abbrechen** verwendet werden. Es reicht nicht aus, einfach auf eine andere Seite der Administrationskonsole zu wechseln, ohne zuerst auf einer Anwendungsinstallationsseite auf **Abbrechen** geklickt zu haben.

1. Navigieren Sie zu **Anwendungen** > **Neue Anwendung**.
2. Wählen Sie die Option **Neue Unternehmensanwendung** aus.
3. Klicken Sie auf das entsprechende Optionsfeld und geben Sie wahlweise über die Schaltfläche **Durchsuchen** oder das Fenster **Pfad der neuen Anwendung** den vollständigen Pfadnamen der Quellenanwendungsdatei oder EAR-Datei ein. Klicken Sie anschließend auf **Weiter**.

   Die Standardposition für die Anwendungs-EAR-Dateien ist

   `%SERVER_DIR%/build/ear/WAS/Curam.ear`
4. Wählen Sie im Fenster **Wie soll die Anwendung installiert werden?** das Optionsfeld **Schnell - Nur anfragen, wenn weitere Informationen erforderlich sind** aus. Klicken Sie auf **Weiter**.
5. Belassen Sie die Standardwerte, da sie für Schritt 1 gedacht sind, wählen Sie *Installationsoptionen* aus und klicken Sie auf **Weiter**.
6. In Schritt 2, **Servern Module zuordnen**, wählen Sie für jedes aufgeführte Modul aus der Liste **Cluster und Server** einen Zielserver oder -Cluster aus. Aktivieren Sie dazu das Kontrollkästchen neben dem jeweiligen Modul an, wählen Sie den Server oder Cluster aus und klicken Sie auf **Anwenden**.
7. Klicken Sie auf **Weiter** und anschließend auf **Fertigstellen**, um den Installationsvorgang zu beenden. Dieser Schritt kann einige Minuten in Anspruch nehmen. Anschließend sollte die Nachricht *Cúram-Anwendung erfolgreich installiert* erscheinen.
8. Speichern Sie die Änderungen in der Masterkonfiguration. (Weitere Details hierzu finden Sie unter A.2.5, „Masterkonfiguration speichern”, auf Seite 11.)

9. Navigieren Sie zu **Anwendungen** > **Anwendungstypen** > **WebSphere-Unternehmensanwendungen** und wählen Sie die neu installierte Anwendung aus.
10. Wählen Sie im Abschnitt **Detaileigenschaften** die Option **Laden von Klassen und Erkennung von Dateiaktualisierungen** aus.
11. Setzen Sie die Eigenschaft **Reihenfolge der Klassenlader** auf **Mit dem lokalen Klassenlader geladene Klassen zuerst (übergeordneter zuletzt)**.
12. Setzen Sie die Eigenschaft **Klassenladerrichtlinie für WAR-Dateien** auf **Einzelner Klassenlader für gesamte Anwendung**.
13. Klicken Sie auf **OK**.
14. Wählen Sie im Abschnitt **Detaileigenschaften** die Option **Zuordnung von Sicherheitsrollen zu Benutzern/Gruppen** aus und ordnen Sie mithilfe der folgenden Schritte die MDB-Benutzerrolle einem Benutzernamen und Kennwort zu:

    Anmerkung: Der Benutzername, den Sie für die Zuordnung zur MDB-Benutzerrolle verwenden, muss in Ihrer Benutzerregistry bereits definiert sein.

    a. Wählen Sie **Auswählen** für die MDB-Benutzerrolle aus und klicken Sie auf **Benutzer zuordnen**.
    b. Geben Sie den entsprechenden Benutzernamen in das Feld **Suchbegriff** ein und klicken Sie auf **Suchen**.
    c. Wählen Sie die ID aus der Liste **Verfügbar:** und klicken Sie auf **>>**, um es zur Liste **Ausgewählt:** hinzuzufügen. Klicken Sie anschließend auf **OK**.
    d. Klicken Sie auf **OK**.
15. Nachdem die MDB-Benutzerrolle zugeordnet ist, kannn nun die Benutzer-RunAs-Rolle aktualisiert werden. Wählen Sie dazu im Abschnitt **Detaileigenschaften** die Option **RunAs-Rollen für Benutzer** aus.
16. Geben Sie in die Felder **Benutzername** und **Kennwort** jeweils einen entsprechenden Benutzernamen und ein Kennwort ein. Wählen Sie für die MDB-Benutzerrolle **Auswählen** und klicken Sie auf **Anwenden**.
17. Klicken Sie auf **OK**.
18. Speichern Sie die Änderungen in der Masterkonfiguration.
19. Nach der Implementierung ist ein Start der Anwendung notwendig, bevor sie verwendet werden kann. Navigieren Sie zu **Anwendungen** > **Anwendungstypen** > **WebSphere-Unternehmensanwendungen**, wählen Sie die neu installierte Anwendung aus und klicken Sie auf die Schaltfläche **Start**. Dieser Schritt kann einige Minuten in Anspruch nehmen. Anschließend ändert sich der Anwendungsstatus, wodurch angezeigt wird, dass sie jetzt gestartet ist.
20. Testen Sie als letzten Schritt die Anwendungsimplementierung. Verweisen Sie dazu beispielsweise einen Web-Browser auf die implementierte Anwendung: https://localhost:9044/Curam.

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 anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden. Für die in diesem Handbuch beschriebenen 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.

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 Corporation

Dept F6, Bldg 1

294 Route 100

Somers NY 10589-3216

U.S.A.

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Bereitstellung des in diesem Dokument beschriebenen 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.

Aussagen über Pläne und Absichten von IBM 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 Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und 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 für die Betriebsumgebung 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. Die Musterprogramme werden "WIE BESEHEN", ohne Gewährleistung jeglicher Art bereitgestellt. IBM übernimmt keine Haftung für Schäden, die durch Ihre Verwendung der Musterprogramme entstehen.

Kopien oder Teile der Musterprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihres Unternehmens) (Jahr). Teile des vorliegenden Codes wurden aus Musterprogrammen der IBM Corp. abgeleitet.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Website "Copyright and trademark information" unter http://www.ibm.com/legal/us/en/copytrade.shtml.

Andere Namen können Marken der jeweiligen Rechtsinhaber sein. Weitere Firmen-, Produkt- und Servicenamen können Marken oder Servicemarken anderer Unternehmen sein.

Gedruckt in Deutschland