IBM Cúram Social Program Management
Version 6.0.5

Cúram Deployment Guide for WebSphere Application Server on z/OS

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen in „Bemerkungen" auf Seite 51 gelesen werden.

Überarbeitung: März 2014

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellen

Auf IBM WebSphere Application Server für z/OS implementieren

Es sind zahlreiche Tools von anderen Anbietern erforderlich, um IBM Cúram Social Program Management auf IBM WebSphere Application Server for IBM z/OS bereitzustellen. Web-Client-Server- und Anwendungs-EAR-Dateien werden für die Bereitstellung der Anwendung benötigt.

Einführung

Übersicht

In diesem Handbuch wird der Konfigurations- und Implementierungsprozess von IBM® Cúram Social Program Management mit IBM WebSphere Application Server für IBM z/OS beschrieben. Genauere Details zu den unterstützten Versionen finden Sie im Dokument *Cúram Supported Prerequisites* (Unterstützte Voraussetzungen für Cúram).

Die Konfigurationstasks können wie folgt zusammengefasst werden:

1. Installation und Konfiguration erforderlicher Tools von anderen Anbietern
2. Konfiguration von WebSphere Application Server für z/OS für die `.ear` (Enterprise ARchive)-Dateien der IBM Cúram Social Program Management-Anwendung
3. Aufbau und Paketierung der Anwendungs-`.ear`-Dateien

   Die `.ear`-Dateien werden separat (auf einer Microsoft Windows oder **UNIX**-Plattform) aufgebaut.
4. Implementierung der IBM Cúram Social Program Management-Anwendung und des Web-Clients. Dazu sind folgende Schritte notwendig:
   - Erstellen von Eigenschaftendateien
   - Installieren der Anwendungs-`.ear`-Dateien
   - Erstellen einer Datenbank
   - Vorkompilieren von JSPs (optional)
   - Testen der Implementierung

WebSphere Application Server für z/OS kann auf unterschiedliche Arten bezüglich der Leistung, Ressourcen, Sicherheit und anderer Aspekte angepasst und konfiguriert werden. In diesem Dokument wird ein vereinfachter Ansatz zum Konfigurieren von WebSphere Application Server für z/OS veranschaulicht, der möglicherweise nicht für Ihre Installation passend ist.

Voraussetzungen

Jedes Team oder jede Einzelperson, die dieses Dokument verwendet, muss über angemessene Kenntnisse und Erfahrungen mit einer großen Bandbreite an **z/OS**-Produkten, -Technologien usw. verfügen. Weitere Informationen hierzu finden Sie im *Programmverzeichnis für WebSphere Application Server für z/OS 7.0 (GI11-4295)* sowie in der Referenzliteratur.

Die Installation und Anpassung von WebSphere Application Server für z/OS und die zugehörige und abhängige z/OS-basierte Software wird in diesem Dokument nicht behandelt, dafür jedoch alle Schritte, die speziell für IBM Cúram Social Program Management erforderlich sind.

Es könnten weitere kundenspezifische Anpassungen erforderlich sein, zum Beispiel:

- Je nach Ihren lokalen Sicherheitsanforderungen (z.B. IBM RACF) könnte es sein, dass Sie zusätzliche Konfigurationen und Anpassungen vornehmen müssen.

Dokumentkonventionen

In diesem Dokument werden mehrere Konventionen verwendet:

- Werte in spitzen Klammern, z.B. *<WebSphere-Konfigurationsverzeichnis>*, verweisen auf Substitutionen, für die Sie Werte angeben müssen.
- Zur Navigation in der Administrationskonsole von WebSphere Application Server für z/OS:
  - „Navigieren" bezieht sich auf Auswahlen, die über die Baumstruktursteuerung im linken Teilfenster des Browserfensters getroffen werden und folgendermaßen dargestellt werden: **Server** > **Anwendungsserver**
  - „Auswählen" bezieht sich auf Hyperlinks, die im Browserfenster erscheinen und in diesem Dokument kursiv dargestellt werden, z.B. **local_host**
  - „Klicken" bezieht sich auf Schaltflächen wie **OK** oder **Weiter**
  - „Aktivieren" oder „Auswählen" bezieht sich auf Kontrollkästchen bzw. Optionen, die ausgewählt werden müssen, z.B.: Aktivieren Sie die Option **Java-2-Sicherheit erzwingen**

Tools von anderen Anbietern

Einführung

Um die IBM Cúram Social Program Management-Anwendung verwenden zu können, ist es notwendig, Software von anderen Anbietern zu installieren und zu konfigurieren. Genauere Details zu diesen Produkten finden Sie im Dokument *Cúram Supported Prerequisites*.

Es würde über den Umfang dieses Dokuments hinausgehen, zu all den verschiedenen **z/OS**-Softwareprodukten, die für die Unterstützung von WebSphere Application Server for z/OS und DB2 for z/OS benötigt werden, detaillierte Angaben und Anweisungen zu geben. In diesem Kapitel wird lediglich versucht, kurze Details zu der minimal erforderlichen Konfiguration jedes dieser Produkte zu liefern.

In den folgenden Abschnitten werden die Voraussetzungen, Installationshinweise und/oder Konfigurationen nach der Installation für die folgenden Produkte umrissen:

- DB2 for z/OS
- WebSphere Application Server for z/OS
- Apache Ant
- Java™ SE Runtime Environment (JRE) und Java EE

Nachdem die Tools der anderen Anbieter installiert und konfiguriert sind, steht das System für die Konfiguration von WebSphere Application Server for z/OS bereit.

Vor der Installation

Zusätzlich zu den in den Handbüchern *Programmverzeichnis für WebSphere Application Server für z/OS V7.0 (GI11-4295)* und *IBM WebSphere Application Server für z/OS, Version V7.0: Installing your application serving environment (Anwendungsserverumgebung installieren) WebSphere Application Server, Version V7.0 Information Center.* gegebenen Informationen wird für **z/OS** Folgendes empfohlen:

- Hauptspeicher - Er sollte zum Ausführen Ihrer Anwendungen, Factoring in der Anzahl an Benutzern, Leistungsanforderungen usw. geeignet sein
- Speicherplatz für Dateisystem - Es sollte in Ihrem USS-Dateisystem zusätzlicher Speicherplatz für die Cúram-Umgebung und die Implementierung in die Konfiguration von WebSphere Application Server für z/OS eingeplant werden.

DB2 for z/OS

Unterstützte Versionen

Die genaue Version von DB2, die installiert werden sollte, ist im Dokument *Cúram Supported Prerequisites* aufgeführt.

Voraussetzungen

Ziehen Sie das *Programmverzeichnis für IBM DB2 Universal Database für z/OS, Version 8 (GI10-8566) und Version 9 (GI10-8737)* zu Rate.

Installation

Für den Beginn mit der Cúram-Konfiguration und -Installation wird davon ausgegangen, dass DB2 for z/OS erfolgreich mithilfe von SMP/E installiert und die Installation mithilfe der ISPF-Anpassungsfenster konfiguriert worden ist, wie es von der Installation erfordert wird.

Für die Implementierung der Anwendungs-`.ear`-Dateien benötigen Sie die folgenden Informationen:

1. Standortname = *<DB2 Location Name>* - Gibt Ihren Standortnamen für DB2 for z/OS an. Der Standortname sollte während des Systemstarts von DB2 for z/OS (DDF) im **z/OS**-Systemprotokoll angezeigt werden:

   ```
   DSNL004I - DDF START COMPLETE
   LOCATION <DB2 Location Name>
   ```

2. Benutzer-ID = *<database username>* - Stellt eine **z/OS** Benutzer-ID dar, die allen notwendigen Sicherheitszugriff aktiviert hat, um eine Verbindung zur Datenbank von DB2 for z/OS herzustellen und diese zu verwalten
3. Kennwort = *<database password>* - Das Kennwort für *<database username>*

Nach der Installation

Informationen zu diesem Vorgang

Die folgenden Schritte können unter Verwendung der typischen DB2 for z/OS-Schnittstellen wie z.B. SPUFI, DB2 Connect oder Batchbetrieb unter DB2 ausgeführt werden. Geben Sie für die Werte in spitzen Klammern seitenspezifische Werte wie z.B. *<storage_group>* an:

Vorgehensweise

1. Erstellen Sie die notwendige Datenbankspeichergruppe.

   ```
   CREATE STOGROUP <storage_group> VOLUMES (<volumes>)
     VCAT <catalog_name>
   ```

2. Erstellen Sie die Cúram-Anwendungsdatenbank. Diese Datenbank lässt sich für die Modi `EBCDIC`, `ASCII` oder `UNICODE` konfigurieren, was während der Erstel-

lung der Datenbank mithilfe des CCSID-Schlüsselworts geschehen kann. Was ASCII- oder UNICODE-Datenbanken betrifft, finden Sie unter „Bootstrap-Eigenschaften” auf Seite 7 Informationen zum Setzen der erforderlichen Eigenschaft 'curam.db.zos.encoding'.

```
CREATE DATABASE CURAM BUFFERPOOL BP0 INDEXBP BP0
  STOGROUP <storage_group> CCSID <EBCDIC, ASCII or UNICODE>
```

3. Stellen Sie sicher, dass der Parameter DSNZPARM RRULOCK des Makros DSN6SPRM auf YES gesetzt ist.
4. In Ihrer z/OS USS-Shellumgebung muss die Umgebungsvariable 'DB2JCC_LICENSE_CISUZ_JAR' erstellt werden, die auf die installierte Lizenz-JAR-Datei für DB2 for z/OS verweist, die für die Konnektivität zu DB2 for z/OS-Servern unter **z/OS** verwendet wird. Diese Datei wird normalerweise mit db2jcc_license_cisuz.jar benannt und als Teil Ihrer DB2 for z/OS-Installation bereitgestellt.

Ergebnisse

Anmerkung:

Einige Einstellungen des Parametermoduls DSNZPARM müssen möglicherweise angepasst werden, um mit Cúram kompatibel zu sein. Ein besonders wichtiger Parameter ist das Zeitlimit für inaktive Transaktionen (IDTHTOIN). Möglicherweise muss er nach einem Datenbankbuild für bestimmte Aktivitäten, die mit der CER-Initialisierung verbunden sind, erhöht werden, wie z. B. das Ant-Ziel 'prepare.application.data', da dieses länger ausgeführt werden kann, als es normalerweise bei DB2 for z/OS-Anwendungen der Fall ist. Wie viel Zeit diese Aktivitäten in Anspruch nehmen und ob sie das Zeitlimit überschreiten, hängt von einer Anzahl von Faktoren ab, aber ein Anzeichen für den Bedarf an einer solchen Änderung kann sein, dass die Client-Shell eine Fehlermeldung wie diese empfängt:

```
[java] infrastructure:RUN_ID_RUNTIME: A runtime exception occurred:
[jcc][t4][10335][10366][3.63.131] Invalid operation: Connection is closed.
ERRORCODE=-4470, SQLSTATE=08003.
```

Zudem kann im selben Zeitrahmen im z/OS SYSLOG die Zeitlimitnachricht DSNL027I mit dem Ursachencode 00D3003B von DB2 erstellt werden. Die entsprechende DB2 for z/OS-Dokumentation stellt Informationen zum Ändern des Zeitlimitwerts für inaktive Threads bereit.

WebSphere Application Server for z/OS

Unterstützte Versionen

Die genaue Version von WebSphere Application Server for z/OS, die installiert werden sollte, ist im Dokument *Cúram Supported Prerequisites* aufgeführt.

Voraussetzungen

Informationen zu den spezifischen Anforderungen für WebSphere Application Server for z/OS finden Sie im Dokument *Programmverzeichnis für WebSphere Application Server for z/OS V7.0 (GI11-4295)*.

Installation

Für den Beginn mit der Cúram-Konfiguration und -Installation wird davon ausgegangen, dass WebSphere Application Server for z/OS erfolgreich mithilfe der entsprechenden Installationstools installiert worden ist, so wie es von Ihrer Site und von WebSphere Application Server for z/OS erfordert wird.

Die Installation von WebSphere Application Server for z/OS wird in verschiedenen IBM Veröffentlichungen sowie in der Produktdokumentation zu WebSphere Application Server, Version V7.0 erläutert. Die globale Sicherheit erfordert jedoch eine nähere Beschreibung, was im Folgenden geschehen soll.

Globale Sicherheit - Sicherheitseinstellungen konfigurieren: Das Einschalten der globalen Sicherheit von WebSphere Application Server for z/OS wird gelegentlich damit verglichen, dass ein großer Schalter umgelegt wird. Es hat bedeutende Auswirkungen auf das Verhalten Ihres WebSphere Application Server for z/OS-Systems unter z/OS. Aus diesem Grund wird Folgendes dringend empfohlen:

- Machen Sie sich mit der Dokumentation zur Sicherheit von WebSphere Application Server for z/OS vertraut. Insbesondere beschäftigen Sie sich mit diesen Teilen:
  - Die Abschnitte zur Sicherheit im Dokument *WebSphere Application Server for z/OS InfoCenter*
  - IBM WebSphere Application Server for z/OS, Version V7.0: Securing applications and their environment

Man muss sich bewusst sein, dass auch andere Anwendungen, die auf WebSphere Application Server for z/OS laufen, von der eingeschalteten Sicherheit beeinflusst und möglicherweise ihre Funktion verlieren.

Nach der Installation

Folgende Schritte sind auszuführen:

- In Ihrer z/OS USS-Shellumgebung muss die Umgebungsvariable 'WAS_HOME' erstellt werden. Diese sollte auf das Appserver-Verzeichnis der WebSphere Application Server for z/OS-Installation, beispielsweise `/WebSphere/AppServer`, eingestellt sein.

Apache Ant

Übersicht

Apache Ant ist ein Java-basiertes Build-Tool. Für jemanden, der schon mit Tools aus anderen Umgebungen vertraut ist, kann dieses Tool mit dem Maketool verglichen werden.

Unterstützte Versionen

Die genaue Version von Ant, die installiert werden sollte, ist im Dokument *Cúram Supported Prerequisites* aufgeführt.

Installation

Die Ant-ZIP-Datei wird bei Apache angefordert und wie folgt auf Ihrer Maschine in einen Ordner extrahiert:

- Ordnen Sie die Ant-ZIP-Datei im z/OS USS-Dateisystem an, z.B. `/usr/local`, und verarbeiten Sie die Datei beispielsweise folgendermaßen:

  ```
  cd /usr/local
  jar -xf apache-ant-<version>-bin.zip
  ```

  Wobei "<version>" die geeignete Version darstellt, die im Dokument *Cúram v6.0 Supported Prerequisites* angegeben ist.
- Stellen Sie sicher, dass das Ant-Script in `apache-ant-<version>/bin` folgende Eigenschaften aufweist:
  - Das EBCDIC-Format, z.B.:

```
iconv -t IBM-1047 -f ISO8859-1 apache-ant-<version>/bin/ant \
  > /tmp/ant
mv /tmp/ant apache-ant-<version>/bin
```

– Es ist ausführbar, z.B.:

```
chmod a+x apache-ant-<version>/bin/*
```

Nach der Installation
Informationen zu diesem Vorgang

Folgende Schritte sind auszuführen:

Vorgehensweise

1. In Ihrer z/OS USS-Shellumgebung muss die Umgebungsvariable 'ANT_HOME' erstellt werden, die auf das Installationsverzeichnis verweist, das für Ant ausgewählt wurde.
2. Fügen Sie über Ihre PATH z/OS USS-Umgebungsvariable `$ANT_HOME/bin` zum Ausführungspfad hinzu.
3. Erstellen Sie in Ihrer z/OS USS-Shellumgebung eine Systemumgebungsvariable, 'ANT_OPTS', die mindestens auf `-Xmx512m` gesetzt sein sollte.

Ergebnisse

Testen Sie Ant, indem Sie Folgendes ausführen:

```
ant -version
```

In der Ausgabe sollte nun das Versionierungs- und Kompilierungsdatum von Ant angegeben sein.

JRE und Java EE

Übersicht

Sowohl JRE als auch Java EE sind notwendig.

Unterstützte Versionen

Die genauen Versionen, die installiert werden sollten, sind im Dokument *Cúram Supported Prerequisites* aufgeführt.

Installation

Es werden keine speziellen Installationsanweisungen für JRE und Java EE unter **z/OS** bereitgestellt, da WebSphere Application Server for z/OS, Version 7.0 ein integriertes JRE und Java EE zur Verfügung stellt, welches verwendet werden muss. Ziehen Sie für Ihre spezielle Umgebung die entsprechenden von IBM gelieferten Informationen zu Rate.

Nach der Installation

- In Ihrer z/OS USS-Shellumgebung muss die Umgebungsvariable 'JAVA_HOME' erstellt werden, die auf das installierte JRE verweist. '$JAVA_HOME' sollte auf `$WAS_HOME/java` gesetzt sein. `$JAVA_HOME/bin` sollte über Ihre Umgebungsvariable '$PATH' im Pfad angeordnet werden.
- In Ihrer z/OS USS-Shellumgebung muss die Umgebungsvariable 'J2EE_JAR' erstellt werden, die auf die installierte Java EE-JAR-Datei verweist. Diese sollte auf `$WAS_HOME/lib/j2ee.jar` verweisen.

EAR-Dateien erstellen

Einführung

Der wichtigste Schritt vor der Implementierung von IBM Cúram Social Program Management besteht im Paketieren der Anwendung in EAR(Enterprise ARchive)-Dateien. Das Erstellen der Anwendungs-`.ear`-Dateien kann jedoch nicht unter **z/OS** erfolgen, sondern muss unter Windows oder einer anderen Umgebung geschehen, die im Dokument *Cúram Supported Prerequisites* als für die Erstellung unterstützt angegeben ist.

Der Rest dieses Kapitels beschäftigt sich mit den **z/OS**-spezifischen Anforderungen für das Erstellen von **z/OS**-kompatiblen `.ear`-Dateien. Details zum Erstellen von `.ear`-Dateien für IBM Cúram Social Program Management finden Sie im Kapitel 2 des Dokuments *Cúram Deployment Guide for WebSphere Application Server* (Cúram-Implementierungshandbuch für WebSphere Application Server). Hilfreiche Informationen finden Sie möglicherweise auch in den folgenden Handbüchern:

- *Cúram Application Workshop Guide* - In diesem Handbuch werden grundlegende Anweisungen zum Erstellen von Anwendungs-`.ear`-Dateien gegeben
- *Cúram Server Developer's Guide* - In diesem Handbuch werden detaillierte Anweisungen für die Erstellung eines Servers gegeben (Kapitel 3)
- *Cúram Web Client Reference Manual* - In diesem Handbuch werden detaillierte Anweisungen für die Entwicklung eines Web-Clients gegeben, einschließlich Installation und Konfiguration (Kapitel 4)

z/OS-spezifische Notizen zum Erstellen von Anwendungs-EAR-Dateien

In diesen Abschnitten liegt der Schwerpunkt auf den Besonderheiten bei der Erstellung von **z/OS**-kompatiblen `.ear`-Dateien.

Eigenschaftendateien

Für die Erstellung einer IBM Cúram Social Program Management-Anwendung müssen die Dateien `Bootstrap.properties` und `AppServer.properties` ordnungsgemäß für die Ziel-**z/OS**-Plattform gesetzt sein.

Bootstrap-Eigenschaften: Die Datei `Bootstrap.properties` enthält die maschinenspezifischen Konfigurationseigenschaften für den anfänglichen Verbindungsaufbau zur Datenbank. Besondere Aufmerksamkeit sollte auf die folgenden Elemente gerichtet sein:

1. Datenbankeigenschaften:

Tabelle 1. z/OS for DB2-spezifische Datenbankeigenschaften

Eigenschaft	Notizen
curam.db.type	Wert muss auf „zos" gesetzt sein.
curam.db.zos.enableforeignkeys	Muss Ihrer Umgebung entsprechend gesetzt sein („true" oder „false").
curam.db.zos.encoding	Gibt an, ob die unter **z/OS** verwendete Datenbank eine Verarbeitung für EBCDIC, ASCII oder UNICODE erfordert. Sollte auf „EBCDIC", „ASCII" oder „UNICODE" gesetzt sein, je nach verwendeter geeigneter Datenbankcodierung. Standardwert ist „EBCDIC".

Tabelle 1. z/OS for DB2-spezifische Datenbankeigenschaften (Forts.)

Eigenschaft	Notizen
curam.db.zos.dbname	Wert muss der Name der DB2 for z/OS-Datenbank sein.
curam.db.zos.32ktablespace	Wert muss der Name des DB2 for z/OS 32K-Tabellenbereichs sein.
curam.db.username	Wert hängt von der Konfiguration Ihres **z/OS**-Systems ab, wie unter „DB2 for z/OS" auf Seite 3 beschrieben.
curam.db.password	Wert hängt von der Konfiguration Ihres **z/OS**-Systems ab, wie unter „DB2 for z/OS" auf Seite 3 beschrieben. Da es sich hierbei um ein verschlüsseltes Kennwort handelt, muss es durch Ausführung des Ant-Verschlüsselungsziels für jede unterstützte Plattform erstellt werden, z.B. **cd $CURAMSDEJ/bin; ant encrypt -Dpassword=<The password for curam.db.username>**
curam.db.name	Wert ist der DB2 for z/OS-Standortname wie unter „DB2 for z/OS" auf Seite 3 beschrieben.
curam.db.servername	Wert hängt vom Hostnamen (oder der IP-Adresse) Ihres DB2 for z/OS-Systems ab.
curam.db.serverport	Wert hängt von der Konfiguration Ihres DB2 for z/OS-Systems ab.

2. Dateisystemabhängige Eigenschaften:

Tabelle 2. Vom z/OS-Dateisystem abhängige Eigenschaften

Eigenschaft	Notizen
curam.environment.bindings.location	Wert muss ein gültiges Verzeichnis im z/OS USS-Zieldateisystem spiegeln.

Anwendungsserver-Eigenschaften: Besondere Aufmerksamkeit sollte auf die folgenden Elemente gerichtet sein:

1. Portbezogene Eigenschaften von WebSphere Application Server for z/OS werden unter Tabelle 3 erläutert.

Tabelle 3. Porteigenschaften von WebSphere Application Server for z/OS

Eigenschaft	Notizen
curam.server.port	Wert muss mit dem Bootstrap-Port von WebSphere Application Server for z/OS übereinstimmen (siehe „Portzugriff einrichten" auf Seite 37).
curam.client.httpport	Wert muss mit dem Portwert 'CuramClientEndPoint' übereinstimmen (siehe „Portzugriff einrichten" auf Seite 37).
curam.webservices.httpport	Wert muss mit dem Portwert 'CuramWebServicesEndPoint' übereinstimmen (siehe „Portzugriff einrichten" auf Seite 37).

2. Strukturbezogene Eigenschaften von WebSphere Application Server for z/OS werden unter Tabelle 4 erläutert.

Tabelle 4. Strukturbezogene Eigenschaften von WebSphere Application Server for z/OS

Eigenschaft	Notizen
curam.server.host	Wert hängt vom Hostnamen (oder der IP-Adresse) Ihres DB2 for z/OS-Systems ab.
curam.server.name	Wert muss mit dem Namen des Zielservers von WebSphere Application Server for z/OS übereinstimmen.
cell.name	Wert muss mit dem Namen der Zielzelle von WebSphere Application Server for z/OS übereinstimmen.
node.name	Wert muss mit dem Namen des Zielknotens von WebSphere Application Server for z/OS übereinstimmen.
profile.name	Für WebSphere Application Server for z/OS wird nur der standardmäßig eingerichtete Profilname "default" unterstützt.

Cúram-Laufzeit für Installation unter z/OS paketieren

Nach dem Erstellen der `.ear`-Dateien müssen diese und die Laufzeitumgebung für die Installation unter **z/OS** paketiert werden.

Geben Sie dazu beispielsweise unter **Windows** (nachdem Ihre Umgebungskonfiguration entsprechend den Anweisungen im Dokument *Cúram Deployment Guide for WebSphere Application Server* eingerichtet ist) die folgenden Befehle ein:

```
cd %SERVER_DIR%
build release
jar -cf release.zip release
```

Anschließend müssen Sie über eine **FTP**-Verbindung oder durch **Kopieren** die Datei `release.zip` an Ihren **z/OS**-Dateisystemzielort kopieren.

Um die Datei `release.zip` unter **z/OS** zu extrahieren, sollten Sie in Ihrer z/OS USS-Shellumgebung zwei Umgebungsvariablen für diese und nachfolgende Tasks erstellen:

Tabelle 5. Umgebungsvariablen für z/OS USS

Umgebungsvariable	Value
SERVER_DIR	Stellt den Ort dar, an dem Sie `release.zip` extrahieren, z.B.: `/curam/release`.
CURAMSDEJ	Stellt das Verzeichnis zum Ausführen von Erstellungsscripts dar: `$CuramSDEJ`.

Nachdem Sie die Datei `release.zip` in Ihr **z/OS**-System kopiert haben, geben Sie in Ihrer Shellumgebung die folgenden Befehle ein, um sie zu extrahieren:

```
mkdir -p $SERVER_DIR
cd $SERVER_DIR/..
jar -xf <from FTPed location>/release.zip
```

Anwendungsserver konfigurieren

Einführung

Für dieses Kapitel wird vorausgesetzt, dass WebSphere Application Server for z/OS bereits unter **z/OS** installiert worden ist. In „Tools von anderen Anbietern" auf Seite 2 finden Sie Cúram-spezifische Informationen zur Installation von WebSphere Application Server for z/OS.

Die WebSphere-Konfiguration ist für alle Plattformen ähnlich. Zur Unterstützung bei der Konfiguration und Verwaltung der Installation ist eine Anzahl von Ant-Zielen verfügbar. Bei Interesse sind unter „WebSphere Application Server manuell konfigurieren" auf Seite 24 Einzelheiten zu den manuellen Schritten aufgeführt, die von den Konfigurationsscripts durchgeführt werden.

Das vom SDEJ bereitgestellte Konfigurationsziel stellt eine einfache Standardkonfiguration dar und ist für eine Produktionsumgebung möglicherweise ungeeignet.

Anmerkung: Für WebSphere Application Server for z/OS ist nur das Profil *default* verfügbar, eine andere Option ist nicht möglich.

Das Ziel **configure** verwendet das von WebSphere Application Server for z/OS erstellte Profil *default*. Es wird dringend empfohlen, eine Backup-Kopie Ihres Konfigurationsdateisystems für WebSphere Application Server for z/OS einzurichten, für den Fall, dass das Ziel **configure** aus irgendwelchen Gründen erneut ausgeführt werden muss.

Konfiguration von WebSphere Application Server

Zur Konfiguration von WebSphere Application Server for z/OS gehört das Einrichten einer Datenquelle, einer Anzahl von Servern sowie die Konfiguration von JMS und Sicherheitseinstellungen. Alle diese Tasks können durch Ausführen des bereitgestellten Ziels **configure** durchgeführt werden.

Das vom Ant-Ziel **configure** erstellte Profil übernimmt die folgenden Standardwerte. Beim Aufruf des Ziels kann die Eigenschaft 'cell.name' überschrieben werden. Die Eigenschaft 'profile.name' hat möglicherweise keinen anderen Wert als "default", da dies der einzige Wert ist, der von WebSphere Application Server for z/OS unterstützt wird.

- `profile.name=default`
- `cell.name=${node.name}Cell`

Der Befehl **build.sh configure** sollte vom Verzeichnis `$SERVER_DIR` aus ausgeführt werden, damit die automatische Konfiguration aufgerufen wird. Dieses Ziel erfordert, dass die Dateien `AppServer.properties` und `Bootstrap.properties` im Verzeichnis `$SERVER_DIR/project/properties`[1] vorhanden sind. Siehe „Eigenschaftendateien" auf Seite 7 sowie das Dokument *Cúram Server Developer's Guide* zu weiteren Informationen bezüglich der Einrichtung von `Bootstrap.properties`. In „Konfiguration von WebSphere Application Server" werden Beispielinhalte der Datei `AppServer.properties` gezeigt.

1. Es ist möglich, diesen Standardort für die Eigenschaftendatei zu überschreiben, indem man bei der Ausführung des Ziels **configure** -Dprop.file.location=<new location> angibt.

Standardmäßig wird vom Ziel **configure** eine Datenquelle für den DB2 Universaltreiber vom Typ 4 (XA) eingerichtet. Es kann jedoch auch eine Datenquelle für den DB2 Universaltreiber vom Typ 2 (RSS) konfiguriert werden, indem man die Eigenschaft 'curam.db.type2.required' in `AppServer.properties` setzt. Bei Verwendung dieser Eigenschaft müssen Sie die Umgebungsvariable 'DB2DIR' auf Ihren DB2 for z/OS-Installationspfad gesetzt haben.

Es gibt eine Anzahl möglicher Arten, DB2 for z/OS und WebSphere Application Server for z/OS so zu konfigurieren, dass ein Treiber vom Typ 2 unterstützt wird. Lesen Sie hierzu die Produktdokumentation zu WebSphere Application Server Version 7.0 und den Artikel "DB2 Universal JDBC Driver Support" sowie verwandte Informationen.

Es besteht die Möglichkeit, einen Universaltreiber vom Typ 2 zu konfigurieren, indem man die optionale Eigenschaft 'curam.db.zos.jcc.propfile' übergibt und den vollständig qualifizierten Namen einer DB2 for z/OS jcc-Eigenschaftendatei angibt, die in der Servant-JVM-Eigenschaft 'db2.jcc.propertiesFile' gesetzt wird, in der verschiedene Einstellungen wie die Subsystem-ID enthalten sind.

```
## EIGENSCHAFTEN DES ANWENDUNGSSERVERS

# Property to indicate WebSphere is installed.
as.vendor=IBM

# The username and encrypted password for admin server.
security.username=<z.B. websphere>
security.password=<encrypted password>

# The name of the WebSphere Cell.
cell.name=mycell

# The name of the WebSphere Node.
node.name=MyNode

# Name des Servers, auf dem sich die Anwendung befindet.
curam.server.name=CuramServer
curam.server.port=2809

# The alias that should be used for the database authorization
curam.db.auth.alias=dbadmin

# HTTP Port for the server on which the client
# will be accessed
curam.client.httpport=9044

# HTTP Port for the server on which the Web services
# will be accessed
curam.webservices.httpport=9082

# Property to set JVM initial and maximum heap size.
curam.server.jvm.heap.size=1024
```

Abbildung 1. Beispiel für eine Eigenschaftendatei des Anwendungsservers

Standardmäßig setzt das Ziel **configure** die JVM-Initialen und die maximale Größe des Heapspeichers auf "1024" MB. Man kann diese Standardwerte jedoch überschreiben, indem man die Eigenschaft 'curam.server.jvm.heap.size' in der Datei `AppServer.properties` einrichtet.

Für WebSphere Application Server for z/OS muss für die Eigenschaft auch ein Zellenname, 'cell.name', eingeschlossen werden, der gleich dem augeschriebenen Namen der Zelle ist.

Anmerkung:

1. Die Einstellung des Java-Heapspeichers, wie in dem Beispiel unter „Konfiguration von WebSphere Application Server" auf Seite 10 beschrieben und von den Konfigurationsscripts gesetzt, dient nur Anschauungszwecken. Je nach Größe Ihrer angepassten Anwendung, Implementierungsstrategie usw. können diese Einstellungen zu hoch oder zu niedrig sein. Der optimale Wert wird durch das Überwachen der Speicherleistung Ihres Servers bestimmt.
2. Bei den eingeschlossenen Datenbanktreibern von WebSphere Application Server for z/OS können während des Abrufens großer CLOBS und BLOBS (3MB+) aus der Datenbank Speicherprobleme auftreten. Solche Probleme können umgangen werden, indem man auf dem implementierten Server den JVM-Parameter der maximalen Heapspeichergröße angemessen erhöht.

Alternative Speicherpositionen für JAR-Dateien

Bei WebSphere Application Server for z/OS V8 kann eine schreibgeschützte Installationsdatei Probleme mit der Platzierung der Registrierungs- und der Kryptografie-JAR-Dateien von Cúram verursachen (wie in „Anwendungsserver erneut starten" auf Seite 31 beschrieben). Standardmäßig werden diese JAR-Dateien bei jeder Ausführung des Ant-Ziels **configure** in das WebSphere-Konfigurationsdateisystem kopiert (`$JAVA_HOME/lib/ext` und `$WAS_HOME/lib`). Wenn das der Installation zugrundeliegende Dateisystem als schreibgeschütztes System angehängt ist, schlagen diese Kopien fehl und das Dateisystem kann nicht für jeden weiteren Aufruf von **configure** vernünftig mit Lese-/Schreibzugriff angehängt werden. Es ist jedoch möglich, einen symbolischen Link einzurichten, bei dem das Dateisystem einmalig mit Lese-/Schreibzugriff angehängt und ein alternativer Speicherort für die zu kopierenden Dateien angegeben wird.

Diese einmalige Prozedur erfordert die folgenden Schritte:

1. Hängen Sie das Dateisystem der WebSphere-Installation (z. B. `/usr/lpp/zWebSphere/V8R0`) als Dateisystem mit Lese-/Schreibzugriff an.
2. Erstellen Sie im Verzeichnis `lib` von WebSphere für die Cúram-Datei `Registry.jar`, die `CuramLoginModule` enthält, einen symbolischen Link. Beispiel:

```
ln -s /curam/EJBServer/CuramSDEJ/lib/Registry.jar /usr/lpp/zWebSphere/V8R0/lib/Registry.jar
```

3. Erstellen Sie im Verzeichnis `lib/ext` von Java für die Kryptografie-JAR-Datei `CryptoConfig.jar` von Cúram einen symbolischen Link. Beispiel:

```
ln -s /curam/EJBServer/project/properties/CryptoConfig.jar
/usr/lpp/zWebSphere/V8R0/java64/lib/ext/CryptoConfig.jar
```

4. Hängen Sie das Dateisystem der WebSphere-Installation wieder als schreibgeschütztes Verzeichnis an.

Mit den obigen Schritten bleibt Ihr WebSphere-Dateisystem auch weiterhin schreibgeschützt, wenn das Ziel **configure** ausgeführt wird, das diese Dateien an den alternativen Speicherort kopiert, der auf das Dateisystem der Installation verweist. Geben Sie beim Ausführen des Ant-Ziels **configure** die folgenden Eigenschaften an, für die die obigen Beispielspeicherpositionen verwendet wurden:

```
-Dcrypto.ext.dir=/curam/EJBServer/project/properties/
-Dregistry.jar.file.location=/curam/EJBServer/CuramSDEJ/lib/
```

Sicherheitskonfiguration

Die standardmäßig eingerichtete Sicherheitskonfiguration von IBM Cúram Social Program Management in WebSphere Application Server for z/OS beinhaltet die standardmäßige dateibasierte Benutzerregistry sowie ein JAAS-Anmeldemodul. Weitere Details hierzu finden Sie im Abschnitt *Default Configuration for IBM WebSphere Application Server* (Standardkonfiguration für IBM WebSphere Application Server) des Dokuments *Cúram Security Handbook* (Cúram-Sicherheitshandbuch).

Es gibt jedoch eine Reihe alternativer Sicherheitskonfigurationen, die mit WebSphere Application Server for z/OS verwendet werden können. Die Konfigurationen stehen dafür zur Verfügung, die Verwendung von alternativen Authentifizierungsmechanismen wie einem LDAP-Verzeichnisserver oder einer Single Sign-on-Lösung unterstützen.

Um eine andere Konfiguration zu nutzen, sollten die in den folgenden Abschnitten detailliert beschriebenen Eigenschaften in der Datei `AppServer.properties` gesetzt sein, bevor das Ziel `configure` ausgeführt wird. Alternative Authentifizierungsmechanismen sollten manuell konfiguriert werden, nachdem das Ziel `configure` mit den entsprechend gesetzten Eigenschaften ausgeführt worden ist. Um das Anmeldemodul für die Authentifizierung nur anhand der Identität zu konfigurieren, sollte die Eigenschaft 'curam.security.check.identity.only' auf 'true' gesetzt sein. Damit wird sichergestellt, dass der konfigurierte alternative Authentifizierungsmechanismus verwendet wird.

Weitere Details hierzu finden Sie im Abschnitt zur Authentifizierung nur anhand der Identität des Dokuments *Cúram Security Handbook*.

SAF (RACF)-Konfiguration

Wenn Ihr WebSphere Application Server for z/OS-System für die Verwendung von SAF (RACF) konfiguriert werden soll, muss zuerst WebSphere Application Server for z/OS ordnungsgemäß mit dem z/OS Profile Management Tool oder den ISPF-Anpassungsfenstern konfiguriert und anschließend die Eigenschaft 'curam.security.zos.saf' auf 'true' gesetzt werden, bevor das Ziel `configure` ausgeführt wird.

Beim Ausführen des Ziels `configure` ist der Standardwert für die Eigenschaft 'curam.security.user.registry.enabled' auf 'true' gesetzt. Das Überschreiben von 'curam.security.user.registry.enabled' durch Setzen auf 'false' wird nicht empfohlen. Die Eigenschaft 'curam.security.check.identity.only' kann Ihren Anforderungen entsprechend gesetzt werden (siehe unten).

Besondere Konfigurationsschritte bei der Verwendung von 'Authentifizierung nur anhand der Identität' und LDAP

Informationen zu diesem Vorgang

Bei Verwendung der Authentifizierung nur anhand der Identität in Kombination mit WebSphere Application Server for z/OS und LDAP müssen möglicherweise zusätzliche manuelle Konfigurationsschritte durchgeführt werden, unabhängig davon, ob die Konfiguration über die Administrationskonsole von WebSphere Application Server for z/OS oder das Ziel `configure` erfolgt. Wenn Sie bei einer solchen Kombination feststellen, dass WebSphere Application Server for z/OS nicht erfolgreich startet, liegt es daran, dass der Ausschlusslisteneigenschaft (exclude_usernames) des Anmeldemoduls, die in „Anmeldemodul hinzufügen” auf Seite 33 beschrieben wird, ein von WebSphere Application Server for z/OS generierter Benutzername hinzugefügt werden muss. Wenn der Start von WebSphere Application Server for z/OS fehlzuschlagen droht, erscheint zuvor die Fehlernachricht 'SECJ0270E' in der Datei `SystemOut.log`.

Folgende Schritte sind für die Behebung dieses Problems erforderlich:

Vorgehensweise

1. Ermitteln Sie den Benutzernamen, der den Start von WebSphere Application Server for z/OS fehlschlagen lässt. Konfigurieren Sie den Trace des Anmeldemoduls wie in „Authentifizierungsprozess protokollieren” auf Seite 16 (in Bezug auf das Ziel `configure`) oder „Anmeldemodul hinzufügen” auf Seite 33 (in Bezug auf die Konfiguration über die Administrationskonsole) beschrieben, und starten Sie WebSphere Application Server for z/OS erneut. Wenn der Trace des Anmeldemoduls aktiv ist, ermitteln die Trace-Daten vor Erscheinen der SECJ0270E-Fehlermeldung in der Datei `SystemOut.log` den Benutzernamen, der das Fehlschlagen verursacht, und geben einen Eintrag ähnlich dem folgenden aus:

```
SystemOut     O Username: server:MyNodeCell_MyNode_CuramServer
```

   Wobei "MyNode" der Knotenname, "MyNodeCell" der Zellenname und "CuramServer" der Servername des WebSphere Application Server for z/OS ist. Auf die Trace-Daten des Anmeldemoduls folgt der Fehler, der folgendermaßen aussieht:

```
SECJ0270E: Failed to get actual credentials.
   Die Ausnahmebedingung ist 'javax.security.auth.login.LoginException':
   Kontext: MyNodeCell/nodes/MyNode/servers/CuramServer,
   Name: curamejb/LoginHome:
   Erste Komponente im Namen 'curamejb/LoginHome' nicht gefunden.
```

2. Geben Sie den Benutzernamen, der das Fehlschlagen des Starts verursacht, in der Eigenschaft 'exclude_usernames' des Anmeldemoduls in der Konfiguration für WebSphere Application Server for z/OS an. Da sich WebSphere Application Server for z/OS nicht starten lässt, kann diese Änderung nicht über die Administrationskonsole erfolgen, sondern nur über die direkte Bearbeitung der Konfigurationsdatei des WebSphere Application Server for z/OS. Bearbeiten Sie im Konfigurationsdateisystem des WebSphere Application Server for z/OS die Datei `config\cells\MyNodeCell\security.xml`, in der es drei Vorkommen der Eigenschaft 'exclude_usernames' gibt, für jeden Alias eine, z.B.:

```
<options xmi:id="Property_1301940482165"
   name="exclude_usernames"
   value="websphere,db2admin"
   required="false"/>
```

   Alle drei Vorkommen müssen modifiziert werden, so dass sie den neu ermittelten Benutzernamen aus dem obigen Traceeintrag einschließen, z.B.:

```
<options xmi:id="Property_1301940482165"
   name="exclude_usernames"
   value="websphere,db2admin,server:MyNodeCell_MyNode_CuramServer"
   required="false"/>
```

   Beachten Sie, dass in den Vorkommen der Eigenschaft 'exclude_usernames' das `id`-Attribut je nach Ihrer Systemkonfiguration unterschiedlich sein kann und das Kommatrennzeichen des Beispielwertattributs den Standardwert 'curam.security.usernames.delimiter' darstellt, der in Ihrem Fall anders ausfallen kann.
3. Starten Sie WebSphere Application Server for z/OS erneut.

WebSphere Application Server-Benutzerregistry

Standardmäßig wird die konfigurierte Benutzerregistry von WebSphere Application Server for z/OS nicht als Teil der Authentifizierung abgefragt. Das geschieht nur, wenn das Anmeldemodul für eine Authentifizierung nur anhand der Identität konfiguriert ist. Durch Einstellen der Eigenschaft 'curam.security.user.registry.enabled' ist es möglich, dieses Standardverhalten zu überschreiben. Ist diese Eigenschaft auf 'true' gesetzt, wird die Benutzerregistry von WebSphere Application Server for z/OS während des Authentifizierungsprozesses abgefragt, unabhängig davon, ob die Authentifizierung nur anhand der Identität aktiviert oder inaktiviert ist. Ist sie auf 'false' gesetzt, so wird die Benutzerregistry von WebSphere Application Server for z/OS nicht abgefragt. Wenn beispielsweise 'curam.security.check.identity.only' auf 'true' und 'curam.security.user.registry.enabled' auf 'false' gesetzt ist, werden weder die Cúram-Authentifizierungsverifizierungen noch die WebSphere Application Server for z/OS-Benutzerregistry als Teil des Authentifizierungsprozesses verwendet.

Die Authentifizierung von Typen externer Benutzer (d.h. nicht-interner Benutzer) in der WebSphere Application Server for z/OS-Benutzerregistry kann auch mittels der Eigenschaft 'curam.security.user.registry.enabled.types' und/oder der Eigenschaft 'curam.security.user.registry.disabled.types' gesteuert werden. Diese Eigenschaften geben in durch Kommas begrenzten Listen die externen Benutzertypen an, die über die WebSphere Application Server for z/OS-Benutzerregistry authentifiziert bzw. nicht authentifiziert werden:

- Benutzertypen, die in der Liste 'curam.security.user.registry.enabled.types' angegeben sind, werden anhand der WebSphere Application Server for z/OS-Benutzerregistry (z.B. LDAP) und Ihrer `ExternalAccessSecurity`-Implementierung verarbeitet.
- Benutzertypen, die in der Liste 'curam.security.user.registry.disabled.types' angegeben sind, werden nicht anhand der WebSphere Application Server for z/OS-Benutzerregistry verarbeitet, sondern die Verarbeitung Ihrer `ExternalAccessSecurity`-Implementierung wird zur entscheidenden Instanz für die Authentifizierung.

Die Rangfolge für die Verarbeitung dieser drei Eigenschaften und der WebSphere Application Server for z/OS-Benutzerregistry bzw. externen (z.B. LDAP-) Registry ist folgende:

- Standardmäßig wird die WebSphere Application Server for z/OS-Benutzerregistry nicht überprüft und die Authentifizierung der Anwendung verwendet.
- Das Setzen der Eigenschaft 'curam.security.user.registry.enabled' auf `true` erfordert die Authentifizierung sowohl durch die WebSphere Application Server for z/OS-Benutzerregistry bzw. die externe (z.B. LDAP-) Benutzerregistry als auch durch die Anwendungssicherheit (für interne Benutzer) bzw. Ihre `ExternalAccessSecurity`-Implementierung (für externe Benutzer).
- Ein externer Benutzer eines in der Liste 'curam.security.user.registry.enabled.types' angegebenen Typs muss durch die WebSphere Application Server for z/OS-Benutzerregistry bzw. die externe Benutzerregistry sowie durch Ihre `ExternalAccessSecurity`-Implementierung authentifiziert werden.
- Ein externer Benutzer eines in der Liste 'curam.security.user.registry.disabled.types' angegebenen Typs wird nicht durch die WebSphere Application Server for z/OS-Benutzerregistry bzw. die externe Benutzerregistry authentifiziert, sondern Ihre `ExternalAccessSecurity` wird zur entscheidenden Instanz für die Authentifizierung.

Siehe „JAAS-Anmeldemodul für das System einrichten” auf Seite 32 für weitere Informationen zum Einstellen der resultierenden Eigenschaften in der `CuramLoginModule`-Konfiguration.

Authentifizierungsprozess protokollieren

Die optionale Eigenschaft 'curam.security.login.trace' ermöglicht dem Anmeldemodul das Protokollieren. Ist sie auf 'true' gesetzt, führt diese Eigenschaft dazu, dass während des Authentifizierungsprozesses Tracing-Daten zur Datei `SystemOut.log` von WebSphere Application Server for z/OS hinzugefügt werden.

Alternativen Begrenzer zum Ausschließen von Benutzernamen erstellen

Die optionale Eigenschaft 'curam.security.usernames.delimiter' ermöglicht es, einen alternativen Begrenzer für die Benutzernamenliste in der Eigenschaft 'exclude_usernames' einzurichten. Die Eigenschaft kann auf ein Zeichen festgelegt werden, das Benutzernamen mit eingebetteten Kommas wie beim LDAP zulässt.

Caching-Verhalten von WebSphere Application Server

WebSphere Application Server for z/OS speichert Benutzerinformationen und Berechtigungsnachweise in einem Sicherheits-Cache. Solange ein Benutzereintrag in diesem Cache gültig ist, wird das Anmeldemodul der Anwendung nicht aufgerufen. Die standardmäßig eingestellte Inaktivierungszeit beträgt für diesen Sicherheitscache zehn Minuten. Weitere Informationen zu diesem Thema finden Sie im Abschnitt *Caching-Verhalten von WebSphere* des Dokuments *Cúram Security Handbook* (Cúram-Sicherheitshandbuch).

Angepasste Sicherheitseigenschaften

- `com.ibm.ws.security.webChallengeIfCustomSubjectNotFound`

  Diese Eigenschaft bestimmt das Verhalten einer LTPA-Token2-Anmeldung mit Single Sign-on.

  Wenn diese Eigenschaft den Wert 'true' hat, das Token einen angepassten Cache-Schlüssel enthält und das angepasste Subjekt nicht gefunden wird, wird das Token für eine direkte Anmeldung verwendet, weil die angepassten Informationen erneut erfasst werden müssen. Es erscheint eine Aufforderung an den Benutzer zur erneuten Anmeldung. Wenn diese Eigenschaft den Wert 'false' hat und das angepasste Subjekt nicht gefunden wird, wird das LTPA-Token2 für die Anmeldung und das Erfassen aller Registrierungsattribute verwendet. Das Token ist jedoch unter umständen nicht in der Lage, bestimmte Attribute abzurufen, die von Downstream-Anwendungen erwartet werden.

  Standardmäßig setzt das Konfigurationsscript eine WebSphere Application Server for z/OS-Eigenschaft, 'com.ibm.ws.security.webChallengeIfCustomSubjectNotFound', auf `false`, um sicherzustellen, dass Websitzungen nahtlos zwischen zwei Servern eines Clusters übertragen werden können, beispielsweise in einem Übernahmeszenario, ohne dass der Benutzer zur Eingabe von Sicherheitsberechtigungsnachweisen aufgefordert wird. Diese Einstellung ermöglicht, dass das von WebSphere Application Server for z/OS verwendete Sicherheitstoken ordnungsgemäß und ohne Benutzereingabe bewertet wird.

  Ist ein solches Verhalten nicht erforderlich, so ist es möglich, den Wert dieser Eigenschaft in 'true' zu ändern. Weitere Informationen zum Einstellen der *angepassten Sicherheitseigenschaften* finden Sie in „JAAS-Anmeldemodul für das System einrichten” auf Seite 32. Ist der Wert der Eigenschaft auf `true` gesetzt und eine Websitzung wechselt von einem Server zu einem anderen Server innerhalb des Clusters, z.B. aufgrund eines Ausfalls des ursprünglichen Servers, so wird der Benutzer zum Eingeben von Sicherheitsinformationen aufgefordert, bevor er fortfahren kann.

Sicherheitsmaßnahmen zur Abschottung des Systems

Wenn sich ein Benutzer bei der Anwendung anmeldet, gibt er Benutzernamen und Kennwort an. Diese werden an den Server geschickt, der nach erfolgreicher Authentifizierung mit einem eindeutigen Token antwortet. In diesem Fall ist es das 'LTPA-Token'. Es wird für alle nachfolgenden Anforderungen zur Benutzererkennung verwendet und stellt dann privilegierten Inhalt bereit. Man sollte annehmen, dass dieses Token beim Abmelden des Benutzers ungültig wird. Dies ist jedoch nicht der Fall. Es besteht keine Möglichkeit, das LTPA-Token ungültig zu machen, was von IBM bestätigt wurde. **Die Empfehlung von Seiten der IBM ist, die zwei folgenden 'Sicherheitsmaßnahmen zur Abschottung des Systems' vorzunehmen:**

1. Einstellen der Sicherheitsoption 'Erfordert SSL'
2. Einstellen einer angepassten Eigenschaft, mit der LTPA-Cookies auf SSL beschränkt werden.

Diese Änderungen werden mithilfe der Standardkonfigurationsscripts vorgenommen. Die erforderlichen Schritte dazu sind unter „Verwaltungssicherheit konfigurieren” auf Seite 30 beschrieben.

Weitere Informationen finden Sie in:

- http://www.ibm.com/developerworks/websphere/techjournal/1004_botzum/1004_botzum.html?ca=drs#step19
- http://www.ibm.com/developerworks/websphere/techjournal/1004_botzum/1004_botzum.html?ca=drs#step29

Cúram-Kryptografie

Der Begriff der Cúram-Kryptografie bezieht sich auf die Funktionalität für die Verwaltung von Kennwörtern und wird im Dokument *Cúram Security Handbook* ausführlich erläutert, das Sie insbesondere unter Berücksichtigung der folgenden Punkte in Betracht ziehen sollten:

- Bei Produktionsumgebungen wird dringend empfohlen, die Standardeinstellungen zu ändern.
- Bei Entwicklungs- und Testumgebungen müssen Sie abwägen, in welchen Bereichen die Standardwerte ausreichend Schutz in Ihrer Umgebung sicherstellen.
- Für Benutzer, die ein Upgrade von einer Vorgängerversion von IBM Cúram Social Program Management ausführen, funktionieren die vorhandenen Kennwörter nicht ohne Vorbereitungs- oder Anpassungsaufwand. Sie können, wenn Sie bereit sind, ein geringeres Maß an Sicherheit in Kauf zu nehmen, auf eigenes Risiko die entsprechenden Schritte ausführen, um das vorhandene System und die Benutzerkennwörter unverändert zu belassen, doch dies wird nicht empfohlen. Weitere Informationen zu Upgrades enthält das Handbuch *Cúram Upgrade Guide*.

64-Bit-Modus

Bei Verwendung des Ziels **`configure`** kann die Eigenschaft 'curam.zos.64bitmode' in der Datei `AppServer.properties` mit dem Wert 'true' angegeben werden, um den Server für die Unterstützung des 64-Bit-Modus zu konfigurieren.

Anmerkung: Bei Verwendung des 64-Bit-Modus kann es sein, dass Sie auch Ihre JVM-Heapspeichergrößen überprüfen und anpassen müssen, je nach Größe, Durchsatz, Leistungszielen und anderen Faktoren Ihrer Anwendung.

Zeitzonenkonfiguration

Bei der Verwendung mehrerer Servermaschinen müssen alle ihre Taktgeber synchronisiert und auf dieselbe Zeitzone eingestellt sein, so dass die "natürliche" An-

ordnung von Daten und Uhrzeiten in der Datenbank die Reihenfolge der Ereignisse in der realen Welt genau widerspiegelt. Beispiel: Wenn in Datenbanksatz *A* ein Erstellungsdatum oder eine Erstellungszeit früher angegeben ist als in Datensatz *B*, kann man mit Sicherheit sagen, dass *A* vor *B* erstellt wurde, unabhängig davon, welcher Server den einen oder anderen Datensatz erstellt hat.

Die Zeitzone des Servers bzw. der Server darf während der Laufzeit einer Anwendung niemals geändert werden. Der Grund hierfür liegt darin, dass die zum Zeitpunkt der Speicherung der Daten in der Datenbank vorausgesetzte Zeitzone die Zeitzone des aktuellen Servers ist. Wenn also die Zeitzone des Servers geändert wird, dann weichen alle vor der Änderung der Zeitzone eingegebenen Daten um die Stundendifferenz zwischen der neuen und der alten Zeitzone ab.

WebSphere Server starten und stoppen

Zur Unterstützung des Startens und Stoppens von WebSphere Application Server for z/OS-Servern wird eine Reihe von Ant-Zielen bereitgestellt. Diese Ziele sollten vom Verzeichnis `<SERVER_DIR>` aus ausgeführt werden. Was das Ziel **`configure`** betrifft, benötigen sie die Datei `AppServer.properties`, um ordnungsgemäß eingerichtet zu werden (siehe auch „Konfiguration von WebSphere Application Server" auf Seite 10). Ebenso erfordern sie die Angabe einer Anzahl von zusätzlichen Parametern, die unten detailliert aufgeführt sind.

WebSphere Server starten

Das Ant-Ziel zum Starten eines WebSphere Application Server for z/OS-Servers ist **`startserver`**. Es erfordert die folgenden Optionen:

- `-Dserver.name`

  Der Name des zu startenden Servers.

Wichtig: Vor dem ersten Starten des Anwendungsservers muss das Ziel **`database`** ausgeführt worden sein, gefolgt von dem Ziel **`prepare.application.data`**. Werden sie in anderer Reihenfolge ausgeführt, führt das mit einiger Wahrscheinlichkeit zu Transaktionszeitlimits bei der ersten Anmeldung und einem Fehlschlagen der Initialisierung und des Zugriffs auf die Anwendung. Bei jeder erneuten Ausführung des Ziels **`database`** (z.B. in einer Entwicklungsumgebung) muss auch das Ziel **`prepare.application.data`** mit ausgeführt werden.

```
build.sh startserver -Dserver.name=CuramServer
```

Abbildung 2. Anwendungsbeispiel

WebSphere Server stoppen

Das Ant-Ziel zum Stoppen eines WebSphere Application Server for z/OS-Servers ist **`stopserver`**. Es erfordert die folgenden Optionen:

- `-Dserver.name`

  Der Name des zu stoppenden Servers.

```
build.sh stopserver -Dserver.name=CuramServer
```

Abbildung 3. Anwendungsbeispiel

WebSphere Server erneut starten

Das Ant-Ziel zum erneuten Starten eines WebSphere Application Server for z/OS-Servers ist **`restartserver`**. Die Optionen hierfür sind dieselben wie für das Ziel **`startserver`**. Unter „WebSphere Server starten" finden Sie ein Anwendungsbeispiel.

Anmerkung: Wenn der Server beim Neustartversuch nicht bereits gestartet ist, bewirkt der Sperrabschnitt des Ziels kein Fehlschlagen des Neustart-Ziels.

Implementierung

Einführung

Der letzte Schritt nach dem Paketieren der IBM Cúram Social Program Management-Anwendung und der Web-Service-Anwendung in `.ear`-Dateien und nach dem Konfigurieren von WebSphere Application Server for z/OS besteht in der Implementierung der `.ear`-Dateien im Anwendungsserver.

Vor der Implementierung ist es wichtig zu beachten, dass bei WebSphere Application Server for z/OS die mit IBM Cúram Social Program Management gelieferten Konfigurationsscripts eine einfache Konfiguration unterstützen, die auf eine Basisserver-Installation von WebSphere Application Server for z/OS ausgerichtet ist.

Die Implementierung beinhaltet:

- Erstellen von Eigenschaftendateien
- Installieren der `.ear`-Dateien
- Erstellen einer Datenbank
- Optional, aber dringend empfohlen, das Vorkompilieren der JSPs
- Testen der Anwendung

Eigenschaftendateien

Um mithilfe von Ant Anwendungs-`.ear`-Dateien installieren zu können, müssen Sie in Ihrem Verzeichnis `$SERVER_DIR/project/property` über geeignete Eigenschaftendateien verfügen. Dabei handelt es sich um die Dateien

- `Bootstrap.properties` - Zur Datenbankerstellung
- `AppServer.properties` - Zur Installation von `.ear`-Dateien

In diesem Abschnitt soll umrissen werden, was diese Dateien enthalten müssen. Weitere Informationen finden Sie im Dokument *Cúram Server Developer's Guide*.

Die Datei 'bootstrap.properties'

Spezifische oder relevante Implementierungseigenschaften für WebSphere Application Server for z/OS werden in „Die Datei 'bootstrap.properties'" erläutert.

```
# DATABASE-SPECIFIC (DB2 for z/OS)
curam.db.type=ZOS
curam.db.zos.encoding=EBCDIC
curam.db.zos.enableforeignkeys=false
curam.environment.bindings.location=
  /<Value of $SERVER_DIR>/project/properties

curam.db.username=<database username>
curam.db.password=<encrypted database password>

curam.db.name=<DB2 Location Name>
curam.db.servername=<host name>
curam.db.serverport=<DB2 port>

curam.db.zos.dbname=CURAM
curam.db.zos.32ktablespace=CURAMTS
```

Abbildung 4. Implementierungsbezogene 'bootstrap.properties'-Datei

Einige dieser Eigenschaften werden in „Bootstrap-Eigenschaften" auf Seite 7 beschrieben. Es sind dieselben, die Sie auch für den Aufbau von IBM Cúram Social Program Management für Windows für die Implementierung unter z/OS benötigen. Beachten Sie jedoch den folgenden Hinweis:

- Bei dem Wert *<Value of $SERVER_DIR>* handelt es sich um den Wert für Ihre Umgebungsvariable '$SERVER_DIR'.

Die Datei 'AppServer.properties'

Spezifische oder relevante Implementierungseigenschaften für WebSphere Application Server for z/OS werden in „Die Datei 'AppServer.properties'" erläutert.

```
# Property to indicate WebSphere
as.vendor=IBM

# The name of the WebSphere Cell.
cell.name=mycell

# The name of the WebSphere Node.
node.name=mynode

# Name des Servers, auf dem sich die Anwendung befindet.
curam.server.name=CuramServer
```

Abbildung 5. Implementierungsbezogene Anwendungsserver-Eigenschaftendatei

Einige dieser Eigenschaften werden in „Anwendungsserver-Eigenschaften" auf Seite 8 beschrieben. Es sind dieselben, die Sie auch für die Erstellung der Anwendungs-`.ear`-Dateien von IBM Cúram Social Program Management für die Implementierung unter z/OS benötigen.

Konfiguration überprüfen

Sie können Ihre Eigenschaftendateien und die Konfiguration überprüfen, indem Sie das Ant-Ziel **`configtest`** ausführen.

Führen Sie das Ziel **`configtest`** wie folgt von der Shell aus durch:

```
cd $CURAMSDEJ/bin
ant configtest
```

Überprüfen Sie die Ausgabe auf Fehler oder Warnungen und beheben Sie diese.

Implementierung

Es gibt Ant-Ziele zum Installieren und Deinstallieren von Anwendungen auf einem WebSphere Application Server for z/OS-Server. Wie auch die Ziele **`startserver`** und **`stopserver`**, erfordern die Ziele **`installapp`** und **`uninstallapp`** dass die Datei `AppServer.properties` ordnungsgemäß konfiguriert ist (siehe „Konfiguration von WebSphere Application Server" auf Seite 10). Diese Ziele erfordern auch die Angabe einer Anzahl von Optionen, die unten aufgeführt sind.

Stellen Sie sicher, dass vor der Installation der Anwendung der Server gestartet worden ist. Da das Installationsziel die Anwendung automatisch startet, muss der Server nach der Installation nicht erneut gestartet werden.

Anwendung installieren

Das Ant-Ziel für die Installation einer Anwendung (in Form einer `.ear`-Datei) ist **`installapp`**. Es erfordert die folgenden Optionen:

- `-Dserver.name`

  Der Name des Servers, der die Anwendung installieren soll.

- `-Dear.file`

  Der vollständig qualifizierte Name der zu installierenden `.ear`-Datei.
- `-Dapplication.name`

  Der Name der Anwendung.

```
build.sh installapp -Dserver.name=CuramServer
 -Dear.file=/ear/Curam.ear
 -Dapplication.name=Curam
```

Abbildung 6. Anwendungsbeispiel

Anmerkung: Die `.ear`-Datei, die das Servermodul enthält, muss installiert werden, bevor irgendeine andere (nur-Client) EAR-Datei installiert wird.

Um zusätzliche Argumente an das WebSphere-Tool 'wsadmin' zu übergeben, steht die optionale Ant-Eigenschaft namens `wsadmin.extra.args` zur Verfügung. Mit dem folgenden Befehl werden zum Beispiel neue Größenangaben für den Java-Heapspeicher festgelegt und die Option zum Anhängen von Tracing mit wsadmin übergeben:

```
-Dwsadmin.extra.args="-javaoption -Xms1024m -javaoption -Xmx1024m -appendtrace true"
```

Abhängig von Ihrer Shell müssen Sie den Anführungszeichen möglicherweise Escape-Zeichen wie im folgenden Beispiel voranstellen: **`-Dwsadmin.extra.args=\"-appendtrace true\"`**. Diese Eigenschaft sollte nicht verwendet werden, um Argumente anzugeben, die bereits über die Ant-Scripts von Cúram übergeben wurden. Welche Argumente bei der Ausführung von Ant übergeben werden, können Sie feststellen, wenn Sie mit der Option `-v` die ausführliche Anzeige anfordern.

SYSTEM-Benutzernamen ändern

Es wird dringend empfohlen, den Benutzernamen für den JMS-Aufruf im Zuge der Implementierung der Anwendung zu ändern. Um diesen Benutzernamen ändern zu können, sollten vor der Implementierung die folgenden Eigenschaften in der Datei `AppServer.properties` gesetzt sein:

- curam.security.credentials.async.username

  Der Benutzername, unter dem die JMS-Aufrufe ausgeführt werden sollten.
- curam.security.credentials.async.password

  Das verschlüsselte Kennwort, das dem Benutzernamen zugehörig ist. Das Kennwort sollte mithilfe des Ant-Ziels **`encrypt`** verschlüsselt werden. Im Dokument *Cúram Server Developers Guide* finden Sie hierzu weitere Informationen.

Der Benutzername kann auch geändert werden, nachdem die Anwendung mithilfe der Administrationskonsole von WebSphere Application Server for z/OS implementiert worden ist. Navigieren Sie dafür zu **Anwendungen** > **Anwendungstypen** > **WebSphere-Unternehmensanwendungen** und wählen Sie die Anwendung aus. Wählen Sie den Link **RunAs-Rollen für Benutzer** aus. Aktivieren Sie die Rolle `everyone` (jeder), geben Sie einen neuen Benutzernamen und ein neues Kennwort ein (wobei zu beachten ist, dass das Kennwort hier in unverschlüsseltem Format eingegeben werden sollte) und klicken Sie auf die Schaltfläche **Anwenden**. Speichern Sie die Änderungen wie unter „Masterkonfiguration speichern" auf Seite 30 im Detail beschrieben.

Beachten Sie, dass nach dem Ändern des Benutzernamens der neue Benutzername in der Benutzerdatenbanktabelle vorhanden sein und dieser Benutzer die Rolle 'SUPERROLE' besitzen muss.

Der SYSTEM-Benutzer ist der Benutzer, unter dem die JMS-Nachrichten ausgeführt werden.

Anwendung deinstallieren

Das Ant-Ziel zum Deinstallieren einer Anwendung ist **uninstall**. Es erfordert die folgenden Optionen:

- `-Dserver.name`

  Der Name des Servers, auf dem die Anwendung installiert ist.

- `-Dapplication.name`

  Der Name der Anwendung, die deinstalliert werden soll (wie bei der Installation konfiguriert).

```
build.sh uninstallApp -Dserver.name=CuramServer
-Dapplication.name=Curam
```

Abbildung 7. Anwendungsbeispiel

JSPs vorkompilieren

Es ist während der Implementierung ein zusätzliches Ziel verfügbar, **precompilejsp**, das es ermöglicht, die JSPs einer Client-`.ear`-Datei *vor* der Installation der `.ear`-Datei vorzukompilieren. Das Vorkompilieren der JSPs vor der Installation beschleunigt das Anzeigen einer bestimmten Anzeige im Web-Browser beim ersten Zugriff darauf.

Die Optionen für das Ziel **precompilejsp** sind:

- `-Dear.file`

  Der vollständig qualifizierte Name der vorzukompilierenden `.ear`-Datei.

```
build.sh precompilejsp -Dear.file=$SERVER_DIR/ear/WAS/Curam.ear
```

Abbildung 8. Anwendungsbeispiel

Anmerkung: Dies ist eine lang andauernde Aktivität, die je nach den Kapazitäten Ihres Systems einige Stunden in Anspruch nehmen könnte. Stellen Sie sicher, dass Ihre Task nicht hinsichtlich der verfügbaren CPU-Zeit deutlich eingeschränkt ist und dass im Dateisystem '$CURAMSDEJ' ausreichend Platz vorhanden ist.

Auch kann bei der Ausführung des Ziels **precompilejsp** für WebSphere Application Server for z/OS eine Ausnahme wegen abnormaler Speicherbedingungen auftreten (oder es werden einige JSPS im Hintergrund ignoriert und nicht vorkompiliert). Zur Fehlerumgehung sollte das Script `JspBatchCompiler.sh` im Verzeichnis `$WAS_HOME/bin` dahingehend geändert werden, dass die maximale Speichergröße erhöht wird. Ändern Sie die Speicherbelegung von `-Xmx256m` auf mindestens `-Xmx1024m`.

Datenbank erstellen

Um die IBM Cúram Social Program Management-Anwendung verwenden zu können, müssen Sie eine Datenbank erstellen und initialisieren. Für diesen Abschnitt wird davon ausgegangen, dass Sie das Ant-Ziel **database** verwenden, um eine Datenbank zu erstellen. Es ist jedoch auch möglich, DB2-Client-Tools hierfür zu verwenden. Siehe das Dokument *Cúram Installation Guide* für weitere Details zu dieser Methode.

```
cd $CURAMSDEJ/bin
ant database
```

Abbildung 9. Beispiele für Shellbefehle zum Erstellen einer Datenbank

Implementierung testen

Nachdem die `.ear`-Datei(en) der IBM Cúram Social Program Management-Anwendung auf einem konfigurierten WebSphere Application Server for z/OS installiert ist/sind[2], besteht der nächste Schritt darin, die Anwendung zu starten und zu testen.

Stellen Sie sicher, dass der entsprechende Server gestartet ist[3], und öffnen Sie in einem Web-Browser die folgende Seite:

`https://<some.machine.com>:<port>/<context-root>`

Wobei

<*some.machine.com*> den Hostnamen oder die IP-Adresse angibt, unter dem/der Ihr WebSphere Application Server for z/OS-System läuft, <*port*> den Server-Port angibt, auf dem die Client-Anwendung implementiert ist (wie in „Portzugriff einrichten" auf Seite 37) und <*context-root*> das Kontextstammverzeichnis des WAR-Moduls angibt.

Bevor die Seite geöffnet werden kann, wird der Browser zur Anmeldeseite geleitet. Melden Sie sich mit einem gültigen Cúram-Benutzernamen und Kennwort an, woraufhin der Browser zur angeforderten Seite umgeleitet wird.

Anmerkung: Die Verwendung des EAR-Dateinamens `Curam.ear` für die Option `-Dear.file` und des Anwendungsservernamens `Curam` für die Option `-Dapplication.name` in den Beispielen dieses Kapitels dient Anschauungszwecken. Diese Werte können je nach Ihrer angepassten Anwendung und Implementierungsstrategie unterschiedlich sein.

IBM WebSphere Application Server mit der USGCB verwenden

Bei der "United States Government Configuration Baseline" (Konfigurationsbaseline der Regierung der Vereinigten Staaten, USGCB) handelt es sich um eine Initiative der US-Regierung zur Bereitstellung von Anleitungen für Behörden mit dem Ziel der Verbesserung von Konfigurationseinstellungen, vor allem im Bereich der Sicherheit. Bei der Ausführung der Anwendung IBM Cúram Social Program Management unter Verwendung von IBM WebSphere Application Server V7 (siehe dazu das Handbuch *IBM Cúram Social Program Management v6 Supported Prerequisites* zu unterstützten Versionen von IBM WebSphere Application Server V7) mit USGCB-Einstellungen kann es vorkommen, dass Grafiken fehlen. Das Auftreten eines solchen Fehlers zeigt an, dass IBM WebSphere Application Server keine PNG-Dateien erkennt. Zur Behebung dieses Problems muss IBM WebSphere Application Server aktualisiert werden, so dass er den PNG-MIME-Typ unterstützt. Nähere Einzelheiten hierzu finden Sie in der Dokumentation des *WebSphere Application Server Information Center*.

Weitere Informationen zur USGCB finden Sie auf der folgenden Website: http://usgcb.nist.gov/

2. Die Installation einer Web-Services-Anwendung kann ebenfalls erforderlich sein.

3. Nach dem Implementieren einer Anwendung muss der Server nicht erneut gestartet werden.

WebSphere Application Server manuell konfigurieren

Einführung

In diesem Abschnitt werden die manuellen Schritte beschrieben, die zum Konfigurieren und Implementieren auf einer Basisanwendungsserver-Installation von WebSphere Application Server for z/OS erforderlich sind. Diese Schritte müssen für eine Implementierung in einer Network Deployment-Installation von WebSphere Application Server for z/OS angepasst werden. Unter „WebSphere Network Deployment" auf Seite 48 finden Sie weitere Informationen zu diesem Bereich.

WebSphere Application Server manuell konfigurieren

Die IBM WebSphere Application Server for z/OS-Installation kann bei Bedarf manuell konfiguriert werden, jedoch ist dies bei Verwendung einer Basisanwendungsserver-Installation nicht zu empfehlen. Die in diesem Abschnitt detailliert beschriebenen manuellen Schritte für die Konfigurierung von WebSphere Application Server for z/OS dienen lediglich Informationszwecken.

Es wird darauf hingewiesen, dass alle Einstellungen, die unter dem Abschnitt **Ressourcen** der Administrationskonsole vorgenommen werden, auf mehreren Ebenen konfiguriert werden können, die den JNDI-Bereich steuern. Das kann eine Zelle, ein Knoten oder ein Server sein. Nach der Auswahl einer **Ressource** wird dieser Bereich oben im Hauptbrowserfenster angezeigt, wodurch es möglich ist, die verschiedenen Ressourcen im aktuellen Bereich anzuzeigen. Der Bereich und damit die Speicherposition aller eingestellten Ressourcen sollte auf der geplanten Verwendung beruhen. Wenn in einem Cluster gearbeitet wird, ist es möglicherweise nicht notwendig, für jeden Server dieselben Einstellungen einzugeben, und der Bereich kann auf Zelle oder Knoten gesetzt werden.

Administrationskonsole

Ein Großteil der Konfiguration für WebSphere Application Server for z/OS wird mithilfe der WebSphere-Administrationskonsole erstellt. Um die Administrationskonsole auszuführen, muss erst der Server im Standardprofil gestartet werden, da die Administrationskonsole als Webanwendung für diesen Server installiert ist (weitere Informationen zum Starten von Servern finden Sie unter „WebSphere Server starten und stoppen" auf Seite 18).

Um die Administrationskonsole zu öffnen, sollte der Web-Browser auf die folgende Adresse verweisen:

```
http://<Your WebSphere host>:<protocol_http_port>/ibm/console
```

Wobei

<Your WebSphere host> den Hostnamen oder die IP-Adresse angibt, unter dem/der Ihr WebSphere Application Server for z/OS-System läuft, und *<protocol_http_port>* den Port angibt, der in Ihrer Installation und Anpassung von WebSphere Application Server for z/OS zugewiesen ist.

Unterstützung zum Erstellen von Scripts

Um die Ausführung der bereitgestellten Ant-Scripts zu unterstützen, sind in den Eigenschaftendateien von WebSphere Application Server for z/OS Änderungen notwendig.

sas.client.props: Öffnen Sie die Datei `sas.client.props`, die sich im Verzeichnis `profiles/default/properties` der WebSphere Application Server for z/OS-Installa-

tion befindet. Um nicht bei jeder Ausführung der Scripts den Benutzernamen und das Kennwort eingeben zu müssen, ist es notwendig, die Anmeldequelle so einzurichten, dass sie Benutzernamen und Kennwort aus einer Eigenschaftendatei abruft. Setzen Sie die folgenden Eigenschaften oder fügen Sie sie bei Bedarf hinzu:

```
com.ibm.CORBA.loginSource=properties
# RMI/IIOP user identity
com.ibm.CORBA.loginUserid=websphere
com.ibm.CORBA.loginPassword=websphere
```

Wobei *websphere* sowohl Benutzername als auch Kennwort für die Administrationskonsole ist.

soap.client.props: Öffnen Sie die Datei `soap.client.props`, die auch im Verzeichnis `profiles/default/properties` der WebSphere Application Server for z/OS-Installation zu finden ist. Um nicht bei jeder Ausführung der Scripts den Benutzernamen und das Kennwort eingeben zu müssen, ist es notwendig, die Anmeldequelle so einzurichten, dass sie Benutzernamen und Kennwort aus einer Eigenschaftendatei abruft. Geben Sie die folgenden Eigenschaften so an, dass sie mit den für WebSphere wie in „Konfiguration von WebSphere Application Server" auf Seite 10 konfigurierten Berechtigungsnachweisen übereinstimmen. Bei den Werten in dem nachfolgenden Beispiel handelt es sich einfach um Beispielwerte und das in dieser Datei angegebene Kennwort kann nicht verschlüsselt werden:

```
com.ibm.SOAP.loginUserid=websphere
com.ibm.SOAP.loginPassword=websphere
```

Wobei *websphere* sowohl Benutzername als auch Kennwort für die Administrationskonsole ist.

Um Zeitlimitüberschreitungen bei der Installation von `.ear`-Dateien zu vermeiden, sollte folgender Wert entsprechend gesetzt sein, z. B.:

```
com.ibm.SOAP.requestTimeout=3600
```

Je nach Leistung Ihrer Umgebung könnte ein anderer Wert notwendig sein.

server.policy: Öffnen Sie die Datei `server.policy`, die im Verzeichnis `profiles/default/properties` der WebSphere Application Server for z/OS-Installation zu finden ist. Fügen Sie am Ende dieser Datei die folgenden Zeilen hinzu:

```
grant codeBase "file:<CURAMSDEJ>/drivers/-" {
permission java.security.AllPermission;
};
```

Wobei *<CURAMSDEJ>* das SDEJ-Installationsverzeichnis bezeichnet.

```
grant codeBase "file:${was.install.root}/
profiles/default/installedApps/
<cell.name>/<SERVER_MODEL_NAME>.ear/
guice-2.0.jar" { permission java.lang.RuntimePermission
"modifyThread"; permission java.lang.RuntimePermission
"modifyThreadGroup"; },
```

Wobei *<cell.name>* der Name der Zielzelle von WebSphere Application Server for z/OS

und *<SERVER_MODEL_NAME>* der Name der Anwendungs-`.ear`-Datei ist.

Datenquellen-Anmeldealias erstellen

Informationen zu diesem Vorgang

Die für z/OS unterstützte Datenbank ist DB2 for z/OS. Die WebSphere Application Server for z/OS-Administrationskonsole wird dazu verwendet, einen Anmeldealias für die DB2 for z/OS-Datenquellen wie folgt einzurichten:

Vorgehensweise

1. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
2. Erweitern Sie die Option **Java Authentication and Authorization Service** im Feld **Authentifizierung** und wählen Sie die Option **JAAS-J2C-Authentifizierungsdaten**.
3. Klicken Sie auf die Schaltfläche **Neu**, um die Konfigurationsanzeige zu öffnen.
4. Setzen 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 die Schaltfläche **OK**, um die Änderungen zu bestätigen.

DB2 for z/OS-Datenquellen konfigurieren

Unter **z/OS** haben Sie die Wahl, ob Sie für die Konfigurierung den DB2 JDBC Universal Driver Typ 4 (XA) oder den DB2 JDBC Universal Driver Typ 2 (RRS) verwenden.

Für einen Typ-4-JDBC Universal Driver (XA) konfigurieren:

DB2 for z/OS für Umgebungsvariable einrichten

1. Navigieren Sie zu **Umgebung** > **WebSphere-Variablen**.
2. *Hinweis:* An dieser Stelle sollte der geeignete Bereich ausgewählt werden, in dem die Datenquelle definiert werden soll.
3. Wählen Sie den Link 'DB2UNIVERSAL_JDBC_DRIVER_PATH' aus der Liste von Umgebungsvariablen aus. Damit wird die Konfigurationsanzeige für diese Variable geöffnet.
4. Setzen Sie das Feld **Wert** so, dass es auf das Verzeichnis verweist, in dem die Typ-4-Treiber enthalten sind. Das ist normalerweise das Cúram-SDEJ`Treiber`-Installationsverzeichnis, z.B. `/CuramSDEJ/drivers`.
5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu bestätigen.

Anbieter für Datenbanktreiber einrichten

1. Navigieren Sie zu **Ressourcen** > **JDBC** > **JDBC-Provider**.
2. *Hinweis:* An dieser Stelle sollte der geeignete Bereich ausgewählt werden, in dem die Datenquelle definiert werden soll.
3. Klicken Sie auf die Schaltfläche **Neu**, um einen neuen Treiber hinzuzufügen. Damit öffnet sich eine Konfigurationsanzeige.
4. Wählen Sie den Eintrag **DB2** aus der Dropdown-Liste **Datenbanktypen** aus, die angezeigt wird.

5. Wählen Sie den Eintrag **DB2 Universal JDBC Driver Provider** aus der Dropdown-Liste von **Providertypen** aus, die angezeigt wird.
6. Wählen Sie den Eintrag **XA-Datenquelle** aus der Dropdown-Liste von **Implementierungstypen**aus, die angezeigt wird.
7. Klicken Sie auf die Schaltfläche **Weiter**, um fortzufahren.
8. Überprüfen Sie die Eigenschaften in der Konfigurationsanzeige, die geöffnet wird. Ändern Sie die Klassenpfadzeile `${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar` dahingehend, dass sie auf die DB2 for z/OS-Lizenz verweist, die von IBM für die z/OS-Konnektivität bereitgestellt wird, und klicken Sie auf **Anwenden**;
9. Klicken Sie auf die Schaltfläche **Weiter** und anschließend auf die Schaltfläche **Fertigstellen**, um die Änderungen zu bestätigen.

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

   Datenquellenname: <*DatasourceName*>

   JNDI-Name: *jdbc/*<*DatasourceName*>

   Klicken Sie auf **Weiter**.
5. Setzen Sie die Felder wie folgt:

   Treibertyp: 4

   Datenbankname: Der Name der DB2 for z/OS-Datenbank

   Servername: Der Name des DB2-Datenbankservers

   Portnummer: Der DB2 for z/OS-Datenbankserverport

   Lassen Sie alle anderen Felder unverändert, es sei denn, es ist eine bestimmte Änderung erforderlich. Klicken Sie auf **Weiter**.
6. Setzen Sie die Felder wie folgt:

   Setzen Sie den Wert aus der Drop-down-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 „Datenquellen-Anmeldealias erstellen” auf Seite 26 eingerichtet wird.

   Lassen Sie alle anderen Felder unverändert, es sei denn, es ist eine bestimmte Änderung erforderlich. Klicken Sie auf **Weiter**.
7. Klicken Sie auf die Schaltfläche **Fertigstellen**, um die Änderungen zu bestätigen und fortzufahren.
8. Wählen Sie die neu erstellte Datenquelle *DatasourceName* aus der angezeigten Liste.

9. Wählen Sie den Link **Angepasste Eigenschaften** unter **Weitere Eigenschaften**.
10. Wählen Sie den Eintrag `fullyMaterializeLobData`.
11. Setzen Sie den `Wert` auf `false`.
12. Klicken Sie auf die Schaltfläche **OK**, um die Änderung zu bestätigen.

Typ-2-JDBC Universal Driver (RRS) konfigurieren:

DB2-Umgebungsvariablen einrichten

1. Navigieren Sie zu **Umgebung** > **WebSphere-Variablen**.
2. *Hinweis:* An dieser Stelle sollte der geeignete Bereich ausgewählt werden, in dem die Datenquelle definiert werden soll.
3. Wählen Sie den Link 'DB2UNIVERSAL_JDBC_DRIVER_PATH' aus der Liste von Umgebungsvariablen aus. Damit wird die Konfigurationsanzeige für diese Variable geöffnet.
4. Setzen Sie das Feld **Wert** so, dass es auf das Verzeichnis verweist, in dem der Typ-2-Treiber enthalten ist. Das ist normalerweise der DB2-Installationspfad, der die Datei `db2jcc.jar` enthält.
5. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu bestätigen.
6. Wählen Sie den Link 'DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH' aus der Liste von Umgebungsvariablen aus. Damit wird die Konfigurationsanzeige für diese Variable geöffnet.
7. Setzen Sie das Feld **Wert** so, dass es auf das Verzeichnis verweist, welches die DB2 for z/OS-Links für die gemeinsam genutzte Bibliothek für den Typ-2-Treiber enthält. Dies ist der DB2 for z/OS-Installationspfad, der die Typ-2-Treiberbibliotheken (wie z.B. `libdb2jcct2zos.so`, was je nach Version von DB2 for z/OS sowie 31/64-Bit-Implementation unterschiedlich sein kann) enthält.
8. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu bestätigen.

Anbieter für Datenbanktreiber einrichten

1. Navigieren Sie zu **Ressourcen** > **JDBC** > **JDBC-Provider**.
2. *Hinweis:* An dieser Stelle sollte der geeignete Bereich ausgewählt werden, in dem die Datenquelle definiert werden soll.
3. Klicken Sie auf die Schaltfläche **Neu**, um einen neuen Treiber hinzuzufügen. Damit öffnet sich eine Konfigurationsanzeige.
4. Wählen Sie den Eintrag **DB2** aus der Dropdown-Liste **Datenbanktypen** aus, die angezeigt wird.
5. Wählen Sie den Eintrag **DB2 Universal JDBC Driver Provider** aus der Dropdown-Liste von **Providertypen** aus, die angezeigt wird.
6. Wählen Sie den Eintrag **Datenquelle des Verbindungspools** aus der Dropdown-Liste von **Implementierungstypen**aus, die angezeigt wird.
7. Klicken Sie auf die Schaltfläche **Weiter**, um fortzufahren.
8. Überprüfen Sie die Eigenschaften auf der Konfigurationsanzeige, die sich öffnet, und stellen Sie sicher, dass die Einstellungen für Klassenpfad und Pfad der nativen Bibliothek korrekt sind und auf den Werten beruhen, die zuvor für die Umgebungsvariablen 'DB2UNIVERSAL_JDBC_DRIVER_PATH' und 'DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH' gesetzt wurden. Es sollten keine Änderungen erforderlich sein.
9. Klicken Sie auf die Schaltfläche **Weiter** und anschließend auf die Schaltfläche **Fertigstellen**, um die Änderungen zu bestätigen.

Datenquelle für Datenbanktreiber einrichten

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

1. Wählen Sie die Option `DB2 Universal JDBC Driver Provider` aus, die jetzt in der Liste **JDBC-Provider** angezeigt wird. Damit wird die Konfigurationsanzeige für den Anbieter (Provider) geöffnet.
2. Wählen Sie den Link **Datenquellen** unter **Weitere Eigenschaften**.
3. Klicken Sie auf die Schaltfläche **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:

   Datenbankname:: Name der DB2 for z/OS-Datenbank

   Treibertyp: 2

   Lassen Sie alle anderen Felder unverändert, es sei denn, es ist eine bestimmte Änderung erforderlich. Klicken Sie auf **Weiter**.
7. Setzen Sie die Felder wie folgt:

   Setzen Sie den Wert aus der Drop-down-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 „Datenquellen-Anmeldealias erstellen" auf Seite 26 eingerichtet wird.

   Lassen Sie alle anderen Felder unverändert, es sei denn, es ist eine bestimmte Änderung erforderlich. Klicken Sie auf **Weiter**.
8. Klicken Sie auf die Schaltfläche **Fertigstellen**, um die Änderungen zu bestätigen und fortzufahren.
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 die Schaltfläche **OK**, um die Änderung zu bestätigen.

Richten Sie die JVM-Eigenschaft 'db2.jcc.propertiesFile' ein (optional).

Wenn Sie für Ihren DB2 Typ 2 Universal JDBC-Treiber eine externe Konfigurationsdatei verwenden möchten, die von der Eigenschaft 'db2.jcc.propertiesFile' ermittelt wird, gehen Sie dazu wie folgt vor:

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Erweitern Sie im Fenster **Serverinfrastruktur** die Option **Java- und Prozessverwaltung**.
4. Wählen Sie den Link **Prozessdefinition** aus.

5. Führen Sie im Fenster **Prozesstyp** die folgenden Schritte für jedes Element in der Liste aus (Adjunct, Controller und Servant):
   a. Wählen Sie den Link **Prozesstyp** aus.
   b. Wählen Sie im Fenster **Weitere Eigenschaften** den Link **Java Virtual Machine** aus.
   c. Wählen Sie im Fenster **Weitere Eigenschaften** den Link **Angepasste Eigenschaften** aus.
   d. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie die Eigenschaft wie folgt:

      Name: db2.jcc.propertiesFile

      Wert: fully qualified name of the property file

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

      Ziehen Sie auch die Informationen in „Konfiguration von WebSphere Application Server" auf Seite 10 zum Einrichten der Eigenschaftendatei zu Rate.

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.

Verwaltungssicherheit konfigurieren

Informationen zu diesem Vorgang

Die standardmäßig verwendete Benutzerregistry ist die dateibasierte Standard-Benutzerregistry von WebSphere Application Server for z/OS.

Vorgehensweise

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 die Schaltfläche **OK**.
6. Geben Sie das Kennwort für den Standard-Benutzer mit Verwaltungsaufgaben, z.B. `websphere`, ein, geben Sie die Bestätigung ein und klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu bestätigen.
7. Wählen Sie **Verwaltungssicherheit aktivieren**.
8. Wählen Sie **Anwendungssicherheit aktivieren**.
9. Wählen Sie **Java-2-Sicherheit verwenden, um den Anwendungszugriff auf lokale Ressourcen zu beschränken** und **Warnen, wenn Anwendungen angepasste Berechtigungen erteilt werden**.
10. Setzen Sie **Verfügbare Realmdefinitionen** auf **Eingebundene Repositorys**.
11. Klicken Sie auf die Schaltfläche **Anwenden**, um die Änderungen zu bestätigen.
12. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
13. Erweitern Sie **Web- und SIP-Sicherheit** und wählen Sie **Single Sign-on (SSO)** aus.
14. Wählen Sie **Erfordert SSL** aus.
15. Klicken Sie auf **OK**, um die Änderung zu bestätigen.

16. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
17. Wählen Sie den Link **Angepasste Eigenschaften** aus.
18. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie Namen und Wert wie folgt:

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

    Wert: `true`
19. Klicken Sie auf die Schaltfläche **OK**, um die neue Eigenschaft hinzuzufügen.
20. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie Namen und Wert wie folgt:

    Name: `com.ibm.ws.security.addHttpOnlyAttributeToCookies`

    Wert: `true`
21. Klicken Sie auf **OK**, um die Änderung zu bestätigen.
22. Speichern Sie die Änderungen in der Masterkonfiguration.

Anwendungsserver erneut starten

Dieser Schritt ist obligatorisch. Die WebSphere Application Server for z/OS-Adressräume müssen erneut gestartet werden, damit die Änderungen an den Sicherheitseinstellungen wirksam werden und zusätzliche erforderliche Benutzer hinzugefügt werden können. Die Adressräume können mithilfe des geeigneten `stopServer.sh`-Scripts im Verzeichnis `profiles/default/bin` der WebSphere Application Server for z/OS-Installation oder mithilfe des Befehls **`STOP`** des **z/OS**-Operators gestoppt werden, je nachdem, wie es für Ihre Installation angemessen ist.

Vor dem Neustart des Anwendungsservers ist es notwendig, die Registrierungs- und die Kryptografie-JAR-Dateien für WebSphere Application Server for z/OS verfügbar zu machen. Die Registrierungs-JAR-Datei enthält Klassen, die für die Sicherheitskonfiguration notwendig sind. Die Kryptografie-JAR-Datei enthält Konfigurationseinstellungen und -daten, die für die Kennwortsicherheit erforderlich sind.

Die Datei `Registry.jar` befindet sich im `lib`-Verzeichnis der SDEJ-Installation. Kopieren Sie diese Datei in das `lib`-Verzeichnis der WebSphere Application Server for z/OS-Installation.

Die Datei `CryptoConfig.jar` kann generiert werden, indem das Ant-Ziel 'configtest' wie folgt ausgeführt wird: *build configtest -Dcrypto.ext.dir=filedir*. Kopieren Sie die Datei 'CryptoConfig.jar' aus der generierten Position. Kopieren Sie diese Datei in das Verzeichnis Java `jre/lib/ext`. Wenn Sie Anpassungen an die Kryptografie-Konfiguration für Cúram benötigen, lesen Sie die entsprechenden Angaben im Dokument *Cúram Security Handbook*.

Richten Sie sich bei Sites mit einem schreibgeschützten Dateisystem der WebSphere-Installation nach der in „Alternative Speicherpositionen für JAR-Dateien” auf Seite 12 beschriebenen Prozedur.

Starten Sie nun den Anwendungsserver mithilfe des Scripts `startServer.sh` im Verzeichnis `profiles/default/bin` der WebSphere Application Server for z/OS-Installation oder mithilfe des **`START`**-Befehls des **z/OS**-Operators, wie es für Ihre Installation angemessen ist. Öffnen Sie die Administrationskonsole und fahren Sie mit den Konfigurationsschritten fort.

Da die Sicherheitskonfiguration vollständig ist und die Scripting-Änderungen vorgenommen wurden, ist es nun möglich, die SDEJ-Scripts für den Neustart des Anwendungsservers zu verwenden. Weitere Details zum Neustarten des Servers finden Sie unter „WebSphere Server starten und stoppen” auf Seite 18.

Um mit der Konfiguration fortzufahren, muss jetzt die Administrationskonsole geöffnet werden. Nachdem nun die globale Sicherheit aktiviert ist, müssen Sie sich mit dem zuvor eingerichteten Benutzernamen *websphere* und Kennwort *websphere* bei der Konsole anmelden.

DB2 for z/OS-Verbindung testen

Informationen zu diesem Vorgang

Nach dem Neustart des Anwendungsservers können Sie Ihre DB2 for z/OS-Verbindungen testen:

Vorgehensweise

1. Navigieren Sie zu **Ressourcen** > **JDBC** > **Datenquellen**.
2. Aktivieren Sie das Kontrollkästchen **curamdb DataSource** und/oder **curamsibdb DataSource**.
3. Klicken Sie auf die Schaltfläche **Verbindung testen**.
4. War der Test erfolgreich, sollte(n) die folgende(n) Nachricht(en) angezeigt werden:

```
Test Connection for DataSource <DataSource name> on
server <server name> at node <node name> was successful.
```

   Andernfalls überprüfen Sie die WebSphere Application Server for z/OS-Protokolle nach Details zum Fehlschlagen des Versuchs, korrigieren Sie den Fehler und versuchen Sie es erneut.

Benutzer konfigurieren

Informationen zu diesem Vorgang

Wie in „Sicherheitskonfiguration" auf Seite 13 detailliert beschrieben, wird die konfigurierte WebSphere Application Server for z/OS-Benutzerregistry für die Authentifizierung der Benutzer mit Verwaltungsaufgaben und des Datenbankbenutzers verwendet. Die Benutzer mit Verwaltungsaufgaben von WebSphere Application Server for z/OS und der Datenbankbenutzer müssen der Benutzerregistry wie folgt manuell hinzugefügt werden.

Vorgehensweise

1. Navigieren Sie zu **Benutzer und Gruppen** > **Benutzer verwalten**.
2. Wählen Sie die Schaltfläche **Erstellen** aus.
3. Geben Sie die Details für den Benutzer mit Verwaltungsaufgaben für WebSphere Application Server for z/OS ein und klicken Sie auf die Schaltfläche **Erstellen**.
4. Wiederholen Sie diese Schritte für den Datenbankbenutzer.

Ergebnisse

Hinweis: Wenn die WebSphere Application Server for z/OS-Verwaltungssicherheit während der Erstellung des Profils aktiviert war, kann der Benutzer mit Verwaltungsaufgaben bereits in der Registry definiert sein.

JAAS-Anmeldemodul für das System einrichten

Die Anwendungssicherheit verwendet für die Authentifizierung ein JAAS(Java Authentication and Authorization Service)-Anmeldemodul. Dieses Anmeldemodul

muss für die Konfigurationen DEFAULT, WEB_INBOUND and RMI_INBOUND konfiguriert werden. Wiederholen Sie die unten aufgeführten Schritte für jede dieser Konfigurationen.

Anmeldemodul hinzufügen:

1. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
2. Erweitern Sie den Eintrag **Java Authentication and Authorization Service** unter der Überschrift **Authentifizierung** und wählen Sie **Systemanmeldungen** aus.
3. Wählen Sie den entsprechenden Alias aus der Liste aus. Das Anmeldemodul sollte für die Aliasse DEFAULT, WEB_INBOUND und RMI_INBOUND wie folgt konfiguriert werden:
4. Klicken Sie auf die Schaltfläche **Neu**, um ein neues Anmeldemodul zu konfigurieren.
5. Setzen Sie das Feld **Name der Modulklasse** auf `curam.util.security.CuramLoginModule`.
6. Wählen Sie die Option **Proxy für Anmeldemodul verwenden** aus.
7. Wählen Sie im Feld **Authentifizierungsstrategie** REQUIRED aus.
8. Klicken Sie auf die Schaltfläche **OK**, um das Hinzufügen des neuen Anmeldemoduls zu bestätigen.
9. Wählen Sie das neu hinzugefügte `curam.util.security.CuramLoginModule` aus der Liste aus.
10. Wählen Sie den Link **Angepasste Eigenschaften** unter der Überschrift **Weitere Eigenschaften** aus.
11. Klicken Sie auf die Schaltfläche **Neu**, um die erforderlichen Eigenschaften wie unten aufgeführt hinzuzufügen.

Tabelle 6. Angepasste 'CuramLoginModule'-Eigenschaften

Name	Beispielwert	Beschreibung
exclude_usernames	websphere, db2admin	Erforderlich. Eine Liste von Benutzernamen, die von der Authentifizierung ausgeschlossen werden sollen. Diese Liste sollte den Benutzer mit Administrationsberechtigungen für WebSphere Application Server for z/OS (wie in „Verwaltungssicherheit konfigurieren" auf Seite 30 angegeben) und den Datenbankbenutzer (wie in „Datenquellen-Anmeldealias erstellen" auf Seite 26 angegeben) enthalten. Der Standardbegrenzer ist ein Komma, was aber mit dem Begrenzer 'exclude_usernames_delimiter' überschrieben werden kann. Alle hier aufgeführten Benutzer sollten in der WebSphere Application Server for z/OS-Benutzerregistry definiert sein.
exclude_usernames_delimiter	|	*Optional*. Ein Begrenzungszeichen für die Benutzernamenliste, die in 'exclude_usernames' bereitgestellt wird. In Fällen, wo die Benutzernamen eingebettete Kommas enthalten, wie bei LDAP-Benutzern, kann es hilfreich sein, wenn der Begrenzer nicht das standardmäßige Komma ist.

Tabelle 6. Angepasste 'CuramLoginModule'-Eigenschaften (Forts.)

Name	Beispielwert	Beschreibung
login_trace	true	*Optional*. Diese Eigenschaft sollte auf `true` gesetzt sein, um den Debugger für den Authentifizierungsprozess auszuführen. Wenn sie auf `true` gesetzt ist, bewirkt der Aufruf des Anmeldemoduls, dass Tracing-Daten zur Datei `SystemOut.log` von WebSphere Application Server for z/OS hinzugefügt werden.
module_name	DEFAULT, WEB_INBOUND oder RMI_INBOUND	*Optional*. Diese Eigenschaft sollte auf DEFAULT, WEB_INBOUND oder RMI_INBOUND gesetzt sein, je nach der Konfiguration, für die das Anmeldemodul gerade definiert wird. Sie wird nur dann verwendet, wenn 'login_trace' für Tracing-Zwecke auf `true` gesetzt ist.
check_identity_only	true	*Optional*. Wenn diese Eigenschaft auf `true` gesetzt ist, führt das Anmeldemodul nicht die üblichen Authentifizierungsverifizierungen durch. Stattdessen stellt es nur fest, ob der Benutzer in der Datenbanktabelle vorhanden ist. In diesem Fall wird die konfigurierte WebSphere Application Server for z/OS-Benutzerregistry nicht umgangen, sondern nach dem Anmeldemodul abgefragt. Diese Option ist für Fälle gedacht, in denen LDAP-Unterstützung erforderlich ist oder ein alternativer Authentifizierungsmechanismus verwendet werden soll.
user_registry_enabled	true	*Optional*. Diese Eigenschaft wird zum Überschreiben des Verhaltens verwendet, die Benutzerregistry zu umgehen. Ist sie auf 'true' gesetzt, so wird die WebSphere Application Server for z/OS-Benutzerregistry während des Authentifizierungsprozesses abgefragt. Ist sie auf 'false' gesetzt, so wird die WebSphere Application Server for z/OS-Benutzerregistry nicht abgefragt. **Anmerkung:** Wenn Sie 'Authentifizierung nur anhand der Identität' angeben und LDAP verwenden, müssen unter Umständen zusätzliche Konfigurationsschritte ausgeführt werden. Nähere Informationen dazu finden Sie unter „Besondere Konfigurationsschritte bei der Verwendung von 'Authentifizierung nur anhand der Identität' und LDAP" auf Seite 13.
user_registry_enabled_types	EXTERNAL	*Optional*. Mit dieser Eigenschaft wird eine durch Kommas begrenzte Liste externer Benutzertypen angegeben, die anhand der WebSphere Application Server for z/OS-Benutzerregistry (z.B. LDAP) verarbeitet werden. Weitere Informationen zur Verarbeitung der WebSphere Application Server for z/OS-Benutzerregistry finden Sie in „WebSphere Application Server-Benutzerregistry" auf Seite 15.

Tabelle 6. Angepasste 'CuramLoginModule'-Eigenschaften (Forts.)

Name	Beispielwert	Beschreibung
user_registry_disabled_types	EXTGEN,EXTAUTO	*Optional*. Mit dieser Eigenschaft wird eine durch Kommas begrenzte Liste externer Benutzertypen angegeben, die nicht anhand der WebSphere Application Server for z/OS-Benutzerregistry (z.B. LDAP) verarbeitet werden. Weitere Informationen zur Verarbeitung der WebSphere Application Server for z/OS-Benutzerregistry finden Sie in „WebSphere Application Server-Benutzerregistry" auf Seite 15.

12. Klicken Sie auf **OK**, um das Hinzufügen des neuen Anmeldemoduls zu bestätigen.

Anmeldemodul verschieben:

1. Navigieren Sie zu **Sicherheit** > **Globale Sicherheit**.
2. Erweitern Sie den Eintrag **Java Authentication and Authorization Service** unter der Überschrift **Authentifizierung** und wählen Sie **Systemanmeldungen** aus.
3. Wählen Sie den entsprechenden Alias aus der Liste aus. Das Anmeldemodul sollte für die Aliasse DEFAULT, WEB_INBOUND und RMI_INBOUND verschoben werden.
4. Wählen Sie den Link **JAAS-Anmeldemodule** unter der Überschrift **Weitere Eigenschaften** aus.
5. Klicken Sie auf die Schaltfläche **Reihenfolge festlegen**.
6. Wählen Sie die Eigenschaft **curam.util.security.CuramLoginModule** aus und klicken Sie auf die Schaltfläche **Nach oben verschieben**. Wiederholen Sie diesen Schritt, bis 'CuramLoginModule' der oberste Eintrag in der Liste ist.
7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen an der Reihenfolge zu bestätigen.

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` gesetzt, um sicherzustellen, dass Websitzungen nahtlos zwischen zwei Servern eines Clusters übertragen werden können, beispielsweise 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** unter der Überschrift **Authentifizierung** und wählen Sie die Eigenschaft **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** aus der Liste verfügbarer Eigenschaften aus.
3. Ändern Sie unter 'General Properties' den Wert der Eigenschaft **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** in *false*.
4. Klicken Sie auf die Schaltfläche **OK**, um die Hinzufügung zu bestätigen.

Änderungen speichern: Speichern Sie die Änderungen in der Masterkonfiguration wie unter „Masterkonfiguration speichern" auf Seite 30 beschrieben.

Serverkonfiguration

64-Bit-Unterstützung konfigurieren:

Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Aktivieren Sie das Kontrollkästchen **Im 64-Bit-JVM-Modus ausführen**.
4. Klicken Sie auf **Anwenden** oder **OK**, um die Änderungen anzuwenden.
5. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

Ergebnisse

Anmerkung: Es kann sein, dass Sie auch Ihre JVM-Heapspeichergrößen überprüfen und anpassen müssen, je nach Größe, Durchsatz, Leistungszielen und anderen Faktoren Ihrer Anwendung.

Port für JNDI-Suche konfigurieren:
Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Erweitern Sie **Ports** im Feld **Kommunikation** 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.

Klassenlader-Einstellungen konfigurieren:
Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Setzen Sie die **Richtlinie für Klassenlader** auf `MULTIPLE`.
4. Klicken Sie auf **OK**, damit die Änderungen wirksam werden.
5. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

Pass-by-Reference für Object-Request-Broker konfigurieren:
Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
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.

Java Virtual Machine konfigurieren:

Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Erweitern Sie im Fenster **Serverinfrastruktur** die Option **Java- und Prozessverwaltung**.
4. Wählen Sie den Link **Prozessdefinition** aus.
5. Führen Sie im Fenster **Prozesstyp** die folgenden Schritte für jedes Element in der Liste aus (Adjunct, Controller und Servant):
   a. Wählen Sie den Link **Prozesstyp** aus.
   b. Wählen Sie im Fenster **Weitere Eigenschaften** den Link **Java Virtual Machine** aus.
   c. Nehmen Sie in den Feldern folgende Einstellungen vor:

      Anfangsgröße des Heapspeichers :`1024`

      Maximale Größe des Heapspeichers: `1024`

      Klicken Sie auf **Anwenden**, um die Werte festzulegen.
   d. Wählen Sie im Fenster **Weitere Eigenschaften** den Link **Angepasste Eigenschaften** aus.
   e. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie die Eigenschaften wie folgt:

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

      Wert: `false`

      Klicken Sie auf die Schaltfläche **OK**, um die Eigenschaft hinzuzufügen.
6. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

Zeitgeberservice konfigurieren:
Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Erweitern Sie im Fenster **Containereinstellungen EJB-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. Nehmen Sie in den Feldern folgende Einstellungen vor:

   JNDI-Name der Datenquelle: `jdbc/curamtimerdb`

   Datenquellenalias: <*valid for database*>

   Wobei der verwendete Alias der ist, der in„Datenquellen-Anmeldealias erstellen” auf Seite 26 eingerichtet wird.
7. Klicken Sie auf die Schaltfläche **OK**, um die Änderungen zu bestätigen.
8. Speichern Sie die Änderungen in der Masterkonfiguration mithilfe der Option **Speichern** wie zuvor.

Portzugriff einrichten:
Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Wählen Sie den Link **Ports** im Feld **Kommunikation** aus.
4. Aktivieren Sie das Kontrollkästchen **Details**.

5. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie die folgenden Felder für den Client-TCP/IP-Port:

   User-defined Port Name: CuramClientEndPoint

   Host: *

   Port: *<client port>*

   Setzen Sie *<client port>* so, dass es mit dem Wert der Eigenschaft 'curam.client.httpport' in Ihrer `AppServer.properties`-Datei übereinstimmt.

   Klicken Sie auf die Schaltfläche **OK**, um die Änderungen anzuwenden.
6. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie für den WebServices Client-TCP/IP-Port die folgenden Felder:

   Benutzerdefinierter Portname: CuramWebServicesEndPoint

   Host: *

   Port: *<webservices port>*

   Setzen Sie *<webservices port>* so, dass es mit dem Wert der Eigenschaft 'curam-.webservices.httpport' in Ihrer `AppServer.properties`-Datei übereinstimmt.

   Klicken Sie auf die Schaltfläche **OK**, um die Änderungen anzuwenden.
7. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
8. Wählen Sie den entsprechenden Server aus der Liste aus.
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 die Schaltfläche **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 die Schaltfläche **Neu** und setzen Sie für die WebServices-Transportkette die folgenden Felder:

    Name : `CuramWebServicesChain`

    1Transportkettenschablone: `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 Keepalive-Verbindung verwenden** aktiviert ist.
16. Klicken Sie auf die Schaltfläche **OK**, um die Hinzufügung zu bestätigen.
17. Navigieren Sie zu **Umgebung** > **Virtuelle Hosts**.
18. Klicken Sie auf die Schaltfläche **Neu**, um durch Setzen der folgenden Felder einen neuen `Virtual Host` 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 Feld **Weitere Eigenschaften** aus.

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

Hostname = *

Port = *<client port>*

Setzen Sie *<client port>* so, dass es mit dem Wert der Eigenschaft 'curam.client.httpport' in Ihrer `AppServer.properties`-Datei übereinstimmt. Wiederholen Sie diesen Schritt für den anderen verwendeten Host und Port (z.B. 'webservices_host').

20. Klicken Sie auf die Schaltfläche **OK**, um die Hinzufügung zu bestätigen.
21. Speichern Sie die Änderungen in der Masterkonfiguration wie unter „Masterkonfiguration speichern" auf Seite 30 beschrieben.

Sicherheitsintegration für Sitzungen konfigurieren: Vorgehensweise

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Wählen Sie den entsprechenden Server aus der Liste aus.
3. Klicken Sie im Abschnitt **Containereinstellungen** auf **Sitzungsverwaltung**.
4. Inaktivieren Sie die Option **Sicherheitsintegration**. *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.

Anmerkung:

Die obige Einstellung ist für IBM Cúram Social Program Management-Webanwendungen erforderlich.

Buskonfiguration

Service Integration Bus einrichten: Vorgehensweise

1. Navigieren Sie zu **Serviceintegration** > **Busse**.
2. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie 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 geeignet sind, 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** in der Liste **Topologie** aus.

7. Klicken Sie auf **Hinzufügen**, woraufhin der Assistent **Neues Bus-Member hinzufügen** geöffnet wird.
8. Wählen Sie den Server aus, der zum Bus hinzugefügt werden soll, und klicken Sie auf die Schaltfläche **Weiter**.
9. Wählen Sie **Datenspeicher** aus und klicken Sie auf die Schaltfläche **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 „Masterkonfiguration speichern" auf Seite 30 beschrieben.

JMS(Java Message Service)-Konfiguration

JMS-Verbindungsfactorys einrichten:
Vorgehensweise

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 den Link **Verbindungsfactorys** im Feld **Weitere Eigenschaften**.
5. Klicken Sie auf die Schaltfläche **Neu** und setzen Sie die folgenden Felder:

   Name: CuramQueueConnectionFactory

   JNDI-Name: jms/CuramQueueConnectionFactory

   Beschreibung: Die Factory für alle Verbindungen zu den 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 den Authentifizierungsalias für die XA-Wiederherstellung.

Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf die Schaltfläche **OK**, um die Änderungen anzuwenden.

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

   Name: CuramTopicConnectionFactory

   JNDI-Name: jms/CuramTopicConnectionFactory

   Beschreibung: Die Factory für alle Verbindungen zu den 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 die Schaltfläche **OK**, um die Änderungen anzuwenden.

7. Speichern Sie die Änderungen in der Masterkonfiguration wie unter „Masterkonfiguration speichern” auf Seite 30 beschrieben.

Ergebnisse

Anmerkung: Mit den obigen manuellen Konfigurationsschritten ist es nicht möglich, die Sicherheit für die Cúram-Warteschlange und die Topic-Verbindungsfactorys ordnungsgemäß zu konfigurieren. Für diesen Teil der Konfiguration müssen Sie das Tool wsadmin verwenden. Verlassen Sie dazu die Administrationskonsole und befolgen Sie diese Schritte:

1. Geben Sie die Einträge für die Warteschlange und die Topic-Verbindungsfactory in die resources.xmlKonfigurationsdatei von WebSphere Application Server for z/OS ein. Diese Datei befindet sich in der Dateisystemhierarchie %WAS_HOME%\profiles\<profile_name>\config. Ihr Ort ist von Ihren Namenskonventionen und dem Bereich abhängig, in dem Sie Ihre JMS-Ressourcen definiert haben. Beispielsweise würde sich die Datei bei einem Knotenebenenbereich mit dem Profilnamen AppSrv01, dem Zellennamen MyNodeCell und dem Knotennamen MyNode an folgendem Ort befinden: C:\WebSphere\profiles\AppSrv01\config\cells\MyNodeCell\nodes\MyNode\resources.xml. In dieser Datei müssen Sie die <factories>-Entitäten für CuramQueueConnectionFactory und CuramTopicConnectionFactory suchen und die ID für jede von ihnen vermerken, die mit J2CConnectionFactory_ beginnt und von einem numerischen Wert gefolgt wird, z.B. 1264085551611.
2. Rufen Sie das wsadmin-Script von WebSphere Application Server for z/OS auf. In diesen Beispielen ist die Sprache Jacl, so dass das *-lang jacl*-Argument möglicherweise mit Berechtigungsnachweisen für Anmeldung o.ä., je nach Ihrer lokalen Konfiguration, angegeben werden muss.
3. Rufen Sie in wsadmin die folgenden Befehle auf, wieder mit den angenommenen Definitionen auf Knotenebene, dem Zellennamen MyNodeCell und dem Knotennamen MyNode. Die Ressourcen-IDs werden in Ihrer Umgebung andere sein:
   a. Rufen Sie den Knoten und die Zellkennung auf: $AdminConfig getid /Node:MyNode

b. Kombinieren Sie den Knoten und die Zellkennung aus dem vorherigen Schritt mit der Kennung der Verbindungsfactory, die Sie im obigen Schritt erhalten haben, um die Verbindungsfactory anzuzeigen: `$AdminTask showSIBJMSConnectionFactory CuramQueueConnectionFactory(cells/MyNodeCell/nodes/MyNode|resources.xml#J2CConnectionFactory_1264085551611)`

   Anhand der obigen Befehlsausgabe sollten Sie verifizieren, dass 'authDataAlias' nicht gesetzt ist (z. B. `authDataAlias=`), sonst bekommen Sie Probleme, wie folgendes Beispiel für eine wsadmin-Ausgabe zeigt:

```
{password=, logMissingTransactionContext=false,
readAhead=Default, providerEndpoints=,
shareDurableSubscriptions=InCluster,
targetTransportChain=, authDataAlias=, userName=,
targetSignificance=Preferred,
shareDataSourceWithCMP=false,
nonPersistentMapping=ExpressNonPersistent,
persistentMapping=ReliablePersistent, clientID=,
jndiName=jms/CuramQueueConnectionFactory,
manageCachedHandles=false,
consumerDoesNotModifyPayloadAfterGet=false,
category=, targetType=BusMember, busName=CuramBus,
description=None,
xaRecoveryAuthAlias=crouch/databaseAlias,
temporaryTopicNamePrefix=, remoteProtocol=,
producerDoesNotModifyPayloadAfterSet=false,
connectionProximity=Bus, target=,
temporaryQueueNamePrefix=,
name=CuramQueueConnectionFactory}
```

c. Um den 'authDataAlias' so einzurichten, dass er dieselben Informationen zur Verbindungsfactory verwendet wie oben, gehen Sie beispielsweise folgendermaßen vor: `$AdminTask modifySIBJMSConnectionFactory CuramQueueConnectionFactory(cells/MyNodeCell/nodes/MyNode|resources.xml#J2CConnectionFactory_1264085551611) {-authDataAlias crouch/databaseAlias}`

d. Speichern Sie die Änderungen: `$AdminConfig save`

e. Sie können den Befehl `showSIBJMSConnectionFactory` aufrufen, um die Änderung zu überprüfen.

f. Wiederholen Sie die obigen Schritte für `CuramTopicConnectionFactory`.

g. Verlassen Sie die 'wsadmin'-Sitzung mithilfe des Befehls `quit`, nachdem Sie überprüft haben, ob Ihre Änderungen gespeichert wurden.

Erforderliche Warteschlangen einrichten:
Informationen zu diesem Vorgang

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

Vorgehensweise

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

5. Setzen Sie die folgenden Warteschlangenattribute:

   Kennung: 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 7. Einstellungen für Ausnahmeziele

Name der Warteschlange	Ausnahmeziel
SIB_CuramDeadMessageQueue	System
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**, um die Änderungen anzuwenden.
11. Navigieren Sie zu **Ressourcen** > **JMS** > **JMS-Provider**.
12. Wählen Sie den Link **Standard-Messaging-Provider** aus.
13. Wählen Sie den Link **Warteschlangen** im Feld **Weitere Eigenschaften** aus.
14. Klicken Sie auf die Schaltfläche **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 die Schaltfläche **OK**, um die Änderungen anzuwenden.

Ergebnisse

Speichern Sie die Änderungen in der Masterkonfiguration wie unter „Masterkonfiguration speichern" auf Seite 30 beschrieben.

Erforderliche Themen einrichten:
Vorgehensweise

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

   Name: CuramCacheInvalidationTopic

   JNDI-Name des Ziels: jms/CuramCacheInvalidationTopic

   Beschreibung: Cache Invalidation Topic

Busname: CuramBus

Topicbereich: Default.Topic.Space

JMS-Übermittlungsmodus: Nonpersistent

Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf die Schaltfläche **OK**, um die Änderungen anzuwenden.

5. Speichern Sie die Änderungen in der Masterkonfiguration wie unter „Masterkonfiguration speichern" auf Seite 30 beschrieben.

Erforderliche Warteschlangen-Aktivierungsspezifikationen einrichten: Informationen zu diesem Vorgang

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

Vorgehensweise

1. Navigieren Sie zu **Ressourcen** > **JMS** > **JMS-Provider**.
2. Wählen Sie den Link **Standard-Messaging-Provider** aus.
3. Wählen Sie den Link **Aktivierungsspezifikationen** im Feld **Weitere Eigenschaften** aus.
4. Erstellen Sie eine neue Spezifikation, indem Sie auf die Schaltfläche **Neu** klicken, und setzen Sie die folgenden Felder:

   Name: <QueueName>

   JNDI-Name: eis/ <*QueueName*> AS

   Zieltyp: Queue

   JNDI-Name des Ziels: jms/ <*QueueName*>

   Busname: CuramBus

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

   Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf **OK**, um den Port hinzuzufügen.

Ergebnisse

Speichern Sie die Änderungen in der Masterkonfiguration wie unter „Masterkonfiguration speichern" auf Seite 30 beschrieben.

Erforderliche Themen-Aktivierungsspezifikationen einrichten: Vorgehensweise

1. Fügen Sie wie bei den Aktivierungsspezifikationen für Warteschlangen im vorigen Abschnitt eine neue Aktivierungsspezifikation hinzu und setzen Sie die folgenden Felder:

   Name: CuramCacheInvalidationTopic

   JNDI-Name: eis/CuramCacheInvalidationTopicAS

   Zieltyp: Topic

   JNDI-Name des Ziels: jms/CuramCacheInvalidationTopic

   Busname: CuramBus

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

2. Belassen Sie alle anderen Werte als Standardwerte und klicken Sie auf die Schaltfläche **OK**, um die Änderungen anzuwenden.
3. Speichern Sie die Änderungen in der Masterkonfiguration wie unter „Masterkonfiguration speichern" auf Seite 30 beschrieben.

Nach dem Konfigurieren

Datenbanktabellen für den Service Integration Bus: Nach der Installation müssen Datenbanktabellen manuell erstellt werden, die für den Service Integration Bus erforderlich sind. WebSphere Application Server for z/OS stellt hierfür ein Dienstprogramm bereit, das die SQL für die Erstellung dieser Tabellen generiert, den SIB-DDL-Generator.

Dieser Generator wird mithilfe des folgenden Befehls ausgeführt:

```
$WAS_HOME/bin/sibDDLGenerator.sh
  -system system
  -platform platform
  -schema username
  -database database_name
  -user username
  -statementend ';'
  -create
```

Wobei gilt:

- *system* die zu verwendende Datenbank ist, z.B. `db2`
- *platform* das Betriebssystem ist, z.B. `zos`
- *username* ist der Benutzername, der für den Zugriff auf die Datenbank erforderlich ist, wie in der `Bootstrap.properties`-Eigenschaft `curam.db.username` angegeben
- *database_name* ist der Name der zu verwendenden Datenbank, wie in der `Bootstrap.properties`-Eigenschaft `curam.db.zos.dbname` angegeben

Beispiel:

```
$WAS_HOME/bin/sibDDLGenerator.sh
            -system db2 -platform zos
            -schema db2admin -database curam -user db2admin
            -statementend ';' -create
```

Dieser Befehl bewirkt die Ausgabe von SQL-Anweisungen zum Definieren der Service Integration Bus-Tabellen. Diese SQL-Anweisungen müssen für die Zieldatenbank ausgeführt werden.

Anmerkung: Es gibt DB2 for z/OS-spezifische Standardwerte für STOGROUP und BUFFERPOOL; weitere Informationen finden Sie in der Produktdokumentation zu WebSphere Application Server.

Datenbanktabellen für den Zeitgeberservice: Nach der Installation müssen Datenbanktabellen manuell erstellt werden, die für den Zeitgeberservice erforderlich sind. WebSphere Application Server for z/OS stellt in seinem Verzeichnis `$WAS_HOME/Scheduler` die DDL für diese Tabellen zur Verfügung.

Die auszuführenden DDL-Dateien sind `createTablespaceDB2ZOS.ddl` und `createSchemaDB2ZOS.ddl` in dieser Reihenfolge.

Jede DDL-Datei enthält Anweisungen entsprechend der Ausführung für Ihre Zieldatenbank.

Fertigstellung

WebSphere Application Server for z/OS ist nun konfiguriert und steht für die Installation der .ear-Dateien für die IBM Cúram Social Program Management-Anwendung bereit. Melden Sie sich bei der Administrationskonsole ab und starten Sie WebSphere Application Server for z/OS mithilfe der in „WebSphere Server starten und stoppen" auf Seite 18 beschriebenen Ziele erneut.

Manuelle Anwendungsimplementierung

Informationen zu diesem Vorgang

Zum Installieren einer Unternehmensanwendung in WebSphere Application Server for z/OS kann die Administrationskonsole verwendet werden. Mit den untenstehenden 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.

Vorgehensweise

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 den vollständigen Pfadnamen der Quellenanwendungsdatei oder .ear-Datei an, optional über die Schaltfläche **Durchsuchen** im Fenster **Pfad der neuen Anwendung**, und klicken Sie auf **Weiter**.

   Der Standardstandort für die Anwendungs-.ear-Dateien ist:

   ```
   $SERVER_DIR/ear/WAS/
   ```
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, wählen Sie den Server oder Cluster aus und klicken Sie auf **Anwenden**.
7. Um den folgenden Schritt oder die folgenden Schritte durchführen zu können, klicken Sie auf **Weiter** und in der Zusammenfassungsanzeige auf **Fertigstellen**, um die Installation abzuschließen. 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 in „Masterkonfiguration speichern" auf Seite 30.)
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. Navigieren Sie zu **Benutzer und Gruppen -> Benutzer verwalten**. Klicken Sie auf **Erstellen...** und geben Sie Benutzer-ID, Kennwort, Vornamen und Nachnamen ein. Klicken Sie anschließend auf **Erstellen**.

    Weitere Informationen bezüglich der Berechtigungsnachweise, die an dieser Stelle von der Anwendung erwartet werden, und ihrer Änderung finden Sie unter „SYSTEM-Benutzernamen ändern" auf Seite 21.
15. Gehen Sie zurück zur Unternehmensanwendung (**Anwendungen** > **Anwendungstypen** > **WebSphere-Unternehmensanwendungen**, wählen Sie die neu installierte Anwendung), wählen Sie aus dem 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 und klicken Sie auf **Benutzer zuordnen...**.
    b. Geben Sie im Feld **Suchbegriff** einen geeigneten Benutzernamen an 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**.
16. Nachdem die MDB-Benutzerrolle zugeordnet ist, kann nun die Benutzer-RunAs-Rolle aktualisiert werden. Wählen Sie dazu im Abschnitt **Detaileigenschaften** die Option **RunAs-Rollen für Benutzer** aus.
17. Geben Sie in den Feldern **Benutzername** und **Kennwort** jeweils den entsprechenden Benutzernamen und das Kennwort ein. Wählen Sie **Auswählen** für die MDB-Benutzerrolle und klicken Sie auf **Anwenden**.
18. Klicken Sie auf **OK**.
19. Speichern Sie die Änderungen in der Masterkonfiguration.
20. Nach der Implementierung ist ein Start der Anwendung notwendig, bevor sie verwendet werden kann. Navigieren Sie zu **Anwendungen** > **Anwendungstypen** > **WebSphere-Unternehmensanwendungen**, aktivieren Sie das Kontrollkästchen für die neu installierte Anwendung 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.
21. Testen Sie als letzten Schritt die Anwendungsimplementierung. Lassen Sie dazu beispielsweise einen Web-Browser auf die URL der implementierten Anwendung verweisen, z.B.:

    ```
    https://<Your WebSphere host>:<CuramClientEndPoint>/Curam
    ```

    Wobei

    <*Your WebSphere host*> den Hostnamen oder die IP-Adresse angibt, unter dem/der Ihr WebSphere Application Server for z/OS-System läuft, und <*CuramClientEndPoint_http_port*> den zugewiesenen Port angibt (wie in „Portzugriff einrichten" auf Seite 37 beschrieben).

WebSphere Network Deployment

IBM WebSphere Application Server Network Deployment bietet hochwertige Implementierungsservices, darunter Clustering, Ersterkennungsservices und Hochverfügbarkeit für verteilte Konfigurationen.

Tipps zum Arbeiten mit WebSphere Network Deployment

Anpassungen für WebSphere Network Deployment: Das Anpassen von WebSphere Network Deployment (mithilfe des z/OS Profile Management Tools oder ISPF) liegt außerhalb des Bereichs dieses Dokuments; jedoch werden Sie im Verlaufe dieses Handbuchs feststellen, dass IBM eine Anzahl Dokumentationen dazu anbietet, *Program Directory for WebSphere Application Server for z/OS V7.0 (GI11-4295)* und *IBM WebSphere Application Server for z/OS, Version 7.0: Installing your application serving environment* sowie *WebSphere Application Server, Version V7.0 product documentation*. Sie finden diese Dokumente auf der IBM Redbook-Website: http://www.redbooks.ibm.com/.

Änderungen synchronisieren: Wenn Sie in einer Network Deployment-Umgebung arbeiten, wird dringend empfohlen, sicherzustellen, dass WebSphere Application Server for z/OS seine Konfiguration nach *jeder* Änderung in der Administrationskonsole oder einem Ant-Ziel synchronisiert.

Stellen Sie beim Speichern der Masterkonfiguration sicher, dass Sie die Synchronisation über die Administrationskonsole manuell erzwingen:

1. Navigieren Sie zu **Systemadministration** > **Änderungen an Master-Repository speichern**.
2. Aktivieren Sie das Kontrollkästchen **Änderungen mit Knoten synchronisieren**.
3. Klicken Sie auf die Schaltfläche **Speichern**. Die Synchronisation kann einige Zeit in Anspruch nehmen.
4. Überprüfen Sie das System und/oder WebSphere Application Server nach z/OS-Protokollen zur Fertigstellung der Synchronisation. Diese Nachrichten können sich je nach Release von WebSphere Application Server for z/OS unterscheiden, sollten aber etwa folgendermaßen aussehen:

```
ADMS0208I: Die Konfigurationssynchronisation für die Zelle ist abgeschlossen.
```

   Nachdem die Synchronisation abgeschlossen ist, überprüfen Sie den Serverstatus und verschiedene WebSphere Application Server for z/OS-Protokolle, um sich des erfolgreichen Vorgangs zu vergewissern.

Knotenkonfiguration

Vor dem Implementieren einer Anwendung muss zunächst der Server konfiguriert werden. Dies geschieht mithilfe der Deployment Manager-Administrationskonsole. Die Konfiguration wird daraufhin mit den eingebundenen Servern des Knotens synchronisiert.

Der Knotenagent, der die Kommunikation zwischen dem Deployment Manager und seinen eingebundenen Servern ermöglichen soll, muss gestartet werden. Dies kann über den für Ihre Installation geeigneten **START**-Befehl des **z/OS**-Operators geschehen oder über den Befehl `startNode.sh` im Verzeichnis `profiles/<federated profile name>/bin` der WebSphere Application Server for z/OS-Installation.

Nach dem Starten des Knotenagenten wird die Steuerung der Server dieses Knotens vollständig an den Deployment Manager übergeben. Um einen Server in der Deployment Manager-Administrationskonsole zu starten oder zu stoppen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Server** > **Servertypen** > **WebSphere-Anwendungsserver**.
2. Heben Sie die Auswahl des Servers, der gestartet bzw. gestoppt werden soll, in der Liste auf und klicken Sie je nach Erforderlichkeit auf die Schaltfläche **Start** bzw. **Stoppen**.

Der nächste Prozessschritt besteht in der Konfiguration der eingebundenen Server. Wie schon erwähnt, erfolgt die gesamte Konfiguration über die Deployment Manager-Administrationskonsole. In „WebSphere Application Server manuell konfigurieren" auf Seite 24 wird die manuelle Konfiguration für WebSphere Application Server for z/OS für eine Basisinstallation beschrieben. Mit den unten beschriebenen Abweichungen sollte dieser Beschreibung gefolgt werden. Stellen Sie beim Speichern der Masterkonfiguration sicher, dass Ihre Änderungen wie in „Änderungen synchronisieren" auf Seite 48 beschrieben synchronisiert werden.

In „JAAS-Anmeldemodul für das System einrichten" auf Seite 32 finden Sie Details zu der Sicherheitseinrichtung, die für die manuelle Konfiguration erforderlich ist. Diese Einrichtung erfordert, dass die Datei `Registry.jar` in ein Verzeichnis innerhalb der WebSphere Application Server for z/OS-Installation kopiert wird. Die Datei `Registry.jar` muss aus `CuramSDEJ/lib` in das Verzeichnis `lib` der Deployment Manager-Installation und in alle eingebundenen Installationen kopiert werden.

„JAAS-Anmeldemodul für das System einrichten" auf Seite 32 Für diese Sicherheitseinrichtung ist es auch erforderlich, die Datei `CryptoConfig.jar` innerhalb der WebSphere Application Server-Installation in das Verzeichnis `java64/lib/ext` zu kopieren. Für jede andere WebSphere Application Server-Installation der Umgebung sollte die Datei `CryptoConfig.jar` in dieselbe Verzeichnisstruktur kopiert werden.

Anmerkung: Vor der Erstellung der Anwendungs-`.ear`-Dateien für die Implementierung sollte auf die *BOOTSTRAP_ADDRESS* des Servers hingewiesen werden, auf die sie installiert werden sollen. Die *BOOTSTRAP_ADDRESS* befindet sich in derselben Liste von Ports wie die bereits beschriebene *SOAP_CONNECTOR_ADDRESS*.

Standardmäßig hat die von der Anwendung erwartete *BOOTSTRAP_ADDRESS* den Wert '2809'. Um dieses Problem zu beheben, ändern Sie entweder diese Adresse oder die entsprechende Eigenschaft in Ihrer `AppServer.properties`-Datei.

Die zu ändernde Eigenschaft ist der Wert 'curam.server.port' in der Datei `AppServer.properties`. Diese Änderung beeinflusst den Portwert in der `web.xml`-Datei für die Erstellung einer `.ear`-Datei. Weitere Informationen zu der Datei `web.xml` finden Sie im Dokument *Cúram Web Client Reference Manual* (Cúram-Referenzhandbuch zum Webclient).

Bereitstellungen auf dem Knoten

Zum Schluss sollten die Anwendungen anhand der Anweisungen unter „Manuelle Anwendungsimplementierung" auf Seite 46 manuell auf dem erforderlichen Server implementiert werden. Daraufhin ist es möglich, Anwendungen mithilfe der Deployment Manager-Administrationskonsole zu starten und zu stoppen.

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.

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. IBM kann daher die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programm nicht garantieren oder implizieren. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. 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.

© Copyright IBM Corp. _Jahreszahl oder Jahreszahlen eingeben_. Alle Rechte vorbehalten.

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

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Je nachdem, welche Konfigurationen implementiert wurden, ist es möglich, dass dieses Softwareangebot Sitzungscookies und persistente Cookies zum Erfassen der Namen, Benutzernamen, Kennwörter, Profilnamen oder anderer personenbezogener Daten einzelner Benutzer für die Sitzungsverwaltung, Authentifizierung, Single-Sign-on-Konfiguration oder für einen besseren Bedienungskomfort und/oder andere Zwecke der Nutzungsverfolgung bzw. funktionale Einsatzmöglichkeiten. Diese Cookies oder ähnliche Technologien können nicht inaktiviert werden.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der "IBM Online-Datenschutzerklärung, Schwerpunkte" unter http://www.ibm.com/privacy und in der "IBM Online-Da-

tenschutzerklärung" unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und unter "IBM Software Products and Software-as-a-Service Privacy Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation. Weitere Produkt- oder Servicenamen können Marken von IBM oder anderen Herstellern 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.

Apache ist eine eingetragene Marke der Apache Software Foundation.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind eingetragene Marken von Oracle und/oder Tochterunternehmen.

Andere Namen können Marken der jeweiligen Rechtsinhaber sein. Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken oder Dienstleistungsmarken anderer Unternehmen sein.

Gedruckt in Deutschland