IBM Cúram Social Program Management
Version 6.0.5

Guide de déploiement de Cúram pour WebSphere Application Server on z/OS

Important
Avant d'utiliser ces informations et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 53

Dernière révision : Mars 2014

Cette édition s'applique à IBM Cúram Social Program Management version 6.0.5 et à toutes les versions ultérieures, sauf indication contraire dans les nouvelles éditions.

Eléments sous licence - Propriété d'IBM.

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

© Copyright IBM France 2014. Tous droits réservés.

© Copyright IBM Corporation 2012, 2013.

© Cúram Software Limited. 2011. All rights reserved.

Table des matières

© Copyright IBM Corp. 2012, 2013

Figures

© Copyright IBM Corp. 2012, 2013

Tableaux

© Copyright IBM Corp. 2012, 2013

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

© Copyright IBM Corp. 2012, 2013

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

Brevets

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

Assistance téléphonique

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

Déploiement sur IBM WebSphere Application Server sous z/OS

Plusieurs outils tiers sont requis pour déployer IBM Cúram Social Program Management sur IBM WebSphere Application Server pour IBM z/OS. Des fichiers du serveur de client Web et des fichiers EAR d'application sont requis pour déployer l'application.

Introduction

Présentation

Ce guide décrit le processus de configuration et de déploiement d'IBM® Cúram Social Program Management avec IBM WebSphere Application Server for IBM z/OS. Pour des informations précises sur les versions prises en charge, consultez le document *Conditions requises prises en charge Cúram*.

Les tâches de configuration peuvent être résumées comme suit :

1. Installation et configuration des outils tiers obligatoires ;
2. Configuration de WebSphere Application Server for z/OS pour les fichiers `.ear` (Enterprise ARchive) d'application IBM Cúram Social Program Management ;
3. Génération et envoi des fichiers `.ear` d'application.

   Les fichiers `.ear` sont générés séparément (sur une plateforme Microsoft Windows ou **UNIX**) ;
4. Déploiement de l'application et du client Web IBM Cúram Social Program Management. Les étapes impliquées sont les suivantes :
   - Etablissement des fichiers de propriétés ;
   - Installation des fichiers `.ear` d'application ;
   - Création d'une base de données ;
   - Pré-compilation de JavaServer Pages (facultatif) ;
   - Test du déploiement.

WebSphere Application Server for z/OS peut être personnalisé et configuré de plusieurs manières à des fins de performances, de ressources, de sécurité et pour d'autres raisons. Ce document présente une approche simple, à serveur unique, permettant de configurer WebSphere Application Server for z/OS. Celle-ci n'est peut-être pas appropriée à votre installation.

Prévisions

Une équipe ou un individu utilisant ce document doit posséder des connaissances et une expérience satisfaisantes d'une large gamme de produits et de technologies **z/OS** notamment. Pour plus d'informations, consultez le document *Program Directory for WebSphere Application Server for z/OS 7.0 (GI11-4295)* ainsi que la documentation connexe.

L'installation et la personnalisation de WebSphere Application Server for z/OS, ainsi que les logiciels z/OS connexes et liés à ce dernier ne sont pas abordés ici. Cependant, les étapes spécifiques éventuellement requises pour IBM Cúram Social Program Management sont traitées dans ce document.

© Copyright IBM Corp. 2012, 2013

Une personnalisation spécifique au client supplémentaire peut être nécessaire, notamment :

- En fonction de vos exigences de sécurité locales (par exemple fonction RACF IBM), vous pouvez être amené à effectuer une configuration et une personnalisation supplémentaires.

Conventions du document

Plusieurs conventions sont utilisées dans ce document :

- Les valeurs entre un signe inférieur et un signe supérieur, par exemple *<WebSphere Configuration Directory>*, font référence aux substitutions pour lesquelles vous devez fournir des valeurs.
- Navigation dans la console d'administration WebSphere Application Server for z/OS :
  - «Navigate» fait référence aux sélections effectuées via le contrôle d'arborescence dans le panneau gauche de la fenêtre du navigateur et qui sont affichées comme suit : **Servers (Serveurs)** > **Application Servers (Serveurs d'applications)**.
  - «Select» renvoie aux liens hypertexte qui apparaissent dans la fenêtre du navigateur et qui s'affichent dans ce document en italique ; par exemple **local_host**.
  - «Click» fait référence aux boutons comme **OK** et **Next**.
  - «Check» ou «Select» renvoie aux cases ou options que vous devez sélectionner. Sélectionnez par exemple l'option **Enforce Java 2 Security**.

Outils tiers

Introduction

Pour pouvoir utiliser l'application IBM Cúram Social Program Management, il est nécessaire d'installer et de configurer des logiciels tiers. Les détails précis concernant ces produits sont disponibles dans le document *Conditions requises prises en charge Cúram*.

Dans un document tel que celui-ci, il n'est pas prévu de fournir des données détaillées et des instructions sur l'installation et la configuration de tous les différents produits logiciels **z/OS** nécessaires pour prendre en charge WebSphere Application Server for z/OS and DB2 for z/OS. Ce chapitre vise uniquement à fournir de brefs détails au sujet de la configuration requise minimale de chaque produit.

Les sections qui suivent présentent les conditions requises, les notes sur l'installation et/ou les activités de configuration post-installation pour chacun des éléments suivants :

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

Une fois que les outils tiers ont été installés et configurés, ces derniers laissent le système prêt pour la configuration de WebSphere Application Server for z/OS.

Avant l'installation

Outre les informations fournies dans les manuels *Program Directory for WebSphere Application Server for z/OS V7.0 (GI11-4295)* et *IBM WebSphere Application Server for z/OS, Version V7.0: Installing your application serving environment WebSphere Application Server, Version V7.0 Information Center.*, pour **z/OS**, les éléments suivants sont recommandés :

- Mémoire système - appropriée à l'exécution de vos applications, en incluant le nombre d'utilisateurs, les exigences de performances, etc.
- Espace du système de fichiers - vous devez planifier l'affectation d'espace supplémentaire dans votre système de fichiers des services système UNIX pour l'environnement Cúram et pour le déploiement dans la configuration WebSphere Application Server for z/OS.

DB2 for z/OS

Versions prises en charge

La version exacte de DB2 à installer est répertoriée dans le document *Conditions requises prises en charge Cúram*.

Conditions préalables

Reportez-vous au document *Program Directory for IBM DB2 Universal Database for z/OS; version 8 (GI10-8566) and version 9 (GI10-8737)*.

Installation

Avant de commencer la configuration et l'installation de Cúram, on suppose que DB2 for z/OS a bien été installé à l'aide de l'outil SMP/E et que l'installation a été configurée à l'aide des panneaux de personnalisation de l'utilitaire Interactive System, conformément à vos exigences d'installation.

Vous aurez besoin des informations suivantes pour le déploiement des fichiers `.ear` d'application :

1. Nom d'emplacement = *<Nom d'emplacement DB2>* - indique votre nom d'emplacement DB2 for z/OS. Le nom d'emplacement doit être affiché dans le journal système **z/OS** lors du démarrage de DB2 for z/OS (DDF) :

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

2. ID utilisateur = *<nom d'utilisateur de base de données>* - représente un ID utilisateur **z/OS** ayant tous les accès de sécurité nécessaires activés pour se connecter à et gérer la base de données DB2 for z/OS ;
3. Mot de passe = *<mot de passe de la base de données>* - est le mot de passe de *<nom d'utilisateur de la base de données>*.

Post-installation

Pourquoi et quand exécuter cette tâche

Les étapes suivantes peuvent être exécutées à l'aide des interfaces DB2 for z/OS typiques ; par exemple SPUFI, DB2 Connect ou batch DB2. Fournissez des valeurs appropriées au site pour remplacer celles entre signes inférieur et supérieur (par exemple *<groupe_stockage>*) :

Procédure

1. Créez le groupe de stockage de base de données nécessaire.

   ```
   CREATE STOGROUP <groupe_stockage> VOLUMES (<volumes>)
     VCAT <nom_catalogue>;
   ```

2. Créez la base de données d'application Cúram - la base de données peut être configurée pour le mode EBCDIC, ASCII ou UNICODE. Cette étape peut être réalisée lors de la création de la base de données à l'aide du mot clé CCSID. Concernant les bases de données ASCII ou UNICODE, consultez «Propriétés d'amorce», à la page 7 pour plus d'informations sur la propriété obligatoire curam.db.zos.encoding.

   ```
   CREATE DATABASE CURAM BUFFERPOOL BP0 INDEXBP BP0
     STOGROUP <groupe_stockage> CCSID <EBCDIC, ASCII ou UNICODE>;
   ```

3. Assurez-vous que le paramètre DSNZPARM RRULOCK de la macro DSN6SPRM est défini sur YES.
4. Une variable d'environnement appelée DB2JCC_LICENSE_CISUZ_JAR doit être créée dans votre environnement shell de services système UNIX z/OS qui pointe vers le fichier JAR de licence DB2 for z/OS installé, servant pour la connectivité aux serveurs DB2 for z/OS sous **z/OS**. Cette variable est généralement appelée db2jcc_license_cisuz.jar et est fournie avec votre installation DB2 for z/OS.

Résultats

Remarque :

Les paramètres du module de paramètre DSNZPARM peuvent nécessiter des ajustements en vue de leur compatibilité avec Cúram, notamment le paramètre de seuil de délai d'attente de transaction inactive (IDTHTOIN). Il peut être nécessaire de l'augmenter pour certaines activités liées à l'initialisation de règles CER suite à une génération de base de données, comme la cible Ant prepare.application.data, car elle peut s'exécuter plus longtemps que les applications DB2 for z/OS en général. La durée d'exécution de ces activités et leur expiration dépend de plusieurs facteurs, mais les symptômes indiquant qu'il est nécessaire de modifier ce paramètre peuvent se manifester par l'envoi d'une erreur similaire à la suivante à l'interpréteur de commandes du client :

```
[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.
```

De plus, dans le journal système de z/OS, un message de dépassement de délai d'attente DSNL027I dont le code anomalie est 00D3003B peut être généré par DB2 simultanément. La documentation DB2 for z/OS pertinente contient des informations sur la modification de la valeur de délai d'attente des unités d'exécution inactives.

WebSphere Application Server for z/OS

Versions prises en charge

La version exacte de WebSphere Application Server for z/OS à installer est répertoriée dans le document *Conditions requises Cúram*.

Conditions préalables

Reportez-vous au manuel *Program Directory for WebSphere Application Server for z/OS V7.0 (GI11-4295)* pour connaître les conditions requises spécifiques de WebSphere Application Server for z/OS.

Installation

Avant de commencer la configuration et le déploiement de Cúram, on suppose que WebSphere Application Server for z/OS a bien été installé à l'aide des outils d'installation appropriés, conformément aux exigences de votre site et WebSphere Application Server for z/OS.

L'installation de WebSphere Application Server for z/OS est abordée dans plusieurs publications IBM et ainsi que dans la documentation du produit WebSphere Application Server version 7.0. Toutefois, la sécurité globale nécessite une discussion approfondie, qui est développée ci-après.

Sécurité globale - Configuration des paramètres de sécurité : L'activation de la sécurité globale WebSphere Application Server for z/OS fait basculer un gros commutateur, ce qui influence significativement le comportement de votre système WebSphere Application Server for z/OS sous z/OS. C'est pourquoi il vous est fortement recommandé de :

- Vous familiariser avec la documentation WebSphere Application Server for z/OS documentation sur la sécurité. Vous devez consulter ce qui suit en particulier :
  - Rubriques sur la sécurité dans le *centre de documentation WebSphere Application Server for z/OS*
  - Sécurisation des applications et de leur environnement dans la documentation du produit IBM WebSphere Application Server for z/OS version 7.0

Sachez que si vous possédez d'autres applications s'exécutant sur WebSphere Application Server for z/OS, celles-ci sont impactées par l'activation de la sécurité globale et risquent de ne plus fonctionner.

Post-installation

Les étapes suivantes doivent être effectuées :

- Une variable d'environnement appelée WAS_HOME doit être créée dans votre environnement shell de services système UNIX z/OS. Elle doit être définie sur le répertoire AppServer de l'installation WebSphere Application Server for z/OS (par exemple `/WebSphere/AppServer`).

Apache Ant

Présentation

Apache Ant est un outil intégré basé sur Java. Pour les utilisateurs habitués à des outils utilisés dans d'autres environnements, cet outil peut être considéré comme similaire à l'outil de marque.

Versions prises en charge

La version exacte d'Ant à installer est répertoriée dans le document *Conditions requises prises en charge Cúram*.

Installation

Le fichier zip Ant peut être obtenu à partir d'Apache et extrait vers un dossier sur votre machine comme suit :

- Placez le fichier zip Ant dans le système de fichiers des services système UNIX z/OS (par exemple `/usr/local`) et traitez le fichier, par exemple :

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

Où "<version>" représente la version appropriée identifiée dans le document *Conditions requises prises en charge Cúram v6.0*.

- Vérifiez que le script Ant dans `apache-ant-<version>/bin` est :
  - Au format de code EBCDIC ; par exemple :

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

  - Exécutable ; par exemple :

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

Post-installation

Pourquoi et quand exécuter cette tâche

Les étapes suivantes doivent être effectuées :

Procédure

1. Une variable d'environnement appelée ANT_HOME doit être créée dans votre environnement shell de services système UNIX z/OS qui pointe vers le répertoire d'installation sélectionné pour Ant ;
2. Ajoutez `$ANT_HOME/bin` au chemin d'exécution via votre variable PATH d'environnement de services système UNIX z/OS ;
3. Créez une variable d'environnement système, ANT_OPTS, dans votre environnement shell de services système UNIX z/OS, qui doit être définie au moins sur `-Xmx512m`.

Résultats

Test de la cible Ant en exécutant :

```
ant -version
```

Vous devez voir s'afficher la sortie indiquant la version et la date de compilation de la cible Ant.

Java SE Runtime Environment et Java EE

Présentation

Java SE Runtime Environment et Java EE sont tous les deux nécessaires.

Versions prises en charge

Les versions exactes à installer sont répertoriées dans le document *Conditions requises prises en charge Cúram*.

Installation

Les instructions d'installation spécifiques ne sont pas fournies pour Java SE Runtime Environment et Java EE sous **z/OS** car WebSphere Application Server for z/OS, version 7.0 fournit un environnement Java SE Runtime Environment et Java EE intégré, qui doit être utilisé. Consultez les informations fournies par IBM appropriées à votre environnement particulier.

Post-installation

- Une variable d'environnement appelée JAVA_HOME doit être créée dans votre environnement shell de services système UNIX z/OS qui pointe vers

l'environnement Java SE Runtime Environment installé. $JAVA_HOME doit être définie sur `$WAS_HOME/java`. `$JAVA_HOME/bin` doit être placée sur le chemin via votre variable d'environnement $PATH.

- Une variable d'environnement appelée J2EE_JAR doit être créée dans votre environnement shell de services système UNIX z/OS qui pointe vers le fichier JAR Java EE installé. Celui-ci doit pointer vers `$WAS_HOME/lib/j2ee.jar`.

Génération de fichiers EAR

Introduction

L'étape principale avant le déploiement d'une application IBM Cúram Social Program Management consiste à insérer l'application dans des fichiers EAR (Enterprise ARchive). Toutefois, la génération des fichiers `.ear` d'application ne peut pas être effectuée sous **z/OS** et doit être réalisée sous Windows ou tout autre environnement identifié comme pris en charge pour la génération dans le document *Conditions requises Cúram*.

Le reste de ce chapitre présente les exigences spécifiques à **z/OS** pour la génération de fichiers `.ear` compatibles avec **z/OS**. Pour plus d'informations sur la génération de fichiers `.ear` IBM Cúram Social Program Management, consultez le chapitre 2 du *Guide de déploiement Cúram pour WebSphere Application Server*. Vous trouverez également des informations utiles dans les manuels suivants :

- *Guide de l'atelier d'application Cúram* - Ce manuel contient des instructions de base concernant les fichiers `.ear` d'application ;
- *Guide de développement de serveur Cúram* - Ce manuel contient des instructions détaillées concernant une génération de serveur (chapitre 3) ;
- *Manuel de référence du client Web Cúram* - Ce manuel contient des instructions détaillées concernant le développement de client Web, y compris l'installation et la configuration (chapitre 4) ;

Remarques spécifiques à z/OS pour la génération de fichiers EAR d'application

Ces sections mettent en évidence les aspects spécifiques de la génération de fichiers `.ear` compatibles avec **z/OS**.

Fichiers de propriétés

Lors de la génération d'une application IBM Cúram Social Program Management, les fichiers `Bootstrap.properties` et `AppServer.properties` doivent être définis correctement pour la plateforme **z/OS** cible.

Propriétés d'amorce : Le fichier `Bootstrap.properties` contient les propriétés de configuration spécifiques à la machine pour obtenir une connexion initiale à la base de données. Accordez une attention particulière aux éléments suivants :

1. propriétés de base de données :

Tableau 1. propriétés de base de données spécifiques à z/OS for DB2

Propriété	Remarques
curam.db.type	Cette valeur doit être définie sur «zos».
curam.db.zos.enableforeignkeys	Définissez la valeur appropriée à votre environnement («vrai» ou «faux»).

Tableau 1. propriétés de base de données spécifiques à z/OS for DB2 (suite)

Propriété	Remarques
curam.db.zos.encoding	Indique si la base de données utilisée sur **z/OS** nécessite un traitement pour EBCDIC, ASCII ou UNICODE. Cette valeur doit être définie sur «EBCDIC», «ASCII» ou «UNICODE», en fonction du codage de base de données approprié en cours d'utilisation. «EBCDIC» est la valeur par défaut.
curam.db.zos.dbname	Cette valeur doit correspondre au nom de la base de données DB2 for z/OS.
curam.db.zos.32ktablespace	Cette valeur doit correspondre au nom de l'espace table 32K DB2 for z/OS.
curam.db.username	Cette valeur dépend de la configuration de votre système **z/OS** comme indiqué dans «DB2 for z/OS», à la page 3.
curam.db.password	Cette valeur dépend de la configuration de votre système **z/OS** comme indiqué dans «DB2 for z/OS», à la page 3. Etant donné qu'il s'agit d'un mot de passe chiffré, vous devez le générer en exécutant la cible chiffrée Ant sur n'importe quelle plateforme prise en charge ; par exemple **cd $CURAMSDEJ/bin; ant encrypt -Dpassword=<The password for curam.db.username>**
curam.db.name	Cette valeur correspond au nom de l'emplacement DB2 for z/OS comme indiqué dans «DB2 for z/OS», à la page 3.
curam.db.servername	Cette valeur dépend du nom d'hôte (ou de l'adresse IP) de votre système DB2 for z/OS.
curam.db.serverport	Cette valeur dépend de la configuration de votre système DB2 for z/OS.

2. propriétés dépendantes du système de fichiers :

Tableau 2. Propriétés dépendantes du système de fichiers z/OS

Propriété	Remarques
curam.environment.bindings.location	Cette valeur doit correspondre à un répertoire valide dans le système de fichiers des services système UNIX z/OS cible.

Propriétés AppServer : Accordez une attention particulière aux éléments suivants :

1. Les propriétés associées au port WebSphere Application Server for z/OS sont affichées dans tableau 3.

Tableau 3. Propriétés associées au port WebSphere Application Server for z/OS

Propriété	Remarques
curam.server.port	Cette valeur doit correspondre au port d'amorce WebSphere Application Server for z/OS (voir «Configuration de l'accès au port», à la page 38).

Tableau 3. Propriétés associées au port WebSphere Application Server for z/OS (suite)

Propriété	Remarques
curam.client.httpport	Cette valeur doit correspondre à la valeur de port CuramClientEndPoint (voir «Configuration de l'accès au port», à la page 38).
curam.webservices.httpport	Cette valeur doit correspondre à la valeur de port CuramWebServicesEndPoint (voir «Configuration de l'accès au port», à la page 38).

2. Les propriétés associées à la structure WebSphere Application Server for z/OS sont affichées dans tableau 4.

Tableau 4. Propriétés associées à la structure WebSphere Application Server for z/OS

Propriété	Remarques
curam.server.host	Cette valeur dépend du nom d'hôte (ou de l'adresse IP) de votre système DB2 for z/OS.
curam.server.name	Cette valeur doit correspondre au nom du serveur WebSphere Application Server for z/OS cible.
cell.name	Cette valeur doit correspondre à la cellule WebSphere Application Server for z/OS cible.
node.name	Cette valeur doit correspondre au nom du noeud WebSphere Application Server for z/OS cible.
profile.name	Pour WebSphere Application Server for z/OS, le seul nom de profil pris en charge est "défaut", qui correspond à la valeur par défaut.

Préparation de l'exécution de Cúram pour l'installation sous z/OS

Après avoir généré les fichiers `.ear`, vous devez les conditionner avec l'environnement d'exécution pour l'installation sous **z/OS**.

Par exemple, sous **Windows** (avec votre configuration d'environnement identique à celle du *Guide de déploiement Cúram pour WebSphere Application Server*), entrez les commandes suivantes :

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

Vous devez ensuite transmettre par **FTP** ou **copier** le fichier `release.zip` vers l'emplacement de votre système de fichiers **z/OS** cible.

Pour décompresser le fichier `release.zip` sous **z/OS**, vous devez établir deux variables d'environnement dans votre environnement shell de services système UNIX z/OS pour cette tâche et les suivantes :

Tableau 5. Variables d'environnement pour les services système UNIX z/OS

Variable d'environnement	Valeur
SERVER_DIR	représente l'emplacement dans lequel vous décompressez `release.zip` ; par exemple : `/curam/release`.

Tableau 5. Variables d'environnement pour les services système UNIX z/OS (suite)

Variable d'environnement	Valeur
CURAMSDEJ	représente le répertoire permettant d'exécuter des scripts de génération : `$CuramSDEJ`.

En ce qui concerne `release.zip` sur votre système **z/OS**, dans votre environnement shell, entrez les commandes suivantes pour le décompresser :

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

Configuration du serveur d'application

Introduction

Ce chapitre suppose que WebSphere Application Server for z/OS a déjà été installé sous **z/OS**. Consultez «Outils tiers», à la page 2 pour connaître les informations spécifiques à Cúram sur l'installation de WebSphere Application Server for z/OS.

La configuration de WebSphere est identique sur toutes les plateformes et un certain nombre de cibles Ant contribuent à la configuration et à la gestion de l'installation. Si vous êtes intéressé, la rubrique «Configuration manuelle de WebSphere Application Server», à la page 24 fournit des détails sur les étapes effectuées par les scripts de configuration.

La cible de configuration fournie par l'environnement SDEJ correspond à une simple configuration par défaut et ne convient peut-être pas à un environnement de production.

Remarque : Sous WebSphere Application Server for z/OS, le seul profil disponible est le profil par *défaut*, aucune autre option n'est possible.

La cible **`configure`** utilise le profil par *défaut* créé par WebSphere Application Server for z/OS. Il est fortement recommandé de conserver une copie de sauvegarde de votre système de fichiers de configuration WebSphere Application Server for z/OS au cas où vous auriez besoin de réexécuter la cible **`configure`** pour une raison quelconque.

Configuration de WebSphere Application Server

La configuration de WebSphere Application Server for z/OS inclut la définition d'une source de données, un certain nombre de serveurs ainsi que la configuration de JMS et de paramètres de sécurité. Toutes ces tâches peuvent être effectuées en exécutant la cible **`configure`** fournie.

Le profil créé par la cible **`configure`** Ant possède les valeurs par défaut suivantes. Lors de l'appel de la cible, la propriété cell.name peut être redéfinie ; cependant, la propriété profile.name ne peut posséder aucune autre valeur que celle par "défaut" car il s'agit de la seule valeur prise en charge par WebSphere Application Server for z/OS.

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

La commande **build.sh configure** doit être exécutée à partir du répertoire $SERVER_DIR pour appeler la configuration automatique. Cette cible nécessite que les fichiers AppServer.properties et Bootstrap.properties existent dans le répertoire $SERVER_DIR/project/properties[1]. Voir «Fichiers de propriétés», à la page 7 et le *Guide de développement de serveur Cúram* pour plus d'informations sur la configuration d'un fichier Bootstrap.properties. «Configuration de WebSphere Application Server», à la page 10 présente des exemples de contenus du fichier AppServer.properties.

Par défaut, la cible **configure** établit une source de données DB2 Universal Type 4 Driver (XA). Toutefois, vous pouvez configurer une source de données DB2 Universal Type 2 Driver (RRS) en définissant la propriété curam.db.type2.required dans le fichier AppServer.properties. Lorsque vous utilisez cette propriété, vous devez disposer de la variable d'environnement DB2DIR définie dans votre chemin d'installation DB2 for z/OS.

Il existe plusieurs manières possibles de configurer DB2 for z/OS et WebSphere Application Server for z/OS afin de prendre en charge un pilote de Type 2. Vous devez consulter la documnetation du produit WebSphere Application Server version 7.0 et l'article "DB2 Universal JDBC Driver Support", ainsi que les informations associées.

Il est possible de configurer un pilote Type 2 Universal Driver en transmettant une propriété facultative curam.db.zos.jcc.propfile, en indiquant le nom qualifié complet d'un fichier de propriétés de vérificateur d'exécution de travaux DB2 for z/OS qui est défini dans la propriété db2.jcc.propertiesFile JVM servante, pouvant contenir plusieurs paramètres tels que l'ID de sous-système.

1. Il est possible de redéfinir cet emplacement par défaut pour le fichier de propriétés en indiquant -Dprop.file.location=<new location> lors de l'exécution de la cible **configure**.

```
## APPLICATION SERVER PROPERTIES

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

# The username and encrypted password for admin server.
security.username=<e.g. websphere>
security.password=<encrypted password>

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

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

# The name of the server on which the application will be hosted.
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
```

Figure 1. Exemple de fichier de propriétés AppServer

Par défaut, la cible **configure** définit la taille de segment de mémoire initiale et maximale de la machine virtuelle Java sur "1024" Mo. Toutefois, vous pouvez remplacer la taille de segment de mémoire initiale et maximale par défaut de machine virtuelle Java en définissant la propriété curam.server.jvm.heap.size du fichier `AppServer.properties`.

Pour WebSphere Application Server for z/OS, vous devez également inclure une propriété cell.name égale au nom long de la cellule.

Remarque :

1. La configuration du segment de mémoire Java décrite dans l'exemple «Configuration de WebSphere Application Server», à la page 10 et définie par les scripts de configuration est fournie à titre d'information. Selon la taille de votre application personnalisée, stratégie de déploiement, etc., ces paramètres peuvent être trop faibles ou trop élevés. La valeur optimale doit être déterminée via le contrôle des performances de votre serveur en termes de mémoire.
2. Des problèmes de mémoire peuvent se produire avec les pilotes de base de données livrés WebSphere Application Server for z/OS au cours de la récupération des objets CLOB et BLOB (3 Mo minimum) à partir de la base de données. Ces problèmes peuvent être résolus en augmentant le paramètre JVM de taille de segment de mémoire maximale de manière appropriée sur le serveur déployé.

Autres emplacements des fichiers JAR

Si vous utilisez WebSphere Application Server for z/OS V8, un système de fichiers d'installation en lecture seule risque de causer des problèmes pour le placement des fichiers JAR de registre et de cryptographie de Cúram (décrits dans la rubrique «Redémarrage du serveur d'application», à la page 32). Par défaut, à chaque exécution de la cible Ant **configure**, ces fichiers JAR sont copiés dans le système de fichiers de configuration de WebSphere (`$JAVA_HOME/lib/ext` et `$WAS_HOME/lib`). Si le système sous-jacent de fichiers d'installation est monté en lecture seule, alors ces copies échoueront et il sera raisonnablement impossible de monter à nouveau le système de fichiers en lecture/écriture à chaque appel de la cible **configure**. Toutefois, il est possible de configurer un lien symbolique à l'aide du système de fichiers monté en lecture/écriture (activité unique), en indiquant un autre emplacement de copie pour ces fichiers.

Cette procédure unique s'effectue comme suit :

1. Montez le système de fichiers d'installation de WebSphere (par exemple `/usr/lpp/zWebSphere/V8R0`) en lecture/écriture.
2. Créez un lien symbolique dans le répertoire WebSphere `lib` vers le fichier Cúram `Registry.jar`. Ce fichier contient le module `CuramLoginModule`. Par exemple :

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

3. Créez un lien symbolique dans le répertoire Java `lib/ext` pour le fichier JAR de cryptographie de Cúram :`CryptoConfig.jar`. Par exemple :

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

4. Montez à nouveau le système de fichiers d'installation de WebSphere en lecture seule.

Les étapes ci-dessus permettent au système de fichiers WebSphere de rester en lecture seule lors de l'exécution de la cible **configure**, qui génère une copie de ces fichiers dans un autre emplacement qui pointe vers le système de fichiers d'installation. Lors de l'exécution de la cible Ant **configure**, indiquez les propriétés suivantes. Elles représentent les exemples d'emplacements présentés plus haut :

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

Configuration des paramètres de sécurité

La configuration des paramètres de sécurité par défaut d'IBM Cúram Social Program Management dans WebSphere Application Server for z/OS inclut le registre d'utilisateurs basé sur des fichiers par défaut ainsi qu'un module de connexion JAAS. Reportez-vous à la rubrique *Configuration par défaut d'IBM WebSphere Application Server* du *Manuel de sécurité Cúram* pour plus d'informations détaillées.

Plusieurs autres configurations des paramètres de sécurité peuvent être utilisées avec WebSphere Application Server for z/OS. Ces configurations permettent la prise en charge de l'utilisation de mécanismes d'authentification alternatifs, comme un serveur d'annuaire LDAP ou une solution à connexion unique.

Pour utiliser une configuration différente, les propriétés détaillées dans les rubriques suivantes doivent être définies dans le fichier `AppServer.properties`

avant d'exécuter la cible `configure`. Tous les mécanismes d'authentification alternatifs doivent être configurés manuellement après l'exécution de la cible `configure` avec l'ensemble de propriétés approprié. Pour configurer le module de connexion pour l'authentification par identité uniquement, la propriété curam.security.check.identity.only doit être définie sur Vrai. Cela permet de s'assurer que le mécanisme d'authentification alternatif configuré est utilisé.

Pour plus d'informations, consultez la rubrique Authentification par identité uniquement du *Manuel de sécurité Cúram*.

Configuration de fonction SAF (RACF)

Lors de la configuration de votre système WebSphere Application Server for z/OS pour utiliser la fonction SAF (RACF), après avoir configuré WebSphere Application Server for z/OS correctement avec l'outil de gestion de profil z/OS ou les panneaux de personnalisation de l'utilitaire Interactive System, vous devez définir la propriété curam.security.zos.saf sur Vrai avant d'exécuter la cible `configure`.

Lors de l'exécution de la cible `configure`, la valeur par défaut de la propriété curam.security.user.registry.enabled est Vrai. Le remplacement de cette valeur de curam.security.user.registry.enabled par Faux n'est pas recommandé. La propriété curam.security.check.identity.only peut être définie en fonction de vos exigences (voir ci-après).

Etapes de configuration spécifiques lors de l'utilisation de l'identité uniquement et de LDAP

Pourquoi et quand exécuter cette tâche

Lors de l'utilisation de l'identité uniquement avec WebSphere Application Server for z/OS et LDAP, il se peut que vous deviez effectuer des étapes de configuration manuelle supplémentaires, que la configuration soit effectuée via la console d'administration WebSphere Application Server for z/OS ou la cible `configure`. En utilisant cette combinaison, il se peut que le démarrage de WebSphere Application Server for z/OS échoue, car il est nécessaire d'ajouter un nom d'utilisateur généré par WebSphere Application Server for z/OS à la propriété de la liste d'exclusion du module de connexion (exclude_usernames) décrite dans «Ajout du module de connexion», à la page 34. Dans ce cas d'échec de démarrage de WebSphere Application Server for z/OS, un message d'erreur SECJ0270E apparaît dans le fichier `SystemOut.log` avant l'échec.

Procédez comme suit pour résoudre cette erreur :

Procédure

1. Identifiez le nom d'utilisateur à l'origine de l'échec de démarrage de WebSphere Application Server for z/OS. Configurez le suivi du module de connexion comme indiqué dans «Journalisation du processus d'authentification», à la page 16 (concernant la cible `configure`) ou «Ajout du module de connexion», à la page 34 (concernant la configuration via la console d'administration), puis redémarrez WebSphere Application Server for z/OS. Lorsque le suivi du module de connexion est en cours d'exécution, avant l'apparition de l'erreur SECJ0270E dans le fichier `SystemOut.log`, les données de suivi identifient le nom d'utilisateur à l'origine de l'erreur avec l'enregistrement suivant :

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

Où "MyNode" correspond au nom de noeud, "MyNodeCell" au nom de la cible et "CuramServer" au nom du serveur WebSphere Application Server for z/OS.

L'erreur figure à la suite des données de suivi du module de connexion, et ressemble à ceci :

```
SECJ0270E: Failed to get actual credentials.
   The exception is javax.security.auth.login.LoginException:
   Context: MyNodeCell/nodes/MyNode/servers/CuramServer,
   name: curamejb/LoginHome:
   First component in name curamejb/LoginHome not found.
```

2. Indiquez le nom d'utilisateur à l'origine de l'échec dans la propriété exclude_usernames du module de connexion de la configuration de WebSphere Application Server for z/OS. Dans la mesure où le démarrage de WebSphere Application Server for z/OS échoue, vous ne pouvez pas effectuer ce changement via la console d'administration et vous devez modifier le fichier de configuration de WebSphere Application Server for z/OS directement. Dans le système de fichiers de configuration de WebSphere Application Server for z/OS, modifiez `config\cells\MyNodeCell\security.xml`, qui doit comporter trois occurrences de la propriété exclude_usernames (une par alias) ; par exemple :

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

   Vous devez modifier les trois occurrences pour inclure le nom d'utilisateur nouvellement identifié à partir de l'entrée de suivi ci-dessus ; par exemple :

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

   Notez que dans les occurrences de la propriété exclude_usernames, l'attribut `id` varie selon votre configuration système et la virgule de l'exemple d'attribut de valeur représente la valeur curam.security.usernames.delimiter par défaut, qui peut différer dans votre cas.
3. Redémarrez WebSphere Application Server for z/OS.

Registre d'utilisateurs WebSphere Application Server

Par défaut, le registre d'utilisateurs WebSphere Application Server for z/OS configuré n'est pas requis dans le cadre de l'authentification. Lorsque le module de connexion est configuré pour l'identité uniquement, le registre d'utilisateurs est interrogé. Il est possible de remplacer ce comportement par défaut en définissant la propriété curam.security.user.registry.enabled. Si cette propriété est définie sur Vrai, le registre d'utilisateurs WebSphere Application Server for z/OS est interrogé lors du processus d'authentification, que l'authentification par identité uniquement soit activée ou non. Si cette propriété est définie sur Faux, le registre d'utilisateurs WebSphere Application Server for z/OS n'est pas interrogé. Par exemple, si curam.security.check.identity.only est défini sur Vrai et que curam.security.user.registry.enabled est défini sur Faux, ni les vérifications d'authentification Cúram ni le registre d'utilisateurs WebSphere Application Server for z/OS ne sont utilisés dans le cadre du processus d'authentification.

Vous pouvez également contrôler l'authentification des types d'utilisateurs externes (utilisateurs non internes) dans le registre d'utilisateurs WebSphere Application Server for z/OS via l'utilisation des propriétés curam.security.user.registry.enabled.types et/ou

curam.security.user.registry.disabled.types. Ces propriétés permettent d'indiquer une liste séparée par des virgules des types d'utilisateurs externes qui seront ou non authentifiés via le registre d'utilisateurs WebSphere Application Server for z/OS :

- Les types d'utilisateurs indiqués dans la liste curam.security.user.registry.enabled.types seront traités dans le registre d'utilisateurs WebSphere Application Server for z/OS (par exemple LDAP) et votre implémentation `ExternalAccessSecurity`.
- Les types d'utilisateurs indiqués dans la liste curam.security.user.registry.disabled.types ne seront pas traités dans le registre d'utilisateurs WebSphere Application Server for z/OS et le traitement de votre implémentation `ExternalAccessSecurity` fera autorité en ce qui concerne l'authentification.

L'ordre de priorité concernant le traitement de ces trois propriétés et le registre externe (LDAP) ou d'utilisateurs WebSphere Application Server for z/OS se présente comme suit :

- Par défaut, le registre d'utilisateurs WebSphere Application Server for z/OS n'est pas contrôlé et l'authentification d'application est utilisée.
- La définition de la propriété curam.security.user.registry.enabled sur `Vrai` nécessite l'authentification à la fois de la part de WebSphere Application Server for z/OS, ou du registre d'utilisateurs externe (LDAP), et de la sécurité d'application (pour les utilisateurs internes) ou de votre implémentation `ExternalAccessSecurity` (pour les utilisateurs externes).
- Un utilisateur externe d'un type spécifié dans la liste curam.security.user.registry.enabled.types doit être authentifié par WebSphere Application Server for z/OS, ou le registre d'utilisateurs externe et votre implémentation `ExternalAccessSecurity`.
- Un utilisateur externe spécifié dans la liste curam.security.user.registry.disabled.types n'est pas authentifié par WebSphere Application Server for z/OS, ni par le registre d'utilisateurs externe et votre implémentation `ExternalAccessSecurity` fait autorité.

Voir «Configuration du module de connexion JAAS du système», à la page 33 pour plus d'informations sur la définition des propriétés résultantes de la configuration `CuramLoginModule`.

Journalisation du processus d'authentification

curam.security.login.trace est une propriété facultative permettant la journalisation pour le module de connexion. Lorsqu'elle est définie sur vrai, cette propriété entraîne l'ajout des informations de suivi au fichier `SystemOut.log` de WebSphere Application Server for z/OS lors du processus d'authentification.

Etablissement d'un autre délimiteur Exclude Username

curam.security.usernames.delimiter est une propriété facultative permettant de définir un autre délimiteur pour la liste des noms d'utilisateur de la propriété exclude_usernames. La propriété peut être définie sur un caractère autorisant les noms d'utilisateur avec des virgules intégrées comme avec LDAP.

Comportement de mise en cache de WebSphere Application Server

WebSphere Application Server for z/OS met en mémoire cache les informations utilisateur et les données d'identification dans un cache de sécurité et le module de connexion de l'application n'est pas appelé tant qu'une entrée d'utilisateur est valide dans ce cache. La durée d'invalidation par défaut pour ce cache de sécurité

est de dix minutes, lorsque l'utilisateur a été inactif pendant dix minutes. Pour plus de détails, consultez la section *Comportement de la mise en cache WebSphere* dans le *manuel de sécurité Cúram*.

Propriétés personnalisées des paramètres de sécurité

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

  Cette propriété détermine le comportement d'une connexion Token2 avec authentification LTPA à connexion unique.

  Lorsque la valeur de cette propriété est définie sur Vrai, le jeton contient une clé de mémoire cache personnalisée ; et lorsque le sujet personnalisé est introuvable, le jeton permet de se connecter directement, étant donné que les informations personnalisées doivent être à nouveau regroupées. Une demande d'authentification se produit pour que l'utilisateur se connecte à nouveau. Lorsque la valeur de cette propriété est définie sur Faux et que le sujet personnalisé est introuvable, le jeton LTPA Token2 est utilisé pour se connecter et regrouper tous les attributs de registre. Cependant, le jeton peut n'obtenir aucun attribut spécial que des applications en aval attendent.

  Par défaut, le script de configuration définit une propriété WebSphere Application Server for z/OS, com.ibm.ws.security.webChallengeIfCustomSubjectNotFound, sur `Faux` pour s'assurer que les sessions Web peuvent effectuer un transfert homogène entre deux serveurs dans un cluster (par exemple, dans un scénario de basculement) sans que des données d'identification de sécurité ne soient nécessaires. Ce paramètre permet de valider correctement le jeton de sécurité utilisé par WebSphere Application Server for z/OS, sans intervention de l'utilisateur.

  Si ce comportement n'est pas requis, il est possible de définir cette propriété sur true. Voir «Configuration du module de connexion JAAS du système», à la page 33 pour plus d'informations sur la configuration des *Propriétés personnalisées des paramètres de sécurité*. Si la propriété est définie sur `true`, lorsqu'une session Web bascule d'un serveur du cluster vers un autre, peut-être en raison d'un échec du serveur d'origine, l'utilisateur devra fournir des informations de sécurité avant de pouvoir continuer.

Mesures de renforcement de la sécurité

Lorsqu'un utilisateur se connecte à l'application, il doit fournir un nom d'utilisateur et un mot de passe. Ces éléments sont envoyés au serveur, et si l'authentification aboutit, le serveur répond avec un jeton unique. Dans ce cas, le jeton correspond à un "Jeton LTPA". Ce jeton est utilisé dans toutes les demandes suivantes afin de reconnaître l'utilisateur, puis sert le contenu privilégié. Lorsque l'utilisateur se déconnecte, nous nous attendons à ce que ce jeton devienne invalide. Cependant ce n'est pas le cas, et il n'existe aucun moyen d'invalider le jeton LTPA, ayant été confirmé par IBM. **IBM recommande d'utiliser deux "mesures de renforcement de la sécurité" :**

1. Définition de l'option de sécurité SSL requis ;
2. Définition d'une propriété personnalisée pour limiter les cookies d'authentification LTPA au SSL uniquement.

Les scripts de configuration par défaut permettent d'effectuer ces changements et les étapes sont documentées dans la rubrique «Configuration de la sécurité de l'administration», à la page 31.

Pour plus d'informations, voir :

- 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

Cryptographie Cúram

La cryptographie Cúram est liée à la fonctionnalité de gestion des mots de passe et est abordée en détail dans le guide *Cúram Security Handbook*, que vous devez consulter en tenant compte des éléments suivants :

- Pour les environnements de production, il est fortement recommandé de modifier les paramètres par défaut.
- Pour les environnements de développement et de test, vérifiez si les valeurs par défaut fournissent une protection acceptable pour votre environnement.
- Dans le cadre d'une mise à niveau à partir d'une version précédente de IBM Cúram Social Program Management, les mots de passe existants ne sont pas intantanément utilisables. Si vous consentez à accepter un niveau de sécurité moindre et à vos risques et périls, vous pouvez décider de laisser en place le système et les mots de passe tels quels, mais ce n'est pas recommandé. Pour plus d'informations sur la mise à niveau, consultez le guide *Cúram Upgrade Guide*.

Mode 64 bits

Si vous utilisez la cible **configure**, la propriété curam.zos.64bitmode peut être spécifiée dans le fichier `AppServer.properties` avec une valeur Vrai afin que le serveur soit configuré pour la prise en charge du mode 64 bits.

Remarque : Lors de l'utilisation du mode 64 bits, vous pouvez également avoir besoin de réviser et d'adapter les tailles de segment de mémoire de la machine virtuelle Java en fonction de la taille de votre application, du débit, des objectifs de performances, ainsi que d'autres facteurs.

Configuration du fuseau horaire

Si plusieurs serveurs sont utilisés, leur horloge soit être synchronisée et faire partie du même fuseau afin que la hiérarchisation "naturelle" des dates/heures de la base de données reflète précisément l'ordre dans lequel les événements se sont réellement produits. Par exemple, si l'enregistrement de base de données *A* possède une zone de date/heure de création antérieure à celle de l'enregistrement *B*, nous pouvons donc affirmer que *A* a été créé avant *B*, quel que soit le serveur l'ayant créé.

Le fuseau horaire des serveurs ne doit jamais changer pendant la durée de vie de l'application. Ceci est dû au fait que le fuseau horaire supposé lors de l'enregistrement des dates dans la base de données correspond au fuseau horaire du serveur actuel ; ainsi, si le fuseau horaire du serveur change, alors toutes les dates saisies avant ce changement seront inexactes du nombre d'heure correspondant à la différence entre l'ancien et le nouveau fuseau horaire.

Démarrage et arrêt de serveurs WebSphere

Plusieurs cibles Ant sont fournies pour vous aider lors du démarrage et de l'arrêt de serveurs WebSphere Application Server for z/OS. Ces cibles doivent être exécutées à partir du répertoire `<SERVER_DIR>` et, comme pour la cible **configure**, nécessitent que le fichier `AppServer.properties` soit correctement configuré («Configuration de WebSphere Application Server», à la page 10). Elles nécessitent également la définition de plusieurs paramètres supplémentaires, détaillés ci-après.

Démarrage d'un serveur WebSphere

La cible Ant permettant de démarrer le serveur WebSphere Application Server for z/OS est **startserver** et nécessite les options suivantes :

- `-Dserver.name`

  Le nom du serveur à démarrer.

Important : Avant de démarrer le serveur d'application pour la première fois, vous devez avoir exécuté la cible **database** puis la cible **prepare.application.data**. Dans le cas contraire, cela entraîne des délais d'attente au niveau des transactions lors de la première connexion ainsi qu'un échec de l'initialisation et de l'accès à l'application. Quel que soit le moment où la cible **database** est réexécutée (dans un environnement de développement par exemple), il convient de réexécuter également la cible **prepare.application.data**.

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

Figure 2. Exemple d'utilisation

Arrêt d'un serveur WebSphere

La cible Ant permettant d'arrêter un serveur WebSphere Application Server for z/OS est **stopserver** et nécessite les options suivantes :

- `-Dserver.name`

  Le nom du serveur à arrêter.

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

Figure 3. Exemple d'utilisation

Redémarrage d'un serveur WebSphere

La cible Ant permettant le redémarrage d'un serveur WebSphere Application Server for z/OS est **restartserver** et les options sont identiques à celles de la cible **startserver**. Voir «Démarrage d'un serveur WebSphere» pour obtenir un exemple d'utilisation.

Remarque : Si le serveur n'a pas déjà été démarré lors d'une tentative de redémarrage, la portion d'arrêt de la cible n'entraînera pas un échec du redémarrage de la cible.

Déploiement

Introduction

L'étape finale suivant l'envoi de l'application IBM Cúram Social Program Management et de l'application de services Web dans les fichiers `.ear` et la configuration de WebSphere Application Server for z/OS consiste à déployer les fichiers `.ear` sur le serveur d'applications.

Avant le déploiement, il est important de noter que, dans WebSphere Application Server for z/OS, les scripts de configuration fournis avec IBM Cúram Social Program Management prennent en charge une configuration simple orientée vers une installation de serveur de base de WebSphere Application Server for z/OS.

Le déploiement inclut :

- Etablissement des fichiers de propriétés ;
- Installation des fichiers `.ear` ;

- Création d'une base de données ;
- Pré-compilation de JavaServer Pages (facultative mais fortement recommandée) ;
- Test de l'application.

Fichiers de propriétés

Pour installer les fichiers `.ear` d'application à l'aide de la cible Ant, vous devez posséder les fichiers de propriétés appropriés dans votre répertoire `$SERVER_DIR/project/property`. Ces fichiers sont les suivants :

- `Bootstrap.properties` - pour la création d'une base de données ;
- `AppServer.properties` - pour l'installation des fichiers `.ear`.

Cette section présente les éléments que ces fichiers doivent contenir. Pour plus d'informations, consultez le *Guide de développement de serveur Cúram*.

Bootstrap.properties

Les propriétés de déploiement spécifiques ou pertinentes pour WebSphere Application Server for z/OS sont présentées dans «Bootstrap.properties».

```
# 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
```

Figure 4. Fichier de propriétés Bootstrap relatif au déploiement

Certaines de ces propriétés sont décrites dans «Propriétés d'amorce», à la page 7 et sont identiques à celles dont vous avez besoin pour générer IBM Cúram Social Program Management sous Windows en vue du déploiement sur z/OS, mais notez ce qui suit :

- La <*Valeur de $SERVER_DIR*> est la valeur de votre variable d'environnement $SERVER_DIR.

AppServer.properties

Des propriétés de déploiement spécifiques ou pertinentes de WebSphere Application Server for z/OS sont présentées dans «AppServer.properties».

```
# 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

# The name of the server on which the application will be hosted.
curam.server.name=CuramServer
```

Figure 5. Fichier de propriétés AppServer relatif au déploiement

Certaines de ces propriétés sont décrites dans «Propriétés AppServer», à la page 8 et sont identiques à celles dont vous avez besoin pour générer les fichiers `.ear` de l'application IBM Cúram Social Program Management en vue du déploiement sous z/OS.

Vérification de la configuration

Vous pouvez vérifier vos fichiers de propriétés et votre configuration en exécutant la cible **`configtest`** Ant.

Exécutez la cible **`configtest`** à partir de l'interpréteur de commandes comme suit :

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

Consultez la sortie pour connaître les erreurs ou les avertissements éventuels et les résoudre.

Déploiement

Il existe des cibles Ant pour l'installation et la désinstallation des applications sur un serveur WebSphere Application Server for z/OS. Comme avec les cibles **`startserver`** et **`stopserver`**, les cibles **`installapp`** et **`uninstallapp`** nécessitent que le fichier `AppServer.properties` soit configuré correctement (voir «Configuration de WebSphere Application Server», à la page 10). Les cibles nécessitent également la configuration de plusieurs options, détaillées ci-après.

Vérifiez que le serveur a été démarré avant d'installer une application. Il n'est pas nécessaire de redémarrer le serveur après l'installation, dans la mesure où la cible démarre automatiquement l'application.

Installation d'une application

La cible Ant permettant d'installer une application (sous la forme d'un fichier `.ear`) est **`installapp`** et nécessite les options suivantes :

- `-Dserver.name`

  Nom du serveur permettant d'installer l'application.
- `-Dear.file`

  Nom qualifié complet du fichier `.ear` à installer.
- `-Dapplication.name`

  Nom de l'application

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

Figure 6. Exemple d'utilisation

Remarque : Le fichier `.ear` (EAR) contenant le module de serveur doit être déployé avant d'installer d'autres fichiers EAR (client uniquement).

Une propriété Ant facultative est disponible pour la transmission d'arguments supplémentaires WebSphere wsadmin : `wsadmin.extra.args`. Par exemple, la commande suivante définit de nouvelles tailles de segment de mémoire Java et transmet l'option afin d'ajouter le traçage wsadmin :

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

En fonction de l'interpréteur de commandes que vous utilisez, il se peut que vous deviez échapper les guillemets ci-dessus ; par exemple **`-Dwsadmin.extra.args=\"-appendtrace true\"`**. N'utilisez pas cette propriété pour définir des arguments déjà transmis via les scripts Curam Ant, que vous pouvez observer lorsque vous exécutez Ant en spécifiant son option prolixe : `-v`.

Modification du nom d'utilisateur SYSTEM

Il est fortement conseillé de modifier le nom d'utilisateur pour l'appel JMS lors du déploiement de l'application. Les propriétés suivantes doivent être définies dans le fichier `AppServer.properties` avant le déploiement pour modifier le nom d'utilisateur :

- curam.security.credentials.async.username

  Le nom d'utilisateur sous lequel les appels JMS doivent être exécutés.
- curam.security.credentials.async.password

  Le mot de passe chiffré associé au nom d'utilisateur. Le mot de passe doit être chiffré à l'aide de la cible Ant **`encrypt`**. Consultez le manuel *Cúram Server - Guide de développement* pour plus d'informations.

Il est également possible de modifier le nom d'utilisateur une fois que l'application a été déployée à l'aide de la console d'administration WebSphere Application Server for z/OS. Accédez à **Applications** > **Application Types (Types d'applications)** > **WebSphere enterprise applications (Applications d'entreprise WebSphere)** et sélectionnez l'application. Sélectionnez le lien **User RunAs roles (Rôles RunAs d'utilisateur)**. Sélectionnez le rôle `everyone`, entrez un nouveau nom d'utilisateur et mot de passe (le mot de passe doit être saisi dans un format chiffré) et cliquez sur le bouton **Appliquer**. Enregistrez les modifications comme indiqué dans «Enregistrement de la configuration principale», à la page 31.

Notez que si le nom d'utilisateur est modifié, le nouveau nom d'utilisateur doit exister dans la table de base de données des utilisateurs et cet utilisateur doit avoir un rôle de 'SUPERROLE'.

L'utilisateur SYSTEM correspond à l'utilisateur sous lequel les messages JMS sont exécutés.

Désinstallation d'une application

La cible Ant permettant de désinstaller une application est **`uninstall`** et nécessite les options suivantes :

- `-Dserver.name`

  Nom du serveur sur lequel l'application est installée.

- `-Dapplication.name`

  Nom de l'application à désinstaller (comme configuré lors de l'installation).

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

Figure 7. Exemple d'utilisation

Pré-compilation de JavaServer Pages

Il existe une cible supplémentaire disponible au cours du déploiement, **precompilejsp**, qui permet aux JavaServer Pages d'un client `.ear` d'être pré-compilées *avant* l'installation du fichier `.ear`. La pré-compilation des JavaServer Pages avant l'installation accélère l'affichage d'une page donnée dans le navigateur Web lorsqu'elle est visualisée pour la première fois.

Les options pour la cible **precompilejsp** sont les suivantes :

- `-Dear.file`

  Nom qualifié complet du fichier `.ear` à pré-compiler.

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

Figure 8. Exemple d'utilisation

Remarque : Il s'agit d'une activité d'exécution longue et en fonction des capacités de votre système, notamment, celle-ci peut prendre plusieurs heures. Vérifiez que votre tâche n'est pas limitée de façon significative par rapport au temps UC disponible et qu'il y ait un espace disponible approprié dans le système de fichiers $CURAMSDEJ.

En outre, lors de l'exécution de la cible **precompilejsp** pour WebSphere Application Server for z/OS, une exception de mémoire insuffisante peut se produire (ou des JavaServer Pages peuvent être ignorées et non pré-compilées silencieusement). Pour éviter ce problème, le script `JspBatchCompiler.sh` situé dans le répertoire `$WAS_HOME/bin` doit être modifié afin d'augmenter la taille de mémoire maximale. Modifiez et remplacez la consommation de mémoire `-Xmx256m` par `-Xmx1024m`.

Création d'une base de données

Pour utiliser l'application IBM Cúram Social Program Management, vous devez créer et initialiser une base de données. Cette section suppose l'utilisation de la cible **database** Ant pour créer une base de données. Toutefois, il est possible d'utiliser les outils du client DB2 pour ce faire. Pour plus d'informations sur cette méthode, consultez le *Guide d'installation Cúram*.

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

Figure 9. Exemples de commandes shell permettant de générer une base de données

Test du déploiement

Lorsque le ou les fichiers `.ear` d'application IBM Cúram Social Program Management sont installés[2] sur une installation WebSphere Application Server for z/OS configurée, l'étape suivante consiste à démarrer et à tester l'application.

2. L'installation d'une application de services Web peut également être requise.

Vérifiez que le serveur approprié a été démarré[3]puis ouvrez la page suivante dans un navigateur Web :

```
https://<une.machine.com>:<port>/<racine-contexte>
```

où

<une.machine.com> identifie le nom d'hôte ou l'adresse IP où votre système WebSphere Application Server for z/OS s'exécute, *<port>* désigne le port de serveur sur lequel l'application client est déployée (comme dans «Configuration de l'accès au port», à la page 38) et *<racine-contexte>* identifie la racine de contexte du module de fichier d'archive Web.

Avant d'ouvrir la page, le navigateur est dirigé vers la page de connexion. Connectez-vous à l'aide d'un nom d'utilisateur et d'un mot de passe Cúram valides. Le navigateur affiche alors la page demandée.

Remarque : L'utilisation du nom de fichier EAR `Curam.ear` pour l'option `-Dear.file` et l'utilisation du nom de serveur d'application `Curam` pour l'option`-Dapplication.name` dans les exemples de ce chapitre sont indiquées à titre d'information. Ces valeurs peuvent changer en fonction de votre application personnalisée et de la stratégie de déploiement.

Utilisation d'IBM WebSphere Application Server avec USGCB

L'initiative United States Government Configuration Baseline (USGCB) est une initiative du gouvernement fédéral américain qui guide les agences pour l'amélioration des paramètres de configuration, en mettant l'accent sur la sécurité. Lorsque vous exécutez l'application IBM Cúram Social Program Management, si vous utilisez IBM WebSphere Application Server version 7, (voir le guide *IBM Cúram Social Program Management v6 Supported Prerequisites* pour prendre connaissance des versions prises en charge d'IBM WebSphere Application Server version 7) avec les paramètres USGCB, il est possible que des images manquent. Si tel est le cas, cela signifie qu'IBM WebSphere Application Server ne reconnaît pas les fichiers .png. Pour résoudre ce problème, vous devez mettre à jour IBM WebSphere Application Server pour qu'il prenne en charge le type MIME PNG. Pour plus de détails, voir le *centre de documentation de WebSphere Application*.

Pour plus d'informations sur USGCB, visitez le site Web suivant : http://usgcb.nist.gov/

Configuration manuelle de WebSphere Application Server

Introduction

Ce chapitre présente les étapes manuelles requises pour procéder à la configuration et au déploiement sur une installation de serveur d'applications de base de WebSphere Application Server for z/OS. Il convient de modifier ces étapes de manière appropriée pour le déploiement dans une installation de déploiement réseau de WebSphere Application Server for z/OS. Voir «Déploiement réseau WebSphere», à la page 49 pour plus d'informations.

Configuration manuelle de WebSphere Application Server

L'installation IBM WebSphere Application Server for z/OS peut être configurée manuellement si nécessaire, cependant ce type de configuration n'est pas

3. Il n'est pas nécessaire de redémarrer le serveur une fois que l'application a été déployée.

recommandé si vous utilisez une installation de serveur d'applications de base. Cette section décrit les étapes requises pour la configuration de WebSphere Application Server for z/OS à titre indicatif uniquement.

Il convient de noter que les paramètres saisis sous la section **Ressources** de la console d'administration peuvent être configurés à différents niveaux permettant de contrôler la portée JNDI. Ils incluent la cellule, le noeud ou le serveur. Lors de la sélection d'une **Ressource**, la partie supérieure de la fenêtre de navigateur principale affiche cette portée et permet de visualiser les différentes ressources dans la portée actuelle. La portée ainsi que l'emplacement de l'ensemble de ressource doivent être basés sur une utilisation planifiée. Ainsi, en cas d'utilisation dans un cluster, il n'est pas nécessaire de définir les mêmes paramètres sur chaque serveur, et la portée peut donc être définie sur cellule ou noeud.

Console d'administration

La majeure partie de la configuration de WebSphere Application Server for z/OS est effectuée à l'aide de la console d'administration WebSphere. Pour que vous puissiez exécuter la console d'administration, le serveur du profil par défaut doit être démarré, car la console d'administration est installée en tant qu'application Web sur ce serveur (voir «Démarrage et arrêt de serveurs WebSphere», à la page 18 pour plus d'informations sur le démarrage des serveurs).

Pour ouvrir la console d'administration, un navigateur Web doit être pointé vers l'adresse suivante :

```
http://<Votre hôte WebSphere>:<port_http_protocole>/ibm/console
```

Où :

<*Votre hôte WebSphere*> représente le nom d'hôte ou l'adresse IP où votre système WebSphere Application Server for z/OS s'exécute et <*port_http_protocole*> représente le port affecté dans votre installation et dans la personnalisation de WebSphere Application Server for z/OS.

Prise en charge du scriptage

Pour prendre en charge l'exécution des scripts Ant fournis, il est nécessaire de modifier les fichiers de propriétés WebSphere Application Server for z/OS.

sas.client.props : Ouvrez le fichier `sas.client.props` qui se trouve dans le répertoire `profiles/default/properties` de l'installation WebSphere Application Server for z/OS. Il est nécessaire de définir la source de connexion afin de récupérer le nom d'utilisateur et le mot de passe d'un fichier de propriétés plutôt que de les saisir à chaque fois que les scripts sont exécutés. Définissez ou, le cas échéant, ajoutez les propriétés suivantes :

```
com.ibm.CORBA.loginSource=properties
# Identité de l'utilisateur RMI/IIOP
com.ibm.CORBA.loginUserid=websphere
com.ibm.CORBA.loginPassword=websphere
```

où *websphere* correspond au nom d'utilisateur et au mot de passe de la console d'administration.

soap.client.props : Ouvrez le fichier `soap.client.props`, également disponible dans le répertoire `profiles/default/properties` de l'installation WebSphere Application Server for z/OS. Il est nécessaire de définir la source de connexion afin de récupérer le nom d'utilisateur et le mot de passe d'un fichier de propriétés plutôt que de les saisir à chaque fois que les scripts sont exécutés. Définissez les

propriétés suivantes afin qu'elles correspondent aux données d'identification que vous avez configurées pour WebSphere, comme montré dans la rubrique «Configuration de WebSphere Application Server», à la page 10. Dans l'exemple ci-après, les valeurs sont de simples exemples et le mot de passe spécifié dans ce fichier ne peut pas être chiffré :

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

où *websphere* correspond au nom d'utilisateur et au mot de passe de la console d'administration.

Pour éviter des délais d'attente lors de l'installation des fichiers `.ear` d'application, assurez-vous que le paramètre suivant sont définis de manière appropriée :

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

Selon les performances de votre environnement, une valeur différente peut être requise.

server.policy : Ouvrez le fichier `server.policy` situé dans le répertoire `profiles/default/properties` de l'installation WebSphere Application Server for z/OS. Ajoutez les lignes suivantes à la fin du fichier :

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

Où <*CURAMSDEJ*> correspond au répertoire d'installation SDEJ.

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

où <*cell.name*> correspond au nom de la cellule WebSphere Application Server for z/OS cible

et <*SERVER_MODEL_NAME*> correspond au nom du fichier `.ear` (EAR) de l'application.

Création de l'alias de connexion à la source de données

Pourquoi et quand exécuter cette tâche

DB2 for z/OS est la base de données prise en charge sous z/OS. La console d'administration de WebSphere Application Server for z/OS est utilisée pour configurer un alias de connexion pour les sources de données DB2 for z/OS comme suit :

Procédure

1. Accédez à **Sécurité** > **Sécurité globale** ;
2. Développez l'option **Service JAAS** dans la zone **Authentification** et sélectionnez l'option **Données d'authentification J2C** ;
3. Cliquez sur le bouton **Nouveau** pour afficher l'écran Configuration ;
4. Définissez les zones suivantes :

Alias = dbadmin

ID utilisateur = <*nom d'utilisateur de base de données*>

Mot de passe = <*mot de passe de base de données*>

Description = l'alias de sécurité de la base de données

où <*nom d'utilisateur de base de données*> et <*mot de passe de base de données*> sont définis sur les noms d'utilisateur et mot de passe utilisés pour se connecter à la base de données ;

5. Appuyez sur le bouton **OK** pour confirmer les modifications.

Configuration des sources de données DB2 for z/OS

Pour **z/OS**, vous avez le choix entre la configuration avec le pilote Type 4 DB2 JDBC Universal Driver (XA) ou Type 2 DB2 JDBC Universal Driver (RRS).

Configuration d'un pilote Type 4 JDBC Universal Driver (XA) :

Configuration d'une variable d'environnement DB2 for z/OS

1. Accédez à **Environnement** > **WebSphere variables (Variables WebSphere)** ;
2. *Remarque :* La plage appropriée dans laquelle la source de données est définie doit être sélectionnée à ce moment-là.
3. Sélectionnez le lien DB2UNIVERSAL_JDBC_DRIVER_PATH dans la liste des variables d'environnement. Cela permet d'afficher l'écran de configuration de cette variable ;
4. Définissez la zone **Valeur** de manière à pointer vers le répertoire contenant les pilotes de Type 4. Il s'agit généralement du répertoire d'installation des `pilotes` SDEJ Cúram, par exemple `/CuramSDEJ/drivers` ;
5. Appuyez sur le bouton **OK** pour confirmer les modifications.

Configuration du fournisseur de pilote de base de données

1. Accédez à **Ressources** > **JDBC** > **Fournisseurs JDBC** ;
2. *Remarque :* la plage appropriée dans laquelle vous devez définir la source de données doit être sélectionnée à ce moment-là.
3. Appuyez sur le bouton **Nouveau** pour ajouter un nouveau pilote. Un écran de configuration s'affiche ;
4. Sélectionnez le menu déroulant **DB2** à partir de la liste des **types de base de données** fournie ;
5. Sélectionnez le menu déroulant **Fournisseur de pilote DB2 Universal JDBC** à partir de la liste de **Type de fournisseur** disponible ;
6. Sélectionnez le menu déroulant **Source de données XA** à partir de la liste des **Types d'implémentation** fournie ;
7. Appuyez sur le bouton **Suivant** pour continuer ;
8. Examinez les propriétés de l'écran de configuration qui s'affiche. Modifiez la ligne de chemin d'accès aux classes `${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar` pour qu'elle désigne la licence DB2 for z/OS fournie par IBM pour la connectivité DB2 for z/OS et cliquez sur **Appliquer**.
9. Appuyez sur le bouton **Suivant** puis sur **Terminer** pour confirmer les modifications.

Configurez la source de données du pilote de base de données

Les étapes suivantes doivent être répétées pour chacune des sources de données d'application, en remplaçant `curamdb`, `curamsibdb` et `curamtimerdb` par *<Nom_source_de_données>* (sans les signes supérieurs ou inférieurs) :

1. Sélectionnez le `fournisseur de pilote DB2 Universal JDBC (XA)` qui s'affiche dans la liste des **fournisseurs JDBC**. Cela permet d'afficher l'écran de configuration pour le fournisseur ;
2. Sélectionnez le lien **Sources de données** situé sous **Propriétés supplémentaires** ;
3. Appuyez sur le bouton **Nouveau** pour ajouter une nouvelle source de données ;
4. Définissez les zones comme suit :

   Nom de source de données : *<Nom_source_de_données>*

   Nom JNDI : *jdbc/<Nom_source_de_données>*

   Cliquez sur **Suivant** ;
5. Définissez les zones comme suit :

   Type de pilote : 4 ;

   Nom de base de données : Nom de la base de données DB2 for z/OS ;

   Nom de serveur : Nom du serveur de base de données DB2 for z/OS ;

   Numéro de port : Port du serveur de base de données DB2 for z/OS ;

   Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;
6. Définissez les zones comme suit :

   Définissez la valeur **Alias d'authentification géré par composant** sur : *<valide pour la base de données>* ;

   Définissez la valeur **Alias de configuration de mappage** sur : DefaultPrinicipalMapping ;

   Définissez la valeur **Alias d'authentification géré par conteneur** sur : *<valide pour la base de données>* ;

   où l'alias *<valide pour la base de données>* utilisé correspond à celui défini dans «Création de l'alias de connexion à la source de données», à la page 26 ;

   Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;
7. Appuyez sur le bouton **Terminer** pour confirmer les modifications et continuer ;
8. Sélectionnez la source de données *Nom_source_de_données* nouvellement créée dans la liste qui s'affiche ;
9. Sélectionnez le lien **Propriétés personnalisées** situé sous **Propriétés supplémentaires** ;
10. Sélectionnez l'entrée `fullyMaterializeLobData` ;
11. Définissez la `valeur` sur `false` ;
12. Cliquez sur le bouton **OK** pour confirmer la modification.

Configuration d'un pilote Type 2 JDBC Universal Driver (RRS) :

Configuration de variables d'environnement DB2

1. Accédez à **Environnement** > **WebSphere variables (Variables WebSphere)** ;

2. *Remarque :* La plage appropriée dans laquelle la source de données est définie doit être sélectionnée à ce moment-là.
3. Sélectionnez le lien DB2UNIVERSAL_JDBC_DRIVER_PATH dans la liste des variables d'environnement. Cela permet d'afficher l'écran de configuration de cette variable ;
4. Définissez la zone **Valeur** de manière à pointer vers le répertoire contenant le pilote de Type 2. Il s'agit généralement du chemin d'installation DB2 contenant le fichier `db2jcc.jar`.
5. Appuyez sur le bouton **OK** pour confirmer les modifications.
6. Sélectionnez le lien DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH dans la liste des variables d'environnement. Cela permet d'afficher l'écran de configuration de cette variable ;
7. Définissez la zone **Valeur** de manière à pointer vers le répertoire contenant les liens de la bibliothèque partagée DB2 for z/OS pour le pilote de Type 2. Il s'agit du chemin d'installation DB2 for z/OS contenant les bibliothèques du pilote de Type 2 (comme `libdb2jcct2zos.so`, qui diffère en fonction de la version de DB2 for z/OS et de l'implémentation 31 ou 64 bits) ;
8. Appuyez sur le bouton **OK** pour confirmer les modifications.

Configuration du fournisseur de pilote de base de données

1. Accédez à **Ressources** > **JDBC** > **Fournisseurs JDBC** ;
2. *Remarque :* la plage appropriée dans laquelle vous devez définir la source de données doit être sélectionnée à ce moment-là.
3. Appuyez sur le bouton **Nouveau** pour ajouter un nouveau pilote. Un écran de configuration s'affiche ;
4. Sélectionnez le menu déroulant **DB2** à partir de la liste des **types de base de données** fournie ;
5. Sélectionnez le menu déroulant **Fournisseur de pilote DB2 Universal JDBC** à partir de la liste des **types de fournisseur** disponible ;
6. Sélectionnez le menu déroulant **Source de données de pool de connexions** à partir de la liste des **types d'implémentation** fournie ;
7. Appuyez sur le bouton **Suivant** pour continuer ;
8. Passez en revue les propriétés sur l'écran de configuration qui s'ouvre, en vérifiant que les paramètres du chemin d'accès aux classes et du chemin d'accès à la bibliothèque native sont corrects, en fonction des valeurs préalablement définies pour les variables d'environnement DB2UNIVERSAL_JDBC_DRIVER_PATH et DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH. Aucune modification n'est requise ;
9. Appuyez sur le bouton **Suivant** puis sur **Terminer** pour confirmer les modifications.

Configurez la source de données du pilote de base de données

Les étapes suivantes doivent être répétées pour chacune des sources de données d'application, en remplaçant `curamdb`, `curamsibdb` et `curamtimerdb` par <*Nom_source_de_données*> (sans les signes supérieurs ou inférieurs) en procédant comme suit.

1. Sélectionnez le `Fournisseur de pilote DB2 Universal JDBC` désormais affiché dans la liste des **Fournisseurs JDBC**. Cela permet d'afficher l'écran de configuration pour le fournisseur ;

2. Sélectionnez le lien **Sources de données** situé sous **Propriétés supplémentaires** ;
3. Appuyez sur le bouton **Nouveau** pour ajouter une nouvelle source de données ;
4. Définissez les zones comme suit :

   Nom de source de données : *<Nom_source_de_données>*

   Nom JNDI : *jdbc/<Nom_source_de_données>*
5. Cliquez sur **Suivant** pour continuer ;
6. Définissez les zones comme suit :

   Nom de base de données : Nom de la base de données DB2 for z/OS ;

   Type de pilote : 2 ;

   Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;
7. Définissez les zones comme suit :

   Définissez la valeur **Alias d'authentification géré par composant** sur : *<valide pour la base de données>* ;

   Définissez la valeur **Alias de configuration de mappage** sur : DefaultPrinicipalMapping ;

   Définissez la valeur **Alias d'authentification géré par conteneur** sur : *<valide pour la base de données>* ;

   où l'alias *<valide pour la base de données>* utilisé correspond à celui défini dans «Création de l'alias de connexion à la source de données», à la page 26 ;

   Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;
8. Appuyez sur le bouton **Terminer** pour confirmer les modifications et continuer ;
9. Sélectionnez la source de données *Nom_source_de_données* nouvellement créée dans la liste qui s'affiche ;
10. Sélectionnez le lien **Propriétés personnalisées** situé sous **Propriétés supplémentaires** ;
11. Sélectionnez l'entrée `fullyMaterializeLobData` ;
12. Définissez la `valeur` sur `false` ;
13. Cliquez sur le bouton **OK** pour confirmer la modification.

Configurez le fichier db2.jcc.propertiesFile de la propriété JVM (facultatif)

Si vous souhaitez utiliser un fichier de configuration externe identifié par la propriété db2.jcc.propertiesFile pour votre pilote DB2 Type 2 Universal JDBC, procédez comme suit.

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Dans le panneau Infrastructure du serveur, développez **Gestion des processus et Java** ;
4. Sélectionnez le lien **Définition des processus** ;
5. Dans le panneau Type de processus, réalisez les étapes suivantes pour chaque élément de la liste (Assistant, Commande et Serviteur) :
   a. Sélectionnez le lien **Type de processus** ;

b. Dans le panneau Propriétés supplémentaires, sélectionnez le lien **Machine virtuelle Java** ;
c. Dans le panneau Propriétés supplémentaires, sélectionnez le lien **Propriétés personnalisées** ;
d. Cliquez sur le bouton **Nouveau** et définissez les propriétés comme suit :

   Nom : db2.jcc.propertiesFile

   Valeur : Nom qualifié complet du fichier de propriétés

   Cliquez sur le bouton **OK** pour ajouter la propriété.

   Pour plus d'informations sur la configuration du fichier de propriétés, voir «Configuration de WebSphere Application Server», à la page 10.

Enregistrement de la configuration principale

Un *Enregistrement* peut être effectué en cliquant sur le lien **Enregistrer** de la boîte de dialogue **Message(s)**. Cette boîte de dialogue s'affiche uniquement une fois les changements de configuration effectués.

Configuration de la sécurité de l'administration

Pourquoi et quand exécuter cette tâche

Le registre d'utilisateurs utilisé par défaut est le registre d'utilisateurs basé sur des fichiers WebSphere Application Server for z/OS par défaut.

Procédure

1. Accédez à **Sécurité** > **Sécurité globale** ;
2. Définissez **Définitions de superdomaines disponibles** sur **Référentiels fédérés** et cliquez sur le bouton **Configurer** ;
3. Définissez **Nom d'administrateur principal** sur `websphere` ;
4. Sélectionnez le bouton d'option **Identité de serveur généré automatiquement** ;
5. Sélectionnez **Ignorer maj/min pour l'autorisation** et cliquez sur le bouton **OK** ;
6. Entrez le mot de passe de l'administrateur par défaut, par exemple `websphere`, entrez la confirmation puis cliquez sur le bouton **OK** pour confirmer les modifications ;
7. Sélectionnez **Activer la sécurité administrative** ;
8. Sélectionnez **Activer la sécurité des applications** ;
9. Sélectionnez **Utiliser la sécurité Java 2 pour limiter l'accès aux applications par les ressources locales** et **Prévenir si des applications accordent des droits d'accès personnalisés** ;
10. Définissez **Définitions de superdomaines disponibles** sur **Référentiels fédérés** ;
11. Cliquez sur le bouton **Appliquer** pour confirmer les modifications ;
12. Accédez à **Sécurité** > **Sécurité globale** ;
13. Développez **Sécurité SIP et Web** et sélectionnez **Connexion unique** ;
14. Sélectionnez **Requiert SSL** ;
15. Cliquez sur **OK** pour confirmer la modification
16. Accédez à **Sécurité** > **Sécurité globale**
17. Sélectionnez le lien **Propriétés personnalisées** ;
18. Cliquez sur le bouton **Nouveau** puis définissez le nom et la valeur comme suit :

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

Valeur : `true`

19. Cliquez sur le bouton **OK** pour ajouter la nouvelle propriété.
20. Cliquez sur le bouton **Nouveau** puis définissez le nom et la valeur comme suit :

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

    Valeur : `true`
21. Cliquez sur **OK** pour confirmer la modification
22. Enregistrez les modifications apportées à la configuration principale.

Redémarrage du serveur d'application

Cette étape est obligatoire. Les espaces adresse WebSphere Application Server for z/OS doivent être redémarrés pour que les changements de sécurité s'appliquent et pour ajouter des utilisateurs obligatoires supplémentaires. Les espaces adresse peuvent être arrêtés à l'aide du script `stopServer.sh` approprié dans le répertoire `profiles/default/bin` de l'installation WebSphere Application Server for z/OS ou à l'aide de la commande **`STOP`** de l'opérateur **z/OS** appropriée pour votre installation.

Avant de redémarrer le serveur d'applications, il est nécessaire de mettre à disposition les fichiers JAR de registre et de cryptographie sur WebSphere Application Server for z/OS. Le fichier JAR de registre contient les classes nécessaires à la configuration de sécurité et le fichier JAR de cryptographie contient les paramètres de configuration et les données relatives à la sécurité par mot de passe.

`Registry.jar` est situé dans le répertoire `lib` de l'installation SDEJ. Copiez ce fichier dans le répertoire `lib` de l'installation WebSphere Application Server for z/OS.

Le fichier `CryptoConfig.jar` peut être généré en exécutant la commande configtest pour la cible ant, *build configtest -Dcrypto.ext.dir=filedir*. Copiez-le depuis l'emplacement généré. Copiez ce fichier dans le répertoire Java `jre/lib/ext`. Si vous devez personnaliser la configuration cryptographique de Curam, consultez le *manuel de sécurité Curam*.

Pour les sites disposant d'un système de fichiers d'installation WebSphere en lecture seule, consultez la procédure «Autres emplacements des fichiers JAR», à la page 13.

Démarrez maintenant le serveur d'applications à l'aide du script `startServer.sh` situé dans le répertoire `profiles/default/bin` de l'installation WebSphere Application Server for z/OS ou de la commande **`START`** de l'opérateur **z/OS** appropriée à votre installation puis ouvrez la console d'administration pour poursuivre les étapes de configuration.

Etant donné que la configuration des paramètres de sécurité est terminée et que les changements ont été effectués au niveau du scriptage, il est désormais possible d'utiliser les scripts SDEJ pour redémarrer le serveur d'applications. Voir «Démarrage et arrêt de serveurs WebSphere», à la page 18 pour plus d'informations sur le redémarrage du serveur.

La console d'administration doit ensuite être ouverte afin de poursuivre la configuration. Une fois la sécurité globale activée, il vous sera demandé de vous connecter à la console à l'aide du nom d'utilisateur *websphere* et du mot de passe *websphere* définis précédemment.

Test de la connexion DB2 for z/OS

Pourquoi et quand exécuter cette tâche

Vous pouvez tester vos connexions DB2 for z/OS une fois que le serveur d'applications a été redémarré :

Procédure

1. Accédez à **Resources (Ressources)** > **JDBC** > **Data Sources (Sources de données)** ;
2. Sélectionnez la case **curamdb DataSource** et/ou **curamsibdb DataSource** ;
3. Cliquez sur le bouton **Test Connection (Test de connexion)** ;
4. Le ou les messages suivants doivent s'afficher en cas de réussite :

```
Le test de la connexion pour Source de données <Nom de la source de données> sur le
serveur <nom du serveur> au niveau du noeud <nom du noeud> a abouti.
```

   Sinon, consultez les journaux WebSphere Application Server for z/OS pour des informations détaillées sur l'échec, la réussite et le nouvel essai.

Configuration des utilisateurs

Pourquoi et quand exécuter cette tâche

Comme indiqué dans «Configuration des paramètres de sécurité», à la page 13, le registre d'utilisateurs WebSphere Application Server for z/OS configuré est utilisé pour l'authentification des administrateurs et de l'utilisateur de base de données. Les administrateurs et l'utilisateur de base de données WebSphere Application Server for z/OS doivent être ajoutés manuellement au registre d'utilisateurs comme suit.

Procédure

1. Accédez à **Utilisateurs et groupes** > **Gérer les utilisateurs** ;
2. Sélectionnez le bouton **Créer** ;
3. Complétez les informations concernant l'administrateur WebSphere Application Server for z/OS et cliquez sur le bouton **Créer**.
4. Répétez ces étapes pour l'utilisateur de base de données.

Résultats

Remarque : Si la sécurité administrative de WebSphere Application Server for z/OS a été activée lors de la création du profil, l'administrateur est peut-être déjà défini dans le registre.

Configuration du module de connexion JAAS du système

La sécurité d'application utilise un module de connexion JAAS (Java Authentication and Authorization Service) pour l'authentification. Ce module de connexion doit être configuré pour les configurations DEFAULT, WEB_INBOUND et RMI_INBOUND. Répétez les étapes ci-après pour chacune de ces configurations.

Ajout du module de connexion :

1. Accédez à **Sécurité** > **Sécurité globale** ;
2. Développez l'entrée **Service JAAS** dans la section **Authentification** et sélectionnez **Connexions système** ;
3. Sélectionnez l'alias approprié dans la liste. Le module de connexion doit être configuré pour les alias DEFAULT, WEB_INBOUND et RMI_INBOUND comme suit :
4. Cliquez sur le bouton **Nouveau** pour configurer un nouveau module de connexion ;
5. Définissez la zone **Nom de la classe du module** sur `curam.util.security.CuramLoginModule` ;
6. Sélectionnez l'option **Utiliser le proxy de module de connexion** ;
7. Sélectionnez REQUIRED dans la zone **Stratégie d'authentification** ;
8. Cliquez sur le bouton **OK** pour confirmer l'ajout du nouveau module de connexion ;
9. Sélectionnez le module `curam.util.security.CuramLoginModule` récemment ajouté dans la liste ;
10. Sélectionnez le lien **Propriétés personnalisées** dans la section **Propriétés supplémentaires** ;
11. Cliquez sur le bouton **Nouveau** pour ajouter les propriétés obligatoires telles que répertoriées ci-après.

Tableau 6. Propriétés personnalisées CuramLoginModule

Nom	Exemple de valeur	Description
exclude_usernames	websphere, db2admin	Obligatoire. Une liste de noms d'utilisateurs à exclure de l'authentification. Cette liste doit inclure l'administrateur de WebSphere Application Server for z/OS (comme spécifié dans «Configuration de la sécurité de l'administration», à la page 31) et l'utilisateur de base de données (comme spécifié dans «Création de l'alias de connexion à la source de données», à la page 26). Le délimiteur par défaut est une virgule, cependant celui-ci peut être remplacé par exclude_usernames_delimiter. Tous les utilisateurs répertoriés ici doivent être définis dans le registre d'utilisateurs WebSphere Application Server for z/OS.
exclude_usernames_delimiter	|	*Facultatif*. Un délimiteur pour la liste des noms d'utilisateurs fourni dans exclude_usernames. Un délimiteur autre que la virgule par défaut peut être utile lorsque des noms d'utilisateurs comportent des virgules intégrées, comme dans le cas des utilisateurs LDAP.
login_trace	true	*Facultatif*. Cette propriété doit être définie sur `Vrai` pour déboguer le processus d'authentification. Si elle est définie sur `Vrai`, l'appel du module de connexion entraîne l'ajout des informations de suivi au fichier `SystemOut.log` de WebSphere Application Server for z/OS.

Tableau 6. Propriétés personnalisées CuramLoginModule (suite)

Nom	Exemple de valeur	Description
module_name	DEFAULT, WEB_INBOUND ou RMI_INBOUND	*Facultatif*. Cette propriété doit être définie sur DEFAULT, WEB_INBOUND ou RMI_INBOUND, selon la configuration pour laquelle le module de connexion est défini. Elle est utilisée uniquement lorsque la propriété login_trace est définie sur `Vrai` à des fins de suivi.
check_identity_only	true	*Facultatif*. Si cette propriété est définie sur `Vrai`, le module de connexion ne procède pas aux vérifications d'authentification habituelles. Au lieu de cela, il s'assure simplement que l'utilisateur existe dans la table de base de données. Dans ce cas, le registre d'utilisateurs WebSphere Application Server for z/OS configuré n'est pas ignoré et est interrogé après le module de connexion. Cette option est utile lorsque la prise en charge de LDAP est requise ou qu'un autre mécanisme d'authentification doit être utilisé.
user_registry_enabled	true	*Facultatif*. Cette propriété est utilisée pour remplacer le comportement qui consiste à ignorer le registre d'utilisateurs. Si cette propriété est définie sur Vrai, le registre d'utilisateurs WebSphere Application Server for z/OS est interrogé pendant le processus d'authentification. Si cette propriété est définie sur Faux, le registre d'utilisateurs WebSphere Application Server for z/OS n'est pas interrogé. **Remarque :** Si vous définissez l'identité uniquement et que vous utilisez LDAP, des étapes de configuration supplémentaires peuvent être nécessaires ; consultez la rubrique «Etapes de configuration spécifiques lors de l'utilisation de l'identité uniquement et de LDAP», à la page 14.
user_registry_enabled_types	EXTERNAL	*Facultatif*. Cette propriété permet d'indiquer une liste délimitée par des virgules des types d'utilisateurs externes traités dans le registre d'utilisateurs WebSphere Application Server for z/OS (par exemple LDAP). Pour plus d'informations sur le traitement du registre d'utilisateurs WebSphere Application Server for z/OS, consultez «Registre d'utilisateurs WebSphere Application Server», à la page 15.
user_registry_disabled_types	EXTGEN,EXTAUTO	*Facultatif*. Cette propriété permet d'indiquer une liste délimitée par des virgules des types d'utilisateurs externes non traités dans le registre d'utilisateurs WebSphere Application Server for z/OS (par exemple LDAP). Pour plus d'informations sur le traitement du registre d'utilisateurs WebSphere Application Server for z/OS, consultez «Registre d'utilisateurs WebSphere Application Server», à la page 15.

12. Cliquez sur **OK** pour confirmer l'ajout du nouveau module de connexion.

Réorganisation du module de connexion :

1. Accédez à **Sécurité** > **Sécurité globale** ;
2. Développez **Service JAAS** dans la section **Authentification** et sélectionnez **System logins (Connexions système)** ;

3. Sélectionnez l'alias approprié dans la liste. Le module de connexion doit être réorganisé pour les alias DEFAULT, WEB_INBOUND et RMI_INBOUND ;
4. Sélectionnez le lien **JAAS login modules (modules de connexion JAAS)** dans la section **Additional Properties (Propriétés supplémentaires)** ;
5. Cliquez sur le bouton **Set Order (Définir l'ordre)** ;
6. Sélectionnez **curam.util.security.CuramLoginModule** et cliquez sur le bouton **Déplacer vers le haut**. Répétez cette étape jusqu'à ce que l'entrée CuramLoginModule soit en haut de la liste ;
7. Cliquez sur le bouton **OK** pour confirmer les modifications apportées à l'ordre.

Désactivation de l'authentification entre les clusters : Cette propriété détermine le comportement d'une connexion Token2 avec authentification LTPA à connexion unique. La propriété com.ibm.ws.security.webChallengeIfCustomSubjectNotFound est définie sur `Faux` pour garantir que les sessions Web peuvent effectuer un transfert homogène entre deux serveurs dans un cluster (par exemple, dans un scénario de basculement) sans que des données d'identification de sécurité ne soient nécessaires.

1. Accédez à **Sécurité** > **Sécurité globale** ;
2. Cliquez sur **Propriétés personnalisées** dans la section **Authentification** et sélectionnez la propriété **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** dans la liste des propriétés disponibles.
3. Sous Propriétés générales, modifiez la valeur de la propriété **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** sur *false*
4. Cliquez sur le bouton **OK** pour confirmer l'ajout.

Enregistrement des modifications : Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Configuration de serveur

Configuration de la prise en charge 64 bits :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Cochez la case **Exécuter en mode JVM 64 bits** ;
4. Cliquez sur **Appliquer** ou **OK** pour appliquer les modifications ;
5. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Résultats

Remarque : Vous pouvez également avoir besoin de réviser et d'adapter les tailles de segment de mémoire de la machine virtuelle Java en fonction de la taille de votre application, du débit, des objectifs de performances, ainsi que d'autres facteurs.

Configuration de votre port de recherche JNDI :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;

2. Sélectionnez le serveur approprié dans la liste ;
3. Développez **Ports** dans la zone **Communications** et appuyez sur le bouton **Details (Détails)** ;
4. Sélectionnez l'entrée **BOOTSTRAP_ADDRESS** et définissez le **Port** afin de correspondre à la valeur de la propriété curam.server.port dans votre fichier `AppServer.properties` ;
5. Cliquez sur **OK** pour appliquer les modifications ;
6. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Configuration des paramètres de votre chargeur de classe :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Définissez **Classloader policy (Règle de chargeur de classe)** sur `MULTIPLE`;
4. Cliquez sur **OK** pour appliquer les modifications ;
5. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Configuration de votre Transmission par référence ORB :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Dans la section **Paramètres de conteneur**, développez **Services du conteneur** et cliquez sur le lien **Service ORB** ;
4. Sélectionnez l'option **Transmission par référence** dans la section **Propriétés générales** ;
5. Cliquez sur **OK** pour appliquer les modifications ;
6. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Configuration de votre machine virtuelle Java :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Dans le panneau Infrastructure du serveur, développez **Gestion des processus et Java** ;
4. Sélectionnez le lien **Définition des processus** ;
5. Dans le panneau Type de processus, réalisez les étapes suivantes pour chaque élément de la liste (Assistant, Commande et Serviteur) :
   a. Sélectionnez le lien **Type de processus** ;
   b. Dans le panneau Propriétés supplémentaires, sélectionnez le lien **Machine virtuelle Java** ;
   c. Définissez les zones comme suit :
      Taille de tas initiale : `1024`
      Taille de tas maximale :`1024`
      Cliquez sur **Appliquer** pour définir les valeurs ;

d. Dans le panneau Propriétés supplémentaires, sélectionnez le lien **Propriétés personnalisées** ;
e. Cliquez sur le bouton **Nouveau** et définissez les propriétés comme suit :

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

   Valeur : `false`

   Cliquez sur le bouton **OK** pour ajouter la propriété ;

6. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Configuration du service de minuteur :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Dans le panneau Container Settings (Paramètres du conteneur), développez **EJB Container Settings (Paramètres du conteneur d'EJB)** ;
4. Sélectionnez le lien **EJB timer service settings (Paramètre du service de minuteur EJB)** ;
5. Dans le panneau Scheduler Type (Type de planificateur), sélectionnez l'option **Use internal EJB timer service scheduler instance (Utiliser l'instance de planificateur du service de minuteur EJB interne)** ;
6. Définissez les zones comme suit :

   Data source JNDI name (Nom JNDI de la source de données) :`jdbc/curamtimerdb`

   Data source alias (Alias de la source de données) : *<valide pour la base de données>*

   où l'alias utilisé correspond à celui défini dans «Création de l'alias de connexion à la source de données», à la page 26 ;
7. Cliquez sur le bouton **OK** pour confirmer les modifications ;
8. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Configuration de l'accès au port :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Sélectionnez le lien **Ports** dans la zone **Communications** ;
4. Sélectionnez la zone **détails** ;
5. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes pour le port TCP/IP client :

   Nom de port défini par l'utilisateur : CuramClientEndPoint

   Hôte : *

   Port : *<port client>*

   Définissez le *<port client>* afin de correspondre à la valeur de la propriété curam.client.httpport dans votre fichier `AppServer.properties` ;

   Cliquez sur le bouton **OK** pour appliquer les modifications ;
6. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes pour le port TCP/IP WebServices :

Nom de port défini par l'utilisateur : CuramWebServicesEndPoint

Hôte : *

Port : *<port WebServices>*

Définissez le *<port WebServices>* afin de correspondre à la valeur de la propriété curam.webservices.httpport dans votre fichier `AppServer.properties` ;

Cliquez sur le bouton **OK** pour appliquer les modifications ;

7. Accédez à **Servers (Serveurs)** > **Server Types (Types de serveurs)** > **WebSphere application Servers (Serveurs d'application WebSphere)** ;
8. Sélectionnez le serveur approprié dans la liste ;
9. Développez la branche **Web Container Settings (Paramètres du conteneur Web)** dans la section **Container Settings (Paramètres de conteneur)** ;
10. Sélectionnez le lien **Web container transport chains (Chaînes de transport du conteneur Web)** ;
11. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes pour la chaîne de transport du client :

    Nom : `CuramClientChain`

    Modèle de chaîne de transport : `WebContainer-Secure`

    Cliquez sur **Suivant**

    Utiliser le port existant : `CuramClientEndPoint`

    Cliquez sur **Suivant** et **Terminer**
12. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes pour la chaîne de transport WebServices :

    Nom : `CuramWebServicesChain`

    Modèle de chaîne de transport : `WebContainer`

    Cliquez sur **Suivant**

    Utiliser le port existant : `CuramWebServicesEndPoint`

    Cliquez sur **Suivant** et **Terminer**
13. Sélectionnez l'élément **CuramClientChain** nouvellement créé ;
14. Sélectionnez le lien **HTTP Inbound Channel (Canal entrant HTTP)** ;
15. Vérifiez que la case **Use persistent keep-alive connections (Utiliser les connexions de signal de présence permanentes)** est sélectionnée ;
16. Cliquez sur le bouton **OK** pour confirmer l'ajout.
17. Accédez à **Environnement** > **Virtual hosts (Hôtes virtuels)** ;
18. Cliquez sur le bouton **Nouveau** pour ajouter un nouvel `Hôte virtuel` en définissant les zones suivantes ;

    Nom = *hôte_client*

    Répétez cette étape en remplaçant *hôte_client* par *hôte_webservices* ;
19. Sélectionnez le lien **hôte_client** depuis la liste des hôtes virtuels ;

    Sélectionnez le lien **Host Aliases (Alias hôtes)** dans la zone **Additional Properties (Propriétés supplémentaires)** ;

    Cliquez sur le bouton **Nouveau** pour ajouter un nouvel `Alias` en définissant les zones suivantes ;

    Nom d'hôte = *

    Port = *<port client>*

Définissez le <*port client*> afin de correspondre à la valeur de la propriété curam.client.httpport dans votre fichier `AppServer.properties` ; répétez cette étape pour l'autre hôte virtuel et l'autre port utilisés (par exemple hôte_webservices)

20. Cliquez sur le bouton **OK** pour confirmer l'ajout.
21. Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Configuration de l'intégration de la sécurité de session :
Procédure

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Cliquez sur **Gestion de session** dans la section **Paramètres de conteneur**.
4. Désélectionnez **Intégration de la sécurité**. *Remarque : vérifiez que l'intégration de la sécurité est décochée ;*
5. Cliquez sur **OK** pour appliquer les modifications ;
6. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

   Remarque :

   Le paramètre ci-dessus est obligatoire pour les applications Web IBM Cúram Social Program Management.

Configuration du bus

Configuration du bus d'intégration de services :
Procédure

1. Accédez à **Service integration (Intégration de service)** > **Buses (Bus)** ;
2. Cliquez sur le bouton **Nouveau** et définissez la zone suivante :

   Nom : CuramBus

   Laissez toutes les autres valeurs par défaut et cliquez sur **Suivant** ;
3. Au démarrage de l'assistant **Configure bus security (Configurer les paramètres de sécurité du bus)** (Etape 1.1) cliquez sur **Suivant** ;

   Dans l'**Etape 1.2** de l'assistant **Configure bus security (Configurer les paramètres de sécurité du bus)**, utilisez les paramètres par défaut et cliquez sur **Suivant** ;

   Dans l'**Etape 1.3** de l'assistant **Configure bus security (Configurer les paramètres de sécurité du bus)**, utilisez les paramètres par défaut, le cas échéant, et cliquez sur **Suivant** ;

   Dans l'**Etape 1.4** de l'assistant **Configure bus security (Configurer les paramètres de sécurité du bus)**, vérifiez vos paramètres et cliquez sur **Suivant** ;
4. Lors de l'Etape 2, cliquez sur **Terminer** pour appliquer les modifications.
5. Sélectionnez l'élément **CuramBus** qui s'affiche désormais dans la liste des bus. L'écran de configuration s'affiche ;
6. Sélectionnez **Bus members (Membres de bus)** dans la liste **Topology (Topologie)** ;

7. Cliquez sur **Ajouter** pour ouvrir l'assistant**Add a New Bus Member (Ajouter un nouveau membre de bus)** ;
8. Sélectionnez le serveur pour ajouter le bus et cliquez sur le bouton **Suivant** ;
9. Sélectionnez **Data store (Magasin de données)** et cliquez sur le bouton **Suivant** ;
10. Sélectionnez l'option **Use existing data source (Utiliser une source de données existante)** et définissez les options comme suit :

    Data source JNDI name (Nom JNDI de la source de données) = jdbc/curamsibdb

    Nom de schéma = *nom_utilisateur*

    Où *nom_utilisateur* correspond au nom d'utilisateur de la base de données.

    Désélectionnez l'option **Create tables (Créer des tables)** ;

    Laissez toutes les autres valeurs par défaut et cliquez sur **Suivant** ;
11. Utilisez les paramètres de réglage par défaut, le cas échéant, et cliquez sur **Suivant** ;
12. Cliquez sur **Terminer** pour terminer et quitter l'assistant ;
13. Accédez à **Service integration (Intégration de service)** > **Buses (Bus)** ;
14. Sélectionnez l'élément **CuramBus** qui s'affiche désormais dans la liste des bus. L'écran de configuration s'affiche ;
15. Sélectionnez **Sécurité** dans la section **Additional Properties (Propriétés supplémentaires)** ;
16. Sélectionnez **Users and groups in the bus connector role (Utilisateurs et groupes dans le rôle de connecteur de bus)** dans la section **Règles d'autorisation** ;
17. Cliquez sur **Nouveau** pour ouvrir l'utilitaire **SIB Security Resource Wizard (Assistant de ressources de sécurité SIB)** ;
18. Sélectionnez le bouton d'option **The built in special groups (Groupes spéciaux intégrés)** et cliquez sur **Suivant** ;
19. Sélectionnez les options **Serveur** et **AllAuthenticated** et cliquez sur **Suivant** ;
20. Cliquez sur **Terminer** pour terminer et quitter l'assistant.
21. Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Configuration JMS

Configuration des fabriques de connexions JMS :
Procédure

1. Accédez à **Ressources** > **JMS** > **Fournisseurs JMS** ;
2. *Remarque :* la plage appropriée dans laquelle vous devez définir les ressources JMS doivent être sélectionnées à ce moment-là.
3. Sélectionnez le lien **Fournisseur de messagerie par défaut** ;
4. Sélectionnez le lien **Fabriques de connexions** dans la zone **Propriétés supplémentaires** ;
5. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes :

   Nom : CuramQueueConnectionFactory

   Nom JNDI : jms/CuramQueueConnectionFactory

   Description : Fabrique de toutes les connexions aux files d'attente d'applications.

Nom du bus : CuramBus

Alias d'authentification de la reprise XA : identique à la source de données `jdbc/curamdb` (par exemple : <*SERVERNAME*> /dbadmin)

Alias de configuration de mappage : DefaultPrinicipalMapping

Alias d'authentification géré par conteneur : identique à l'alias d'authentification pour la récupération XA.

Laissez toutes les autres valeurs par défaut et cliquez sur le bouton **OK** pour appliquer les modifications ;

6. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes :

   Nom : CuramTopicConnectionFactory

   Nom JNDI : jms/CuramTopicConnectionFactory

   Description : Fabrique de toutes les connexions aux files d'attente d'applications.

   Nom du bus : CuramBus

   Alias d'authentification de la reprise XA : identique à la source de données `jdbc/curamdb` (par exemple : <*SERVERNAME*> /dbadmin)

   Alias de configuration de mappage : DefaultPrinicipalMapping

   Alias d'authentification géré par conteneur : identique à la source de données `jdbc/curamdb` (par exemple : <*SERVERNAME*> /dbadmin)

   Laissez toutes les autres valeurs par défaut et cliquez sur le bouton **OK** pour appliquer les modifications ;

7. Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Résultats

Remarque : En suivant les étapes de configuration manuelle ci-dessus, il n'est pas possible de configurer correctement les paramètres de sécurité pour la file d'attente Cúram et les fabriques de connexions de rubriques. Pour terminer cette partie de la configuration, vous devez utiliser l'outil `wsadmin`. Pour ce faire, quittez la console d'administration et effectuez les opérations suivantes :

1. Identifiez les entrées de file d'attente et de fabrique de connexions de rubriques dans le fichier `resources.xml` de configuration de WebSphere Application Server for z/OS. Ce fichier est situé dans l'arborescence du système de fichiers `%WAS_HOME%\profiles\<nom_profil>\config` en fonction de vos conventions d'attribution de noms et de la plage dans laquelle vous avez défini vos ressources JMS. Par exemple, lorsque vous utilisez une portée de niveau de noeud avec le nom de profil `AppSrv01`, le nom de cible `MyNodeCell` et le nom de noeud `MyNode`, ce fichier se trouve sous : `C:\WebSphere\profiles\AppSrv01\config\cells\MyNodeCell\nodes\MyNode\resources.xml`. Vous devez trouver dans ce fichier les entités `<factories>` pour `CuramQueueConnectionFactory` et `CuramTopicConnectionFactory` et noter l'ID de chaque élément qui commence `J2CConnectionFactory_` et est suivi d'un nombre (par exemple,1264085551611).
2. Appelez le script `wsadmin` WebSphere Application Server for z/OS. Dans ces exemples, le langage utilisé est JACL, ainsi, il peut être nécessaire de spécifier l'argument *-lang jacl* avec les données d'identification de connexion, etc., en fonction de votre configuration locale.
3. Dans `wsadmin`, appelez les commandes suivantes ; de nouveau, en supposant des définitions de portée de noeud, un nom de cible `MyNodeCell` et un nom de noeud `MyNode`, les ID ressource seront différentes dans votre environnement :

a. Obtenez l'identificateur du noeud et de la cellule : `$AdminConfig getid /Node:MyNode`
b. Combinez l'identificateur de noeud et l'identificateur de cellule obtenus à l'étape précédente avec l'identificateur de fabrique de connexions obtenu précédemment pour afficher la fabrique de connexions : `$AdminTask showSIBJMSConnectionFactory CuramQueueConnectionFactory(cells/MyNodeCell/nodes/MyNode|resources.xml#J2CConnectionFactory_1264085551611)`

   Dans la sortie de la commande ci-dessus, vérifiez que l'élément authDataAlias n'est pas défini (`authDataAlias=`) ; sinon, vous avez terminé, comme l'indique l'exemple de sortie wsadmin suivant :

```
{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. Pour définir authDataAlias, utilisez les mêmes informations de fabrique de connexions que précédemment, par exemple `$AdminTask modifySIBJMSConnectionFactory CuramQueueConnectionFactory(cells/MyNodeCell/nodes/MyNode|resources.xml#J2CConnectionFactory_1264085551611) {-authDataAlias crouch/databaseAlias}`
d. Sauvegardez les modifications : `$AdminConfig save`
e. Vous pouvez émettre la commande `showSIBJMSConnectionFactory` pour vérifier la modification.
f. Répétez les étapes ci-dessus pour `CuramTopicConnectionFactory`.
g. Quittez la session wsadmin avec la commande `quit`, après avoir sauvegardé vos modifications.

Configuration des files d'attente obligatoires :
Pourquoi et quand exécuter cette tâche

Dans la console d'administration, effectuez les étapes ci-après en remplaçant *<nom_file_d'attente>* (sans les chevrons) par les noms de file d'attente suivants : DPEnactment, DPError, CuramDeadMessageQueue, WorkflowActivity, WorkflowEnactment et WorkflowError.

Procédure

1. Accédez à **Intégration de services** > **Bus** > **CuramBus** ;
2. Sélectionnez le lien **Destinations** dans la zone **Ressources de la destination** ;

3. Cliquez sur le bouton **Nouveau** pour ouvrir l'assistant «Création d'une destination» :
4. Sélectionnez **File d'attente** comme type de destination et cliquez sur **Suivant** :
5. Définissez les attributs de file d'attente suivants :

   Identificateur : SIB_ *<nom_file_attente>*

   Laissez toutes les autres valeurs par défaut et cliquez sur le bouton **Suivant** ;
6. Utilisez le **Membre de bus sélectionné** et cliquez sur **Suivant** :
7. Cliquez sur **Terminer** pour confirmer la création de la file d'attente :
8. Sélectionnez la file d'attente SIB_ *<nom_file_d'attente>* nouvellement ajoutée qui s'affiche à présent dans la liste des fournisseurs existants. L'écran de configuration s'affiche à nouveau ;
9. Utilisez le tableau suivant pour définir la destination d'exception via le bouton d'option **Indiquer** et le texte associé classé ;

Tableau 7. Paramètres de destination d'exception

Nom de la file d'attente	Destination d'exception
SIB_CuramDeadMessageQueue	System
SIB_DPEnactment	SIB_DPError
SIB_DPError	SIB_CuramDeadMessageQueue
SIB_WorkflowActivity	SIB_WorkflowError
SIB_WorkflowEnactment	SIB_WorkflowError
SIB_WorkflowError	SIB_CuramDeadMessageQueue

10. Cliquez sur le bouton **OK** pour appliquer les modifications.
11. Accédez à **Ressources** > **JMS** > **Fournisseurs JMS** ;
12. Sélectionnez le lien **Fournisseur de messagerie par défaut** ;
13. Sélectionnez le lien **Files d'attente** dans la zone **Propriétés supplémentaires** ;
14. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes :

    Nom : *<nom_file_d'attente>*

    Nom JNDI : jms/ *<nom_file_d'attente>*

    Nom du bus : CuramBus

    Nom de la file d'attente : SIB_ *<nom_file_d'attente>*

    Mode de livraison : permanent

    Laissez toutes les autres valeurs par défaut et cliquez sur le bouton **OK** pour appliquer les modifications ;

Résultats

Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Configuration des rubriques obligatoires :
Procédure

1. Accédez à **Ressources** > **JMS** > **JMS providers (Fournisseurs JMS)** ;
2. Sélectionnez le lien **Default messaging provider (Fournisseur de messagerie par défaut)** ;
3. Sélectionnez le lien **Topics (Rubriques)** dans la zone **Additional Properties (Propriétés supplémentaires)** ;

4. Cliquez sur le bouton **Nouveau** et définissez les zones suivantes :

   Nom : CuramCacheInvalidationTopic

   Nom JNDI : jms/CuramCacheInvalidationTopic

   Description : rubrique d'invalidation de mémoire cache

   Bus name (Nom de bus) : CuramBus

   Topic space (Espace de sujet) : Default.Topic.Space

   JMS Delivery Mode (Mode de livraison JMS) : Nonpersistent

   Laissez toutes les autres valeurs par défaut et cliquez sur le bouton **OK** pour appliquer les modifications ;
5. Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Configuration des spécifications d'activation de la file d'attente obligatoire : Pourquoi et quand exécuter cette tâche

Comme pour la définition des files d'attente, effectuez ces étapes en remplaçant <*nom_file_d'attente*> (sans les chevrons) par les noms de files d'attente suivants : DPEnactment, DPError, CuramDeadMessageQueue, WorkflowActivity, WorkflowEnactment et WorkflowError.

Procédure

1. Accédez à **Ressources** > **JMS** > **JMS providers (Fournisseurs JMS)** ;
2. Sélectionnez le lien **Default messaging provider (Fournisseur de messagerie par défaut)** ;
3. Sélectionnez le lien **Activation specifications (Spécifications d'activation)** dans la zone **Propriétés supplémentaires** ;
4. Créez une nouvelle spécification en cliquant sur le bouton **Nouveau** et définissez les zones suivantes :

   Nom : <nom_file_d'attente>

   Nom JNDI : eis/ <*nom_file_d'attente*> AS

   Destination Type (Type de destination) : File d'attente

   Destination JNDI name (Nom JNDI de destination) : jms/ <*nom_file_d'attente*>

   Bus Name (Nom de bus) : CuramBus

   Alias d'authentification : identique à la source de données `jdbc/curamdb` (par exemple, <*SERVERNAME*> /dbadmin)

   Laissez toutes les autres valeurs par défaut et cliquez sur **OK** pour ajouter le port ;

Résultats

Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Configuration des spécifications d'activation de la rubrique obligatoire : Procédure

1. Comme pour les spécifications d'activation de file d'attente de la rubrique précédente, ajoutez une nouvelle spécification d'activation et définissez les zones suivantes :

Nom : CuramCacheInvalidationTopic

Nom JNDI : eis/CuramCacheInvalidationTopicAS

Destination Type (Type de destination) : Rubrique

Destination JNDI name (Nom JNDI de destination) : jms/CuramCacheInvalidationTopic

Bus Name (Nom de bus) : CuramBus

Alias d'authentification : identique à la source de données `jdbc/curamdb` (par exemple, <*SERVERNAME*> /dbadmin)

2. Laissez toutes les autres valeurs par défaut et cliquez sur le bouton **OK** pour appliquer les modifications.
3. Enregistrez les modifications apportées à la configuration principale, comme indiqué dans la rubrique «Enregistrement de la configuration principale», à la page 31.

Post configuration

Tables de base de données du bus d'intégration de services : Une fois la configuration effectuée, il convient de créer manuellement les tables de données requises pour le bus d'intégration de services. WebSphere Application Server for z/OS fournit un utilitaire permettant de générer le langage SQL pour la création de ces tables, le générateur de langage de définition de données SIB.

Le générateur peut être exécuté à l'aide de la commande suivante :

```
$WAS_HOME/bin/sibDDLGenerator.sh
  -system système
  -platform plateforme
  -schema nom_utilisateur
  -database nom_base_de_données
  -user nom_utilisateur
  -statementend ';'
  -create
```

Où

- *système* correspond à la base de données à utiliser, par exemple `db2` ;
- *plateforme* correspond au système d'exploitation, par exemple `zos` ;
- *nom_utilisateur* correspond au nom d'utilisateur qui est requis pour accéder à la base de données, comme indiqué dans la propriété `curam.db.username` dans le fichier `Bootstrap.properties` ;
- *nom_base_de_données* correspond au nom de la base de données à utiliser, comme indiqué dans la propriété `curam.db.zos.dbname` du fichier `Bootstrap.properties`.

Par exemple :

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

Cette commande génère des instructions SQL permettant de définir les tables de bus d'intégration de services et ces instructions SQL doivent être exécutées sur la base de données cible.

Remarque : Il existe des valeurs par défaut spécifiques à DB2 for z/OS pour les éléments STOGROUP et BUFFERPOOL. Pour plus d'informations, voir la documentation du produit WebSphere Application Server.

Tables de base de données du service de minuteur : Une fois la configuration effectuée, il convient de créer manuellement les tables de données requises pour le service de minuteur. WebSphere Application Server for z/OS fournit le langage de définition de données (DDL) pour ces tables dans son répertoire `$WAS_HOME/Scheduler`.

Les fichiers DDL qui doivent être exécutés sont `createTablespaceDB2ZOS.ddl` et `createSchemaDB2ZOS.ddl`, dans cet ordre.

Chaque fichier DDL contient des instructions appropriées à une exécution dans votre base de données cible.

Achèvement

WebSphere Application Server for z/OS est désormais configuré et prêt à l'installation des fichiers `.ear` de l'application IBM Cúram Social Program Management. Déconnectez-vous de la console d'administration et redémarrez WebSphere Application Server for z/OS à l'aide de la description des cibles disponible dans «Démarrage et arrêt de serveurs WebSphere», à la page 18.

Déploiement d'application manuel

Pourquoi et quand exécuter cette tâche

Pour installer une application d'entreprise dans WebSphere Application Server for z/OS, il est possible d'utiliser la console d'administration. Les étapes ci-après décrivent comment installer une application, un composant EJB ou le module Web à l'aide de la console d'administration.

Remarque : Une fois l'installation commencée, le bouton **Annuler** doit être utilisé pour quitter si l'installation de l'application est abandonnée. Vous ne pouvez pas simplement passer à une autre page de la console d'administration sans cliquer tout d'abord sur **Annuler** sur la page d'installation d'une application.

Procédure

1. Accédez à **Applications** > **Nouvelle application**;
2. Sélectionnez **Nouvelle application d'entreprise** ;
3. Cliquez sur le bouton d'option approprié et indiquez le chemin d'accès complet du fichier d'application source ou du fichier `.ear`, éventuellement via le bouton **Parcourir**, dans le panneau Chemin de la nouvelle application et cliquez sur **Suivant** ;

   L'emplacement par défaut des fichiers `.ear` d'application est :

   `$SERVER_DIR/ear/WAS/`
4. Sélectionnez le bouton d'option **Raccourci - Ne demander que si des informations supplémentaires sont requises** dans le panneau Comment voulez-vous installer l'application ? et cliquez sur **Suivant** ;
5. Conservez les valeurs par défaut de l'étape 1, *Sélectionner les options d'installation* et cliquez sur **Suivant** ;
6. Dans l'épate 2, **Mappage des modules vers les serveurs**, pour chaque module répertorié, sélectionnez un serveur cible ou un cluster dans la liste **Clusters et serveurs**. Pour ce faire, cochez la case située en regard des modules spécifiques, sélectionnez le serveur ou le cluster et cliquez sur **Appliquer**.

7. Pour l'étape ou les étapes suivantes, cliquez sur **Suivant** puis sur **Terminer** pour terminer l'installation. Cette étape peut prendre quelques minutes et doit se terminer avec un message indiquant que *l'installation de l'application Curam a abouti*.
8. Enregistrez les modifications apportées à la configuration principale. (Voir «Enregistrement de la configuration principale», à la page 31 pour plus d'informations.)
9. Accédez à **Applications** > **Types d'application** > **Applications d'entreprise WebSphere** et sélectionnez l'application nouvellement installée.
10. Sélectionnez l'option **Chargement de classes et détection de mise à jour** dans la section **Propriétés du détail**.
11. Définissez **Ordre du chargeur de classes** sur **Classes chargées en premier avec un chargeur de classe local (dernier parent)**.
12. Définissez **Règle du chargeur de classes WAR** sur **Chargeur de classes unique pour l'application**.
13. Cliquez sur **OK**.
14. Accédez à **Utilisateurs et groupes -> Gérer les utilisateurs**. Cliquez sur **Créer...** puis entrez un ID utilisateur, un mot de passe, un prénom et un nom. Cliquez ensuite sur **Créer**.

    Voir «Modification du nom d'utilisateur SYSTEM», à la page 22 pour plus d'informations concernant les données d'identification attendues par l'application et leur modification.
15. Retournez à l'application d'entreprise (**Applications** > **Types d'application** > **Applications d'entreprise WebSphere**, sélectionnez l'application nouvellement installée) et sélectionnez l'option **Mappage rôle de sécurité-utilisateur/groupe** dans la section **Propriétés du détail**, puis mappez le rôle mdbuser à un nom d'utilisateur et un mot de passe en suivant les étapes ci-après.

    Remarque :

    Le nom d'utilisateur que vous utilisez pour effectuer le mappage vers le rôle mdbuser doit déjà être défini dans votre registre d'utilisateurs.

    a. Cochez l'option **Sélectionner** pour le rôle mdbuser et cliquez sur **Mapper des utilisateurs...** ;
    b. Entrez le nom d'utilisateur approprié dans la zone **Chaîne à rechercher** et cliquez sur **Rechercher** ;
    c. Sélectionnez l'ID dans la liste **Disponible :**, cliquez sur **>>** pour l'ajouter à la liste **Sélectionné :**, puis cliquez sur **OK**.
    d. Cliquez sur **OK**.
16. Une fois le rôle mdbuser mappé, vous pouvez mettre à jour le rôle RunAs de l'utilisateur en sélectionnant l'option **Rôles d'exécution (RunAs) de l'utilisateur** dans la section **Propriétés du détail**.
17. Entrez le nom d'utilisateur et le mot de passe appropriés dans les zones **nom d'utilisateur** et **mot de passe**. Cochez l'option **Sélectionner** pour le rôle mdbuser et cliquez sur **Appliquer**.
18. Cliquez sur **OK**.
19. Enregistrez les modifications apportées à la configuration principale.
20. Une fois le déploiement effectué, il convient de démarrer l'application avant toute utilisation. Accédez à **Applications** > **Types d'application** > **Applications d'entreprise WebSphere**, cochez la case située en regard de l'application nouvellement installée, puis cliquez sur le bouton **Démarrer**.

Cette étape peut prend quelques minutes et doit se terminer par le changement du statut de l'application pour indiquer qu'elle a été démarrée.

21. Enfin, testez le déploiement de l'application. Par exemple, pointez un navigateur Web vers l'adresse URL de l'application déployée, comme :

    ```
    https://<Votre hôte WebSphere>:<CuramClientEndPoint>/Curam
    ```

    Où :

    <Votre hôte WebSphere> identifie le nom d'hôte ou l'adresse IP où votre système WebSphere Application Server for z/OS s'exécute et *<CuramClientEndPoint>* représente le port affecté (comme dans «Configuration de l'accès au port», à la page 38).

Déploiement réseau WebSphere

Le déploiement réseau IBM WebSphere Application Server fournit des services de déploiement avancé, dont le groupement, des services de pointe et une haute disponibilité pour les configurations réparties.

Astuces pour l'utilisation du déploiement réseau WebSphere

Personnalisation du déploiement réseau WebSphere : La personnalisation du déploiement réseau WebSphere (à l'aide de l'outil de gestion de profil z/OS ou de l'utilitaire Interactive System) n'entre pas dans la cadre de ce document. Toutefois, pour ce faire, IBM propose plusieurs documents Redbooks utiles. Ces derniers sont disponibles avec les informations fournies dans les manuels *Program Directory for WebSphere Application Server for z/OS V7.0 (GI11-4295)* et *IBM WebSphere Application Server for z/OS, Version 7.0: Installing your application serving environment (Documentation du produit WebSphere Application Server version 7.0*). IBM propose un grand nombre de Redbooks qui vous seront utiles. Vous trouverez ces documents sur le site Web IBM Redbook : http://www.redbooks.ibm.com/.

Synchronisation des changements : Si vous travaillez dans un environnement de déploiement réseau, il est fortement recommandé de vous assurer que WebSphere Application Server for z/OS synchronise sa configuration après *chaque* changement de console d'administration ou cible Ant.

Lorsque vous enregistrez la configuration principale, assurez-vous de forcer manuellement la synchronisation via la console d'administration :

1. Accédez à **System Administration (Administration de système)** > **Save Changes to Master Repository (Enregistrer les modifications apportées au référentiel maître)** ;
2. Sélectionnez l'option **Synchronize changes with Nodes (Synchroniser les modifications avec les noeuds)** ;
3. Cliquez sur le bouton **Enregistrer**. La synchronisation peut prendre quelques minutes ;
4. Sélectionnez les journaux système et/ou WebSphere Application Server for z/OS pour achever la synchronisation. Ces messages peuvent varier selon la version de WebSphere Application Server for z/OS, cependant vous voyez s'afficher un message du type :

```
ADMS0208I: The configuration synchronization complete for cell.
```

Une fois que la synchronisation est terminée, vérifiez le statut du serveur et divers journaux WebSphere Application Server for z/OS afin de vous assurer de sa réussite.

Configuration du noeud

Avant de déployer une application, le serveur doit d'abord être configuré. Cette opération s'effectue via la console d'administration du gestionnaire de déploiement, puis la configuration est synchronisée avec les serveurs fédérés du noeud.

L'agent de noeud, qui permet la communication entre le gestionnaire de déploiement et ses serveurs fédérés, doit être démarré. Cela peut être effectué via la commande **START** de l'opérateur **z/OS** appropriée à votre installation ou la commande `startNode.sh` du répertoire `profiles/<nom du profil fédéré>/bin` de l'installation WebSphere Application Server for z/OS.

Une fois l'agent de noeud démarré, le contrôle est transmis au gestionnaire de déploiement pour les serveurs de ce noeud. Pour démarrer ou arrêter un serveur de la console d'administration du gestionnaire de déploiement :

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Identifiez le serveur à démarrer/arrêter dans la liste, puis cliquez sur le bouton **Démarrer** ou **Arrêter**.

L'étape suivante du processus consiste à configurer les serveurs fédérés. Comme indiqué précédemment, la totalité de la configuration est effectuée via la console d'administration du gestionnaire de déploiement. «Configuration manuelle de WebSphere Application Server», à la page 24 décrit la configuration manuelle de WebSphere Application Server for z/OS pour une installation de base et doit être suivi avec les différences identifiées ci-après. Lors de l'enregistrement de la configuration principale, assurez-vous de synchroniser vos changements comme indiqué dans «Synchronisation des changements», à la page 49.

«Configuration du module de connexion JAAS du système», à la page 33 détaille la configuration de sécurité nécessaire lors d'une configuration manuelle. Cette configuration nécessite que le fichier `Registry.jar` soit copié dans un répertoire au sein de l'installation WebSphere Application Server for z/OS. Le fichier `Registry.jar` doit être copié depuis `CuramSDEJ/lib` vers le répertoire `lib` de l'installation du gestionnaire de déploiement et des installations fédérées.

«Configuration du module de connexion JAAS du système», à la page 33 Cette configuration de sécurité requiert également la copie du fichier `CryptoConfig.jar` dans le répertoire `java64/lib/ext` de l'installation WebSphere Application Server. Le fichier `CryptoConfig.jar` doit être copié dans la même structure de répertoire pour toutes les autres installations de WebSphere Application Server dans l'environnement.

Remarque : Avant de générer l'application `.ear` pour le déploiement, il convient de noter l'élément *BOOTSTRAP_ADDRESS* du serveur sur lequel celle-ci est installée. l'élément *BOOTSTRAP_ADDRESS* est situé dans la même liste de ports que l'élément *SOAP_CONNECTOR_ADDRESS* décrit précédemment.

Par défaut, l'élément *BOOTSTRAP_ADDRESS* attendu par l'application est 2809. Pour résoudre ce problème, modifiez cette adresse ou modifiez la propriété appropriée dans votre fichier `AppServer.properties`.

La propriété devant être modifiée est la valeur curam.server.port du fichier `AppServer.properties`. La modification de cette propriété affecte la valeur de port

du fichier `web.xml` lors de la génération d'un fichier `.ear` (EAR). Pour plus d'informations sur le fichier `web.xml`, consultez le guide *Cúram Web Client Reference Manual*.

Déploiement sur le noeud

Enfin, suivez les instructions de la rubrique «Déploiement d'application manuel», à la page 47 pour déployer manuellement les applications sur le serveur approprié. Les applications peuvent ensuite être démarrées ou arrêtées à l'aide de la console d'administration du gestionnaire de déploiement.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM. IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous accorde aucune licence pour ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations

IBM Canada Ltd

3600 Steeles Avenue East

Markham, Ontario

L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing

Legal and Intellectual Property Law.

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

© Copyright IBM Corp. 2012, 2013

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun autre pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUT RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

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

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

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies. Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Corporation

Dept F6, Bldg 1

294 Route 100

Somers NY 10589-3216

U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le programme sous licence décrit dans ce document et tous les éléments sous licence associés sont fournis par IBM selon les termes de l'IBM Customer Agreement, de l'IBM International Program License Agreement ou de tout contrat équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles.

IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

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

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Ces informations sont fournies uniquement à titre de planification. Elles sont susceptibles d'être modifiées avant la mise à disposition des produits décrits.

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

LICENCE DE COPYRIGHT :

Ces informations contiennent des exemples de programmes d'application en langage source qui illustrent des techniques de programmation sur diverses plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquels ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "EN L'ÉTAT", sans garantie d'aucune sorte. IBM décline toute responsabilité relative aux dommages éventuels résultant de l'utilisation de ces exemples de programmes.

Toute copie intégrale ou partielle de ces exemples de programmes et des oeuvres qui en sont dérivées doit inclure une mention de droits d'auteur libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des exemples de programmes d'IBM Corp.

© Copyright IBM Corp. _année ou années_. All rights reserved.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

Politique de confidentialité

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent,

aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-après.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des session et d'authentification, pour faciliter l'utilisation des produits, pour la configuration de la connexion unique et/ou pour d'autres fonctions de suivi ou buts fonctionnels. Ces cookies ou d'autres technologies similaires ne peuvent pas être désactivés.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/fr/fr, la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details/fr/fr, ainsi que la page "IBM Software Products and Software-as-a-Service Privacy Statement" à l'adresse http://www.ibm.com/software/info/product-privacy.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produit et de service peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse http://www.ibm.com/legal/us/en/copytrade.shtml.

Apache est une marque d'Apache Software Foundation.

Microsoft et Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

D'autres sociétés sont propriétaires des autres marques qui pourraient apparaître dans ce document. Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.