

IBM Cúram Social Program Management
Version 6.0.5

*Guide de déploiement de Cúram pour
WebSphere Application Server*



Important

Avant d'utiliser ces informations et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 45

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 CONTREFAÇON 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

Figures	v	Déploiement	15
Tableaux	vii	Introduction	15
Avis aux lecteurs canadiens.	ix	Déploiement	15
Déploiement sur IBM WebSphere		Installation d'une application	15
Application Server	1	Modification du nom d'utilisateur SYSTEM.	16
Introduction	1	Désinstallation d'une application	17
Guide de déploiement	1	Pré-compilation de JavaServer Pages	17
Génération de fichiers EAR	1	Test du déploiement	17
Introduction	1	Utilisation d'IBM WebSphere Application	
L'application d'entreprise	1	Server avec USGCB.	18
Génération du fichier EAR d'application	1	Configuration manuelle de WebSphere Application	
Sous le capot	2	Server	18
Contenu du fichier EAR d'application	2	Introduction	18
L'application de services Web.	3	Configuration manuelle de WebSphere	
Génération du fichier EAR de services Web	4	Application Server	18
Sous le capot	4	Console d'administration	19
Contenu du fichier EAR de services Web	4	Prise en charge du scriptage.	19
WSDL de service Web	5	Création de l'alias de connexion à la source de	
Fichiers EAR multiples	5	données	20
Cibles alternatives	7	Configuration de sources de données DB2	21
Configuration du serveur d'application	7	Configuration d'une source de données Oracle	22
Introduction	7	Enregistrement de la configuration principale	26
Configuration de WebSphere Application Server	8	Configuration de la sécurité de	
Configuration des paramètres de sécurité	10	l'administration	26
Etapes de configuration spécifiques lors de		Redémarrage du serveur d'application	27
l'utilisation de l'identité uniquement et de		Configuration des utilisateurs	27
LDAP	10	Configuration du module de connexion JAAS	
Registre d'utilisateurs WebSphere Application		du système	28
Server	11	Configuration de serveur	30
Journalisation du processus d'authentification	12	Configuration du bus	33
Etablissement d'un autre délimiteur Exclude		Configuration JMS	34
Username	12	Configuration des fichiers journaux	
Comportement de mise en cache de		d'historique	39
WebSphere Application Server	12	Post configuration	39
Propriétés personnalisées des paramètres de		Achèvement	40
sécurité.	13	Déploiement d'application manuel.	40
Mesures de renforcement de la sécurité	13	Déploiement réseau WebSphere	42
Cryptographie Cúram	14	Création de profils	42
Configuration du fuseau horaire	14	Fédération d'un noeud	42
Démarrage et arrêt de serveurs WebSphere.	14	Configuration du noeud	43
Démarrage d'un serveur WebSphere	14	Déploiement sur le noeud	44
Arrêt d'un serveur WebSphere	15	Remarques	45
Redémarrage d'un serveur WebSphere	15	Politique de confidentialité	47
		Marques	48

Figures

1.	Exemple de fichier deployment_packaging.xml	6	5.	Exemple d'utilisation	16
2.	Exemple de propriétés AppServer	9	6.	Exemple d'utilisation	17
3.	Exemple d'utilisation	15	7.	Exemple d'utilisation	17
4.	Exemple d'utilisation	15			

Tableaux

1. Propriétés personnalisées CuramLoginModule 28
2. Paramètres de destination d'exception. . . . 37

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Déploiement sur IBM WebSphere Application Server

Des fichiers du serveur de client Web et des fichiers EAR d'application sont requis pour générer une application IBM Cúram Social Program Management à déployer sur IBM WebSphere Application Server. Plusieurs paramètres de configuration sont également requis pour le déploiement.

Introduction

Guide de déploiement

Ce guide présente les étapes nécessaires à la création d'une application IBM® Cúram Social Program Management pour le déploiement sur la version de base de IBM WebSphere Application Server¹. Le guide détaille également la prise en charge fournie pour la configuration et le déploiement sur WebSphere Application Server, et, le cas échéant, les étapes obligatoires devant être effectuée manuellement.

Le lecteur doit connaître l'environnement de développement IBM Cúram Social Program Management. Autrement dit, il doit savoir comment développer et générer un client Web et une application de serveur. Ce guide suppose également que WebSphere Application Server a déjà été installé. Pour plus d'informations sur cette installation, consultez le manuel *Cúram Third Party Tools Installation Guide*².

Génération de fichiers EAR

Introduction

La principale étape avant le déploiement d'une application IBM Cúram Social Program Management consiste à la placer dans des fichiers EAR (Enterprise ARchive). L'application serveur (qui inclut le serveur et le client Web) et application de services Web sont placées dans des fichiers EAR distincts, et Server Development Environment (SDEJ) fournit des cibles générées permettant d'effectuer cette tâche.

Avant que les cibles décrites dans la rubrique suivante ne soient exécutées, vérifiez que la variable d'environnement suivante est définie :

- WAS_HOME

Celle-ci doit pointer vers le répertoire de base de l'installation WebSphere Application Server de base. Par exemple : d:\WebSphere\AppServer ou /opt/WebSphere/AppServer.

L'application d'entreprise

Génération du fichier EAR d'application

La cible suivante doit être exécutée à partir du répertoire principal du projet serveur afin de créer le fichier EAR d'application pour WebSphere Application Server :

1. Pour plus d'informations sur l'utilisation de l'application avec l'édition de déploiement réseau de WebSphere Application Server consultez «Configuration manuelle de WebSphere Application Server», à la page 18.

2. Reportez-vous au guide d'installation relatif à votre plateforme (Microsoft Windows ou UNIX).

build websphereEAR

Cette cible crée un fichier EAR prêt à installer, <SERVER_MODEL_NAME>.ear situé dans <SERVER_DIR>/build/ear/WAS³.

Avant d'exécuter cette cible, une application entièrement générée doit être disponible. Pour plus d'informations sur la génération d'une application IBM Cúram Social Program Management, veuillez consulter le manuel *Cúram Server - Guide de développement*.

Remarque : Il n'est pas possible de générer de fichier EAR pour une base de données H2.⁴

Sous le capot

La cible **websphereEAR** prend plusieurs descripteurs de déploiement et fichiers Java générés précédemment et les regroupe dans un fichier EAR.

Les descripteurs de déploiement et fichiers Java sont générés lors du processus de construction en fonction de l'existence de classes d'objets de processus métier (BPO), soit les méthodes de classes *Façade* ou de classes *WebService*, et peuvent être appelés par des clients distants.

Par défaut, tous les appels distants vers le serveur sont traités par le bean session `curam.util.invoke.EJBMethod`, plutôt qu'un bean session par interface accessible au public. Ce bean fournit une prise en charge des fonctions IBM Cúram Social Program Management comme les autorisations, le contrôle et le suivi. Si nécessaire, il est également possible de générer une interface de façade⁵.

Contenu du fichier EAR d'application

Le fichier EAR généré possède la structure et le contenu suivants :

- Répertoire META-INF
 - `application.xml`

Ce fichier est généré automatiquement et répertorie le mappage de modules EJB vers les fichiers JAR contenus dans l'application.
 - `ibm-application-bnd.xmi`

Un fichier d'extension spécifique à WebSphere Application Server généré.
 - `ibm-application-ext.xmi`

Un fichier d'extension spécifique à WebSphere Application Server généré.
 - `was.policy`

Un fichier de règles de sécurité WebSphere Application Server accordant une autorisation Java `java.security.AllPermission` à l'application.
 - `MANIFEST.MF`

Le fichier manifeste détaillant le contenu du fichier EAR.
- **Fichiers JAR principaux**

Les fichiers JAR principaux incluent les éléments suivants ⁶:

3. `SERVER_MODEL_NAME` et `SERVER_DIR` représentent des variables d'environnement indiquant le nom du modèle dans le projet ainsi que le répertoire principal du projet.

4. Pour plus d'informations sur la base de données H2, consultez le manuel *Cúram Third-Party Tools - Guide d'installation pour Windows*.

5. Le paramètre de génération facultatif `-Denablefacade=true` active la génération du code de façade

6. Les numéros de version ne sont pas répertoriés pour les fichiers JAR détaillés.

- antlr.jar
- appinf.jar
- appinf_internal.jar
- coreinf.jar
- rules.jar
- jde_commons.jar
- log4j.jar
- commons-pool.jar
- commons-codec.jar
- commons-discovery.jar
- jdom.jar
- axis.jar
- castor.jar
- jaxrpc.jar
- saaj.jar
- java_cup.zip
- InfrastructureModule.jar
- InvalidationModule.jar
- DBtoJMS.war
- ClientModule.war

- **Fichiers JAR de façade**

Ils sont présents uniquement si la génération de façade a été activée. Toutes les façades définies dans l'application sont regroupées dans un fichier JAR, FacadeModule.jar. Ce fichier JAR contient les classes d'implémentation bean pour les modules EJB représentant les façades. Le fichier JAR contient les fichiers suivants dans le répertoire META-INF :

- ejb-jar.xml

Ce fichier est généré automatiquement et contient la définition de tous les modules EJB contenus dans le fichier JAR. Toutes les méthodes accessibles au public sont répertoriées et les détails des ressources accessibles aux modules EJB.

- ibm-ejb-jar-bnd.xmi

Un fichier d'extension spécifique à WebSphere Application Server généré.

- ibm-ejb-jar-ext.xmi

Un fichier d'extension spécifique à WebSphere Application Server généré.

- Manifest.mf

Le fichier manifeste, détaillant le chemin d'accès aux classes pour EJB.

- **Autres fichiers JAR**

Les autres fichiers JAR contiennent le code composé à la main et généré depuis l'application. Ils incluent les fichiers suivants : application.jar, codetable.jar, events.jar, struct.jar, messages.jar, implementation.jar et properties.jar. Le fichier properties.jar contient le fichier Bootstrap.properties. Il s'agit du fichier contenant les propriétés de configuration spécifiques à la machine permettant la connexion initiale à la base de données.

L'application de services Web

Une prise en charge est disponible pour la génération automatique des services Web WSDL définis à l'aide de WSDL (Web Service Definition Language). Les

développeurs d'applications peuvent alors combiner la puissance du modèle IBM Cúram Social Program Management à l'accessibilité des services Web afin de produire des composants logiciels réutilisables.

Génération du fichier EAR de services Web

La cible suivante doit être exécutée à partir du répertoire principal du projet pour créer le fichier EAR pour les services Web :

build webspHEREWebServices

Les remplacements facultatifs sont les suivants :

- `prp.webipaddress` correspond à l'adresse IP sur laquelle le serveur hébergeant le service Web est en mode écoute. La valeur par défaut est `http://localhost:2809` ;
- `prp.contextproviderurl` correspond à l'URL du fournisseur de contexte JNDI. Il s'agit de l'adresse du serveur hébergeant les composants IBM Cúram Social Program Management mis à disposition via les services Web. La valeur par défaut est `iiop://localhost:2809` ;
- `prp.contextfactoryname` correspond au nom d'usine du contexte JNDI. La valeur par défaut est `com.ibm.websphere.naming.WsnInitialContextFactory` et doit rarement être modifiée.

Cette cible crée un fichier EAR prêt à installer, `<SERVER_MODEL_NAME>WebServices.ear`, situé dans `<SERVER_DIR>/build/ear/WAS`.

Avant d'exécuter cette cible, une application IBM Cúram Social Program Management entièrement générée, prête pour le déploiement, doit exister.

Sous le capot

La cible **webspHEREWebServices** prend plusieurs descripteurs de déploiement et fichiers Java générés précédemment et les regroupe dans un fichier EAR.

Les descripteurs de déploiement et fichiers Java sont générés lors du processus de construction (voir le manuel *Cúram Server - Guide de développement*) en fonction des *composants de service Web* ayant été définis dans le modèle. Les classes BPO doivent être mappées aux composants serveur avec un stéréotype du service Web pour la réalisation de cette génération.⁷ Tout composant serveur avec un stéréotype de service Web sera traité comme s'il disposait également d'un stéréotype d'Enterprise JavaBeans. Ceci est dû au fait que les interfaces de services Web correspondent à des encapsuleurs sur des BPO accessibles au public.

Contenu du fichier EAR de services Web

Le fichier EAR généré possède la structure et le contenu suivants :

- Répertoire META-INF
 - `application.xml`
Ce fichier détaille le module principal de l'application de services Web, qui correspond au fichier `webservices.war`.
 - `ibm-application-bnd.xmi`
Un fichier d'extension WAS spécifique généré.
 - `ibm-application-ext.xmi`
Un fichier d'extension WAS spécifique généré.

7. Consultez le manuel *Cúram Server Modelling Guide* pour plus d'informations sur l'affectation de BPO aux composants serveur.

- was.policy
Un fichier de règles de sécurité WAS accordant une autorisation Java `java.security.AllPermission` à l'application.
- MANIFEST.MF
Le fichier manifeste détaillant le contenu du fichier EAR.

- **Fichier WAR de service Web**

Ce fichier contient les fichiers JAR de prise en charge dans le répertoire `WEB-INF/lib`, dont :

- `coreinf.jar`
Ce fichier JAR contient les méthodes de conversion utilisées pour la prise en charge de la sérialisation des types complexes utilisés dans l'interface.
- `axis.jar`
Ce fichier JAR contient le moteur de services Web Axis.
- `appwebservices.jar`
Ce fichier JAR contient les classes d'encapsuleurs autorisant les services Web Axis à se connecter aux beans session d'application serveur IBM Cúram Social Program Management ainsi que les classes des types complexes utilisées dans l'interface des services Web.
- `server-config.wsdd`
Ce fichier wsdd est situé dans le répertoire `WEB-INF` et contient la configuration du moteur de service Web permettant de mapper les objets de processus métier IBM Cúram Social Program Management aux services Web.

WSDL de service Web

Un service Web IBM Cúram Social Program Management expose son propre langage WSDL une fois qu'il est déployé.

Par exemple, s'il existe un service à l'adresse :

`http://localhost:9082/CuramWS/services/MyTestService`

la description du langage WSDL est disponible à l'adresse :

`http://localhost:9082/CuramWS/services/MyTestService?wsdl`

L'adresse URL :

`http://localhost:9082/CuramWS/services`

renvoie une page Web répertoriant tous les services Web déployés ainsi qu'un lien vers leurs fichiers WSDL.

Le format général de l'adresse URL des emplacements ci-dessus est le suivant :

`http://<serveur-web>:<numéro-port>/<NomModèleServeur>WS/services/<nom-objet-processus-métier>.`

Fichiers EAR multiples

La génération d'un fichier EAR d'application nécessite également un fichier facultatif afin d'autoriser la répartition des composants client dans différents fichiers WAR et EAR ainsi que davantage de contrôle de certains modules inclus et

de configuration EAR. Ce fichier est appelé `deployment_packaging.xml` et doit être placé dans votre répertoire `REP_SERVEUR/project/config`.

Le format du fichier `deployment_packaging.xml` est le suivant :

```
<deployment-config>
  <ear name="Curam"
    requireServer="true">
    <components>custom,sample,SamplePublicAccess,core</components>
    <context-root>/Curam</context-root>
  </ear>
  <ear name="CuramExternal">
    <components>SamplePublicAccessExternal</components>
    <context-root>/CuramExternal</context-root>
    <custom-web-xml>${client.dir}/custom_web_xml</custom-web-xml>
  </ear>
</deployment-config>
```

Figure 1. Exemple de fichier `deployment_packaging.xml`

Chaque fichier peut avoir plusieurs éléments `ear` et entraîne la génération d'un fichier EAR dans le répertoire `REP_SERVEUR/build/ear/WAS`. Les options de chaque élément sont les suivantes :

- `name`
Cette option contrôle le nom du fichier d'archive d'entreprise créé à partir du processus.
- `requireServer`
Cet attribut facultatif contrôle l'inclusion ou non du module de serveur dans le fichier EAR. Les entrées valides sont `true` ou `false`. La valeur par défaut est `false`. Si le déploiement de plusieurs fichiers EAR est effectué vers un seul serveur d'applications, cet attribut doit être défini sur `true` pour un seul fichier EAR dans la mesure où un seul module de serveur IBM Cúram Social Program Management doit être déployé par cluster. Si `requireServer` est défini sur `true` pour plusieurs fichiers EAR, alors les autres fichiers EAR doivent être déployés dans un autre cluster afin d'éviter les conflits.
- `components`
Cette option permet de déterminer les composants client placés dans le fichier EAR. Elle contrôle également l'ordre des composants pour la régénération du client devant être effectuée. En général, le répertoire principal ne fait pas partie de l'ordre des composants, cependant, il est important dans ce cas de l'ajouter afin d'indiquer s'il doit être inclus dans un fichier WAR spécifique. Les entrées doivent suivre l'ordre classique des composants défini dans le manuel *Cúram Server - Guide de développement* et doivent être séparées par des virgules.
- `context-root`
Cette option forme la racine de contexte du module WAR dans le descripteur de déploiement `application.xml`. Les entrées doivent commencer par une barre oblique.
- `custom-web-xml`
Cet élément facultatif indique si un fichier `web.xml` personnalisé doit remplacer la version standard dans le fichier WAR. Les entrées doivent correspondre à un chemin Apache Ant vers le répertoire contenant le fichier `web.xml`.
Il est possible d'utiliser des références aux variables d'environnement dans le cadre de ce chemin d'accès. Par exemple, `${client.dir}` peut être utilisé pour pointer vers le répertoire du client Web et `${SERVER_DIR}` peut être utilisé pour pointer vers le répertoire du serveur.

- requireSearchServer
Voir *Cúram Generic Search Server* pour plus d'informations.

Pour chaque client Web (fichier WAR) un composant de client Web distinct est requis pour contenir ses personnalisations. Dans le cas de clients Web multiples, votre variable d'environnement CLIENT_COMPONENT_ORDER inclut tous vos composants personnalisés ; toutefois, des éléments <ear> distincts sont requis, un pour chaque composant Web personnalisé (et d'autres composants, si nécessaire).

Comme pour la cible standard, une application IBM Cúram Social Program Management entièrement générée doit être disponible. Pour plus d'informations sur la génération d'une application, veuillez consulter le manuel *Cúram Server - Guide de développement*.

Cibles alternatives

La cible **websphereEAR** permet de générer un fichier .ear d'application IBM Cúram Social Program Management contenant l'application et le client Web. Une prise en charge est fournie pour générer un fichier .ear d'application contenant uniquement l'application Web ou l'application serveur.

Ces cibles peuvent s'avérer nécessaires lorsque le client Web et l'application serveur doivent être installés sur des serveurs distincts. Par exemple, afin de garantir la prise en charge d'un accès sécurisé à l'application Cúram application pour les utilisateurs externes, une nouvelle application de client Web peut être développée. Cette application Web peut être déployée seule et utiliser une application serveur existante.⁸

Pour générer un fichier ear contenant uniquement l'application de client Web, la commande suivant doit être utilisée :

```
build websphereEAR -Dclient.only=true
```

Pour générer un fichier .ear contenant uniquement l'application serveur, la commande suivante doit être utilisée :

```
build websphereEAR -Dserver.only=true
```

Configuration du serveur d'application

Introduction

Ce chapitre suppose que WebSphere a déjà été installé. Consultez le manuel *Cúram Third Party Tools Installation Guide*⁹ pour plus d'informations sur l'installation.

La configuration de WebSphere Application Server est similaire pour toutes les plateformes et Server Development Environment for Java (SDEJ) fournit plusieurs cibles Ant pour vous aider lors de la configuration et la gestion de l'installation. Si vous êtes intéressé, la rubrique «Configuration manuelle de WebSphere Application Server», à la page 18 fournit des détails sur les étapes effectuées par les scripts de configuration.

8. Pour plus d'informations sur la sécurité de l'accès externe consultez le manuel *Cúram Server - Guide de développement*.

9. Reportez-vous au manuel d'installation correspondant à votre plateforme (Windows ou UNIX).

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

Remarque : La cible **configure** remplace le profil *par défaut* créé par WebSphere Application Server sauf si `-Dkeep.profile=true` est transmis à la cible.

Configuration de WebSphere Application Server

La configuration de WebSphere Application Server inclut la définition d'un profil, d'une source de données, d'un nombre de serveurs, ainsi que la configuration de paramètres de sécurité et JMS. Toutes ces tâches peuvent être effectuées via l'exécution de la cible **configure** fournie par SDEJ.

Le profil créé par la cible **configure** prend les valeurs par défaut suivantes, sauf si elles ont été explicitement remplacées lors de l'appel de la cible.

- `profile.name=AppSvr01`
- `cell.name=${node.name}Cell`

La commande **build configure** doit être exécutée à partir du répertoire `<SERVER_DIR>` pour appeler une configuration automatique. Cette cible nécessite que les fichiers `AppServer.properties` et `Bootstrap.properties` soient présents dans le répertoire `<SERVER_DIR>/project/properties`¹⁰. Consultez le manuel *Cúram Server - Guide de développement* pour plus d'informations sur la configuration de `Bootstrap.properties`. «Configuration de WebSphere Application Server» présente un exemple de contenu du fichier `AppServer.properties`.

10. Il est possible de remplacer cet emplacement par défaut pour les fichiers 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 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 FOLLOWING PROPERTIES ARE FOR WebSphere ONLY ##
#####
# The alias that should be used for the database authorization
curam.db.auth.alias=databaseAlias

# 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 2. Exemple de propriétés AppServer

Par défaut, la cible **configure** établit une source de données Type 4 Universal Driver (XA). Toutefois, vous pouvez configurer une source de données Type 2 Universal Driver (XA) en définissant la propriété `curam.db.type2.required` du fichier `AppServer.properties`.

Par défaut, la cible **configure** définit la taille de segment de mémoire initiale et maximale de 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`.

Remarque :

1. La configuration du segment de mémoire Java décrite dans l'exemple «Configuration de WebSphere Application Server», à la page 8 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 ont été détectés avec les pilotes de base de données encapsulés WebSphere Application Server lors de la récupération d'objets CLOB et BLOB (3MB+) importants depuis 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.

3. La cible **configure** ne peut pas être exécutée lorsqu'une base de données H2 est en cours d'utilisation.¹¹

Configuration des paramètres de sécurité

La configuration des paramètres de sécurité par défaut d'IBM Cúram Social Program Management dans WebSphere Application Server 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. 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 `true`. Cela permet de s'assurer que le mécanisme d'authentification alternatif configuré est utilisé.

Consultez la rubrique *Authentification par identité uniquement* du *Manuel de sécurité Cúram* pour plus d'informations détaillées.

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

Lors de l'utilisation de l'identité uniquement avec WebSphere Application Server 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 ou la cible `configure`. En utilisant cette combinaison, il se peut que le démarrage de WebSphere Application Server échoue, car il est nécessaire d'ajouter un nom d'utilisateur généré par WebSphere Application Server à la propriété de la liste d'exclusion du module de connexion (`exclude_usernames`) décrite dans «Ajout du module de connexion», à la page 28. Dans ce cas d'échec de démarrage de WebSphere Application Server, un message d'erreur SECJ0270E apparaît dans le fichier `SystemOut.log` avant l'échec.

Procédez comme suit pour résoudre cette erreur :

1. Identifiez le nom d'utilisateur à l'origine de l'échec de démarrage de WebSphere Application Server. Configurez le suivi du module de connexion comme indiqué dans «Journalisation du processus d'authentification», à la page 12 (concernant la cible `configure`) ou «Ajout du module de connexion», à la page 28 (concernant la configuration via la console d'administration), puis redémarrez WebSphere Application Server. 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 :

11. Pour plus d'information sur la base de données H2, consultez le manuel *Cúram Third-Party Tools - Guide d'installation pour Windows*.

SystemOut 0 Username: server:MyNodeCell_MyNode_CuramServer

Où "MyNode" correspond au nom de noeud, "MyNodeCell" au nom de cible et "CuramServer" au nom du serveur WebSphere. 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 WebSphere Application Server. Dans la mesure où le démarrage de WebSphere Application Server 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 directement. dans le système de fichiers de configuration de WebSphere Application Server 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 `exclude_usernames`, l'attribut d'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.

Registre d'utilisateurs WebSphere Application Server

Par défaut, le registre d'utilisateurs WebSphere Application Server configuré n'est pas interrogé 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 `true` le registre d'utilisateurs WebSphere Application Server est interrogé lors du processus d'authentification, que l'authentification par identité uniquement soit activée ou non. Si cette propriété est définie sur `false`, le registre d'utilisateurs WebSphere Application Server n'est pas interrogé. Par exemple, si `curam.security.check.identity.only` est défini sur `true` et que `curam.security.user.registry.enabled` est défini sur `false`, ni les vérifications d'authentification IBM Cúram Social Program Management ni le registre d'utilisateurs WebSphere Application Server 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 via l'utilisation des propriétés `curam.security.user.registry.enabled.types` et/ou `curam.security.user.registry.disabled.types`. Ces propriétés spécifient une liste séparée par des virgules des types d'utilisateurs externes qui seront ou non authentifiés via le registre d'utilisateurs WebSphere Application Server :

- Les types d'utilisateurs spécifiés dans la liste `curam.security.user.registry.enabled.types` seront traités dans le registre d'utilisateurs WebSphere Application Server (LDAP) et votre implémentation `ExternalAccessSecurity`.
- Les types d'utilisateurs spécifiés dans la liste `curam.security.user.registry.disabled.types` ne seront pas traités dans le registre d'utilisateurs WebSphere Application Server 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 est le suivant :

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

Voir «Configuration du module de connexion JAAS du système», à la page 28 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 `true` cette propriété entraîne le suivi des informations ajoutées au fichier `SystemOut.log` de WebSphere Application Server 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 met en cache des données d'identification et informations concernant l'utilisateur dans un cache de sécurité et le module de connexion 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 `true`, que le jeton contient une clé de mémoire cache personnalisée et que le sujet personnalisé est introuvable, le jeton est utilisé pour se connecter directement car 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 `false` et que le sujet personnalisé est introuvable, l'authentification LTPA Token2 est utilisée pour se connecter et regrouper tous 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, `com.ibm.ws.security.webChallengeIfCustomSubjectNotFound`, sur `false` pour s'assurer que les sessions Web peuvent sans problème effectuer des transferts entre deux serveurs d'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, 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 28 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 26.

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 instantanément utilisables. Vous pouvez, si vous acceptez un niveau de sécurité moindre, choisir, à vos propres risques, d'effectuer les procédures permettant de conserver les mots de passe système et utilisateur existants en l'état, mais cela est déconseillé. Pour plus d'informations sur la mise à niveau, consultez le guide *Cúram Upgrade Guide*.

Configuration du fuseau horaire

Si plusieurs serveurs sont utilisés, leur horloge doit 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. 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 8). Elles nécessitent également la définition de plusieurs paramètres supplémentaires, détaillés ci-après.

Démarrage d'un serveur WebSphere

La cible pour le démarrage d'un serveur WebSphere 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 startserver -Dserver.name=CuramServer
```

Figure 3. Exemple d'utilisation

Arrêt d'un serveur WebSphere

La cible pour l'arrêt d'un serveur WebSphere est **stopserver** et nécessite les options suivantes :

- `-Dserver.name`

Le nom du serveur à arrêter.

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

Figure 4. Exemple d'utilisation

Redémarrage d'un serveur WebSphere

La cible pour le redémarrage d'un serveur WebSphere est **restartserver** et les options sont les mêmes que pour la cible **startserver**. Voir «Démarrage d'un serveur WebSphere», à la page 14 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 consiste à les déployer sur le serveur d'application.

Avant d'effectuer le déploiement, il est important de noter que dans WebSphere Application Server, les scripts de configuration fournis prennent en charge une configuration simple orientée vers le serveur unique dans les éditions Express ou de base de WebSphere Application Server.

Déploiement

SDEJ fournit des cibles pour l'installation et la désinstallation d'applications sur une serveur WebSphere. Pour avec les cibles **startserver** / **stopserver**, les cibles **installapp** / **uninstallapp** demandent à ce que le fichier `AppServer.properties` soit correctement configuré (voir «Configuration de WebSphere Application Server», à la page 8). 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 sur lequel installer l'application.

- `-Dear.file`

Nom qualifié complet du fichier EAR à installer.

- `-Dapplication.name`

Nom de l'application

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

Figure 5. Exemple d'utilisation

Remarque : Le fichier EAR contenant le module de serveur doit être déployé avant l'installation 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"
```

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 prolix : `-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. Accédez à **Applications > Application Types (Types d'applications) > WebSphere enterprise applications (Applications d'entreprise WebSphere enterprise)**, puis sélectionnez l'application IBM Cúram Social Program Management. 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 26.

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 uninstallapp -Dserver.name=CuramServer  
-Dapplication.name=Curam
```

Figure 6. Exemple d'utilisation

Pré-compilation de JavaServer Pages

Une cible supplémentaire est disponible lors du déploiement, **precompilejsp**, et permet de pré-compiler les JavaServer Pages d'un fichier d'archive d'entreprise client *avant* l'installation du fichier EAR. La pré-compilation des JavaServer Pages avant l'installation accélère l'affichage d'une page spécifique dans le navigateur lorsqu'elle est visualisée pour la première fois.

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

- `-Dear.file`
Le nom qualifié complet du fichier EAR à pré-compiler.

```
build precompilejsp -Dear.file=d:/Curam.ear
```

Figure 7. Exemple d'utilisation

Remarque : Lors de l'exécution de la cible **precompilejsp** pour WebSphere Application Server, une exception de mémoire peut se produire (ou des JavaServer Pages peuvent être ignorés de manière silencieuse et ne pas être pré-compilés). Pour contourner ce problème, le script `JspBatchCompiler.bat` 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`.

Test du déploiement

Une fois l'application installée¹² sur une installation WebSphere Application Server configurée, la prochaine étape consiste à démarrer et tester l'application.

Vérifiez que le serveur approprié a été démarré¹³ 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 serveur WebSphere Application Server est en cours d'exécution, `<port>` identifie le port du

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

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

serveur sur lequel l'application client est déployée et *<racine-contexte>* identifie la racine de contexte du module WAR (voir «Fichiers EAR multiples», à la page 5, pour plus d'informations).

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. 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

Les rubriques de ce chapitre couvrent les étapes manuelles requises pour la configuration et le déploiement sur les éditions de base ou Express de WebSphere Application Server. Il convient d'adapter ces étapes de manière appropriée pour effectuer un déploiement dans une installation de déploiement réseau de WebSphere Application Server. Voir «Déploiement réseau WebSphere», à la page 42 pour plus d'informations.

Configuration manuelle de WebSphere Application Server

L'installation IBM WebSphere Application Server peut être configurée manuellement si nécessaire, cependant ce type de configuration n'est pas recommandé. Cette rubrique détaille les étapes requises pour la configuration de WebSphere Application Server à titre indicatif uniquement.

Il convient de noter que les paramètres saisis sous la section **Ressources** de la console d'administration WebSphere Application Server 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 est effectuée à l'aide de la console d'administration. Pour exécuter la console d'administration, le serveur par défaut, par exemple, server1, doit être démarré alors que la console d'administration est installée en tant qu'application Web sur ce serveur.

Pour démarrer server1, le fichier startServer.bat, situé dans le répertoire profiles/AppSvr01/bin de l'installation de WebSphere Application Server, doit être utilisé :

```
<WEBSHERE INSTALL DIR>/profiles/AppSvr01/bin/startServer server1
```

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

```
http://localhost:9060/ibm/console"/>
```

Sinon, il est possible de démarrer la console d'administration depuis **Start (Démarrer) > Programs (Programmes) > IBM WebSphere > Application Server V7.0 > Profiles (Profils) > AppSvr01 > Administrative console (Console d'administration)**. Les commandes **Start the server (Démarrer le serveur)** et **Stop the server (Arrêter le serveur)** peuvent également être utilisées à partir de ce menu pour démarrer et arrêter les serveurs.

Lors de la première ouverture de la console d'administration, un nom d'utilisateur est demandé pour se connecter. Vous pouvez choisir n'importe quel nom d'utilisateur ! La console d'administration est divisée en deux parties. Le côté gauche contient une arborescence permettant de naviguer dans la console et le côté droit affiche les informations relatives au noeud actuellement sélectionné dans l'arborescence. Lorsque l'option Navigate to (Accéder à) est définie, l'arborescence doit être parcourue pour accéder au noeud approprié.

Prise en charge du scriptage

Afin de prendre en charge l'exécution des scripts Ant fournis, il est nécessaire de modifier les fichiers de propriétés WebSphere Application Server.

sas.client.props : Ouvrez le fichier sas.client.props situé dans le répertoire profiles/AppSvr01/properties de l'installation WebSphere Application Server. 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 situé dans le répertoire profiles/AppSvr01/properties de l'installation WebSphere Application

Server. 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 configurées pour WebSphere conformément à la section «Configuration de WebSphere Application Server», à la page 8. 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 les délais d'attente lors de l'installation des fichiers EAR, vérifiez que l'élément suivant est au minimum défini sur :

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

server.policy : Ouvrez le fichier `server.policy` situé dans le répertoire `profiles/AppSvr01/properties` de l'installation WebSphere Application Server. 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/<nom.profil>/installedApps/
<nom.cible>/<NOM_MODELE_SERVEUR>.ear/
guice-2.0.jar" { permission java.lang.RuntimePermission
"modifyThread"; permission java.lang.RuntimePermission
"modifyThreadGroup"; };
```

où `<nom.profil>` correspond au nom du profil WebSphere Application Server cible ;

où `<nom.cible>` correspond au nom de la cellule WebSphere Application Server cible ;

où `<NOM_MODELE_SERVEUR>` correspond au nom de l'application (nom de base du fichier EAR).

Création de l'alias de connexion à la source de données Pourquoi et quand exécuter cette tâche

Les bases de données prises en charge sont IBM DB2, IBM DB2 for z/OS et Oracle Database. La console d'administration peut être utilisée pour configurer un alias de connexion pour les sources de données DB2 et Oracle. Pour ce faire, procédez comme suit.

Procédure

1. Accédez à **Sécurité > Sécurité globale** ;
2. Développez l'option **Service JAAS** dans la section **Authentification** et sélectionnez l'option **J2C authentication data (Données d'authentification J2C)** ;

3. Cliquez sur **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. Cliquez sur **OK** pour confirmer les modifications.

Configuration de sources de données DB2

Configuration de la variable d'environnement DB2 :

Procédure

1. Accédez à **Environnement > WebSphere variables (Variables WebSphere)** ;
2. 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 ;
3. Définissez la zone **Valeur** pour pointer vers le répertoire contenant les pilotes de Type 4/Type 2. Il s'agit du répertoire **drivers** situé sous l'installation **SDEJ**, par exemple : **D:\Curam\CuramSDEJ\drivers** ;
4. Cliquez sur **OK** pour confirmer les modifications.

Configuration du fournisseur de pilote de base de données :

Procédure

1. Accédez à **Ressources > JDBC > JDBC providers (Fournisseurs JDBC)** ;
2. *Remarque* : la plage appropriée dans laquelle vous devez définir la source de données doit être sélectionnée à ce moment-là.
3. Cliquez sur **Nouveau** pour ajouter un pilote. Un écran de configuration s'affiche ;
4. Sélectionnez **DB2** dans la liste du menu déroulant **Type de base de données** ;
5. Sélectionnez **DB2 Universal JDBC Driver Provider (Fournisseur de pilote DB2 Universal JDBC)** dans la liste du menu déroulant **Provider type (Type de fournisseur)** ;
6. Sélectionnez **Source de données XA** dans la liste du menu déroulant **Type d'implémentation** ;
7. Cliquez sur **Suivant** pour continuer ;
8. Examinez les propriétés de l'écran de configuration qui s'affiche. Il n'est pas nécessaire de les modifier, sauf si vous prévoyez de vous connecter à une base de données **zOS**. Si tel est le cas, vérifiez que la zone `{DB2UNIVERSAL_JDBC_DRIVER_PATH}` pointe vers le répertoire approprié de votre système. Par exemple, celle-ci devrait pointer vers le répertoire contenant le fichier jar de licence **DB2 Connect**, `db2jcc_license_cisuz.jar` fourni par IBM pour la connectivité **zOS** ;
9. Cliquez sur **Suivant** puis **Terminer** pour confirmer les modifications.

Configuration de la source de données du pilote de base de données :

Pourquoi et quand exécuter cette tâche

Les étapes suivantes doivent être répétées pour chaque source de données, en remplaçant `curamdb`, `curamsbdb` et `curamtimerdb` pour le `<Nom_source_de_données>` (sans les chevrons) :

Procédure

1. Sélectionnez le DB2 Universal JDBC Driver Provider (XA) (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 **Additional Properties (Propriétés supplémentaires)** ;
3. Cliquez sur **Nouveau** pour ajouter une 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 :
Driver type (Type de pilote) : 2 ou 4, selon les besoins ;
Nom de base de données : Nom de la base de données DB2 ;
Nom de serveur : Nom du serveur de base de données DB2 ;
Numéro de port : Port du serveur de base de données DB2 ;
Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;
7. Définissez la valeur **Component-managed authentication alias (Alias d'authentification géré par des composants)** sur : `<valide pour la base de données>` ;
Définissez la valeur **Mapping-configuration alias (Alias de mappage-configuration)** sur : `DefaultPrincipalMapping` ;
Définissez la valeur **Container-managed authentication alias (Alias d'authentification géré par des conteneurs)** 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 20 ;
Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** pour continuer.
8. Cliquez sur **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 **Custom Properties (Propriétés personnalisées)** situé sous **Additional Properties (Propriétés supplémentaires)** ;
11. Sélectionnez l'entrée `fullyMaterializeLobData` ;
12. Définissez la valeur sur `false` ;
13. Cliquez sur **OK** pour confirmer les modifications.

Configuration d'une source de données Oracle

Configuration de la variable d'environnement Oracle :

Procédure

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

2. Sélectionnez le lien ORACLE_JDBC_DRIVER_PATH dans la liste des variables d'environnement. Cela permet d'afficher l'écran de configuration de cette variable ;
3. Définissez la zone **Valeur** de manière à pointer vers le répertoire contenant le pilote de type 4. Il s'agit du répertoire drivers de l'installation SDEJ :
D:\Curam\CuramSDEJ\drivers ;
4. Cliquez sur **OK** pour confirmer les modifications.

Configuration du pilote de base de données XA :

Procédure

1. Accédez à **Ressources > JDBC > JDBC providers (Fournisseurs JDBC)** ;
2. *Remarque* : la plage appropriée dans laquelle vous devez définir la source de données doit être sélectionnée à ce moment-là.
3. Cliquez sur **Nouveau** pour ajouter un pilote. Un écran de configuration s'affiche ;
4. Sélectionnez **Oracle** dans la liste du menu déroulant **Type de base de données** fourni ;
5. Sélectionnez **Oracle JDBC Driver (Pilote JDBC Oracle)** dans la liste du menu déroulant **Provider type (Type de fournisseur)** fourni ;
6. Sélectionnez **Source de données XA** dans la liste du menu déroulant **Type d'implémentation** ;
7. Définissez la zone **Nom** sur Oracle JDBC Driver (XA) (Pilote JDBC Oracle [XA]), si celle-ci n'est pas renseignée automatiquement ;
8. Cliquez sur **Suivant** pour continuer ;
9. Examinez le **Chemin d'accès aux classes** et vérifiez que la variable d'environnement ORACLE_JDBC_DRIVER_PATH est correcte. Cliquez sur **Suivant** pour continuer ;
10. Examinez les propriétés de l'écran de configuration qui s'affiche. Il n'est pas nécessaire de les modifier ;
11. Cliquez sur **Terminer** pour confirmer les modifications.

Configuration du pilote de base de données Non-XA :

Procédure

1. Accédez à **Ressources > JDBC > JDBC providers (Fournisseurs JDBC)** ;
2. Cliquez sur **Nouveau** pour ajouter un pilote. Un écran de configuration s'affiche ;
3. Sélectionnez **Oracle** dans la liste du menu déroulant **Type de base de données** ;
4. Sélectionnez **Oracle JDBC Driver (Pilote JDBC Oracle)** dans la liste du menu déroulant **Provider type (Type de fournisseur)** fourni ;
5. Sélectionnez **Connection pool data source (Source de données du pool de connexions)** dans la liste du menu déroulant **Type d'implémentation** ;
6. Définissez la zone **Nom** sur Oracle JDBC Driver (Pilote JDBC Oracle), si celle-ci n'est pas renseignée automatiquement ;
7. Cliquez sur **Suivant** pour continuer ;
8. Examinez le **Chemin d'accès aux classes** et vérifiez que la variable d'environnement ORACLE_JDBC_DRIVER_PATH est correcte. Cliquez sur **Suivant** pour continuer ;
9. Examinez les propriétés de l'écran de configuration qui s'affiche. Il n'est pas nécessaire de les modifier ;

10. Cliquez sur **Terminer** pour confirmer les modifications.

Configuration des sources de données du pilote de base de données XA : Pourquoi et quand exécuter cette tâche

Les étapes suivantes doivent être répétées deux fois, en remplaçant *<nom_source_de_données>* (sans les chevrons) par *curamdb* et puis *curamsibdb*.

Procédure

1. Sélectionnez l'élément **Oracle JDBC Driver (XA) (Pilote JDBC Oracle [XA])** qui s'affiche dans la liste des fournisseurs existants. L'écran de configuration s'affiche à nouveau ;
2. Sélectionnez le lien **Sources de données** situé sous **Additional Properties (Propriétés supplémentaires)** ;
3. Cliquez sur **Nouveau** pour ajouter une 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 la zone de valeur **URL** sur :

jdbc:oracle:thin:@//nom_serveur:port/nom_service_base_de_données, pour vous connecter à une base de données à l'aide du nom de service Oracle.

ou

jdbc:oracle:thin:@nom_serveur:port:nom_base_de_données, pour vous connecter à une base de données à l'aide du nom de SID Oracle.

où :

nom_serveur correspond au nom du serveur hébergeant la base de données ;

port correspond au numéro de port sur lequel la base de données est en mode écoute ;

nom_base_de_données correspond au SID de la base de données ; et

nom_service_base_de_données correspond au nom de service de la base de données.

Définissez **Data store helper class name (Nom de classe auxiliaire du magasin de données)** sur Oracle 11g data store helper (Auxiliaire de magasin de données Oracle 11g) ;

Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;

Remarque : Oracle vous recommande d'utiliser le format d'URL

jdbc:oracle:thin:@//nom_serveur:port/nom_service_base_de_données pour vous connecter à la base de données Oracle à l'aide du nom de service.

Cependant ce format d'URL ('/' supplémentaire avant '@' dans l'URL) n'est pas pris en charge par la console d'administration WebSphere Application Server.

Ainsi, l'URL du nom de service Oracle décrite ci-dessus (sans '/'

supplémentaire avant '@' dans l'URL) doit être utilisée lors de la configuration d'une source de données Oracle depuis la console d'administration, pour vous connecter à une base de données Oracle à l'aide du nom de service.

6. Définissez **Authentication alias for XA recovery (Alias d'authentification pour la récupération XA)** : *<valide pour la base de données>*

Définissez la valeur **Component-managed authentication alias (Alias d'authentification géré par des composants)** 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 20 ;

Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;

7. Cliquez sur **Terminer** pour confirmer les modifications et continuer.

Configuration de la source de données du pilote de base de données Non-XA : Procédure

1. Sélectionnez **Pilote JDBC Oracle** s'affichent maintenant sur la liste des fournisseurs existants. L'écran de configuration s'affiche à nouveau ;
2. Sélectionnez le lien **Sources de données** situé sous **Additional Properties (Propriétés supplémentaires)** ;

3. Cliquez sur **Nouveau** pour ajouter une source de données ;

4. Définissez les zones comme suit :

Nom de source de données : curamtimerdb

Nom JNDI : jdbc/curamtimerdb

Cliquez sur **Suivant** ;

5. Définissez la zone de valeur **URL** sur :

jdbc:oracle:thin:@//nom_serveur:port/nom_service_base_de_données, pour vous connecter à une base de données à l'aide du nom de service Oracle.

ou

jdbc:oracle:thin:@nom_serveur:port:nom_base_de_données, pour vous connecter à une base de données à l'aide du nom de SID Oracle.

où :

nom_serveur correspond au nom du serveur hébergeant la base de données.

port correspond au numéro de port sur lequel la base de données est en mode écoute.

nom_base_de_données correspond au SID de la base de données.

nom_service_base_de_données correspond au nom de service de la base de données.

Définissez **Data store helper class name (Nom de classe auxiliaire du magasin de données)** sur Oracle 11g data store helper (Auxiliaire de magasin de données Oracle 11g) ;

Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;

Remarque : Oracle vous recommande d'utiliser le format d'**URL**

jdbc:oracle:thin:@//nom_serveur:port/nom_service_base_de_données pour vous connecter à une base de données Oracle à l'aide du nom de service.

Cependant ce format d'**URL** ('/' supplémentaire avant '@' dans l'**URL**) n'est pas pris en charge par la console d'administration WebSphere. Ainsi, l'**URL** du nom de service Oracle décrite ci-dessus (sans '/' supplémentaire avant '@' dans l'**URL**) doit être utilisée lors de la configuration d'une source de données Oracle depuis la console d'administration, pour vous connecter à une base de données Oracle à l'aide du nom de service.

6. Définissez la valeur **Component-managed authentication alias (Alias d'authentification géré par des composants)** 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 20 ;

Ne modifiez pas les autres zones, sauf en cas de modification spécifique requis, et cliquez sur **Suivant** ;

7. Cliquez sur **Terminer** pour confirmer les modifications et continuer.

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'utilisateur basé sur des fichiers WebSphere Application Server 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 **OK** ;
6. Entrez le mot de passe de l'administrateur par défaut, par exemple websphere, entrez la confirmation et cliquez sur **OK** pour confirmer les modifications ;
7. Définissez **Définitions de superdomaines disponibles** sur **Référentiels fédérés** et cliquez sur le bouton **Définir comme actif** ;
8. Sélectionnez **Activer la sécurité administrative** ;
9. Sélectionnez **Activer la sécurité des applications** ;
10. 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** ;
11. Cliquez sur le bouton **Appliquer** pour confirmer les modifications ;
12. Définissez **Définitions de superdomaines disponibles** sur **Référentiels fédérés** ;
13. Cliquez sur le bouton **Appliquer** pour confirmer les modifications ;
14. Accédez à **Sécurité > Sécurité globale** ;
15. Développez **Sécurité SIP et Web** et sélectionnez **Connexion unique** ;
16. Sélectionnez **Requiert SSL** ;
17. Cliquez sur **OK** pour confirmer la modification
18. Accédez à **Sécurité > Sécurité globale**
19. Sélectionnez le lien **Propriétés personnalisées** ;
20. Cliquez sur le bouton **Nouveau** puis définissez le nom et la valeur comme suit :
Nom : com.ibm.ws.security.web.logoutOnHTTPSessionExpire
Valeur : true
21. Cliquez sur le bouton **OK** pour ajouter la nouvelle propriété.

22. Cliquez sur le bouton **Nouveau** puis définissez le nom et la valeur comme suit :
Nom : `com.ibm.ws.security.addHttpOnlyAttributeToCookies`
Valeur : `true`
23. Cliquez sur **OK** pour confirmer la modification
24. Enregistrez les modifications apportées à la configuration principale.

Redémarrage du serveur d'application

Cette étape est obligatoire. Le serveur doit être redémarré pour appliquer les changements de sécurité et ajouter des utilisateurs obligatoires supplémentaires. Le serveur peut être arrêté à l'aide du fichier `stopServer.bat` du répertoire `profiles/AppSrv01/bin` de l'installation WebSphere Application Server. Cette opération est similaire à l'opération de démarrage du serveur décrite dans la rubrique «Introduction», à la page 18.

Avant de redémarrer le serveur d'applications (server1), il est nécessaire de rendre les fichiers JAR de registre et de cryptographie accessibles à WebSphere Application Server. 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.

Le fichier `Registry.jar` se trouve dans le répertoire `lib` de l'installation SDEJ. Copiez ce fichier dans le répertoire `lib` de l'installation WebSphere Application Server.

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 *Curam Security Handbook*.

Démarrez à présent le serveur d'applications (server1) et ouvrez la console d'administration afin de poursuivre la configuration. Une fois la configuration des paramètres de sécurité terminée et les changements effectués au niveau du scriptage, il est désormais possible d'utiliser les scripts SDEJ pour redémarrer WebSphere Application Server. Voir «Démarrage et arrêt de serveurs WebSphere», à la page 14 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 et du mot de passe définis précédemment.

Configuration des utilisateurs **Pourquoi et quand exécuter cette tâche**

Comme indiqué dans la rubrique «Configuration des paramètres de sécurité», à la page 10, le registre d'utilisateurs WebSphere Application Server configuré est utilisé pour l'authentification des administrateurs et des utilisateurs de base de données. Les administrateurs et les utilisateurs de base de données WebSphere doivent être ajoutés manuellement au registre d'utilisateurs en procédant comme suit.

Procédure

1. Accédez à **Utilisateurs et groupes > Gérer les utilisateurs** ;
2. Cliquez sur le bouton **Créer** ;

3. Complétez les informations concernant l'administrateur WebSphere et cliquez sur le bouton **Créer**.
4. Répétez ces étapes pour l'utilisateur de base de données.

Résultats

Remarque : si la sécurité administrative WebSphere a été activée lors de la création du profil, il se peut que l'administrateur soit 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 :

Procédure

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 ;
4. Cliquez sur **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. Saisissez des paires Nom/Valeur dans la table **Propriétés personnalisées** pour les propriétés obligatoires répertoriées ci-après, en appuyant sur **Nouveau** lorsque nécessaire ;

Tableau 1. Propriétés personnalisées CuramLoginModule

Nom	Exemple de valeur	Description
exclude_usernames	websphere, db2admin	Obligatoire. Une liste de noms d'utilisateurs à exclure de l'authentification. Le délimiteur par défaut est une virgule, cependant celui-ci peut être remplacé par <code>exclude_usernames_delimiter</code> . Cette liste doit inclure l'administrateur WebSphere (comme spécifié dans «Configuration de la sécurité de l'administration», à la page 26) et l'utilisateur de base de données (comme spécifié dans «Création de l'alias de connexion à la source de données», à la page 20). Tous les utilisateurs répertoriés doivent être définis dans le registre d'utilisateurs WebSphere Application Server.
exclude_usernames_delimiter		<i>Facultatif</i> . Un délimiteur pour la liste des noms d'utilisateurs fourni dans <code>exclude_usernames</code> . 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	<i>Facultatif</i> . Cette propriété doit être définie sur <code>true</code> afin de déboguer le processus d'authentification. Si elle est définie sur <code>true</code> , l'appel du module de connexion entraîne le suivi des informations ajoutées au fichier <code>SystemOut.log</code> de WebSphere Application Server.

Tableau 1. Propriétés personnalisées CuramLoginModule (suite)

Nom	Exemple de valeur	Description
module_name	DEFAULT, WEB_INBOUND ou RMI_INBOUND	<i>Facultatif.</i> 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 le login_trace est défini sur true pour le suivi.
check_identity_only	true	<i>Facultatif.</i> Si cette propriété est définie sur true, le module de connexion n'effectue pas les 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 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. Remarque : Si vous définissez l'identité uniquement et que vous utilisez LDAP, des étapes de configuration supplémentaires peuvent être nécessaires ; consultez la rubrique «Étapes de configuration spécifiques lors de l'utilisation de l'identité uniquement et de LDAP», à la page 10.
user_registry_enabled	true	<i>Facultatif.</i> Cette propriété est utilisée pour remplacer le comportement qui consiste à ignorer le registre d'utilisateurs. Si cette propriété est définie sur true, le registre d'utilisateurs WebSphere Application Server est interrogé lors du processus d'authentification. Si cette propriété est définie sur false, le registre d'utilisateurs WebSphere Application Server n'est pas interrogé.
user_registry_enabled_types	EXTERNAL	<i>Facultatif.</i> Cette propriété est utilisée pour spécifier une liste séparée par des virgules des types d'utilisateurs externes traités dans le registre d'utilisateurs WebSphere Application Server (LDAP par exemple). Voir «Registre d'utilisateurs WebSphere Application Server», à la page 11 pour plus d'informations sur le traitement du registre d'utilisateurs WebSphere Application Server.
user_registry_disabled_types	EXTGEN,EXTAUTO	<i>Facultatif.</i> Cette propriété est utilisée pour spécifier une liste séparée par des virgules des types d'utilisateurs externes qui ne seront pas traités dans le registre d'utilisateurs WebSphere Application Server (LDAP par exemple). Voir «Registre d'utilisateurs WebSphere Application Server», à la page 11 pour plus d'informations sur le traitement du registre d'utilisateurs WebSphere Application Server.

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

Réorganisation du module de connexion :

Procédure

1. Accédez à **Sécurité > Sécurité globale** ;
2. Développez **Service JAAS** dans la section **Authentification** et sélectionnez **Connexions au 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 comme suit :
4. Cliquez sur le bouton **Définir l'ordre** ;
5. 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 ;
6. Cliquez sur **OK** pour confirmer les modifications apportées à l'ordre.

Désactivation de l'authentification entre les clusters : Pourquoi et quand exécuter cette tâche

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 `false` pour s'assurer que les sessions Web peuvent sans problème effectuer des transferts entre deux serveurs d'un cluster (par exemple, dans un scénario de basculement) sans que des données d'identification de sécurité ne soient nécessaires.

Procédure

1. Accédez à **Sécurité > Sécurité globale** ;
2. Cliquez sur **Custom properties (Propriétés personnalisées)** 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 **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 26.

Configuration de serveur

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, par exemple, `server1` ;
3. Développez **Ports** dans la section **Communications**, puis cliquez sur le bouton **Détails (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 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, par exemple, `server1` ;
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 la section **Server Infrastructure (Infrastructure du serveur)**, développez **Java and Process Management (Gestion de processus et Java)** ;
4. Sélectionnez le lien **Process definition (Définition de processus)** ;
5. Dans la section **Additional Properties (Propriétés supplémentaires)**, sélectionnez le lien **Java Virtual Machine (Machine virtuelle Java)** ;
6. Définissez les zones comme suit :
Initial heap size (Taille des segments de mémoire initiale) : 1024
Maximum heap size (Taille des segments de mémoire maximale) : 1024
Cliquez sur **Appliquer** pour définir les valeurs ;
7. Dans la section **Additional Properties (Propriétés supplémentaires)**, sélectionnez le lien **Custom Properties (Propriétés personnalisées)** ;
8. Cliquez sur **Nouveau** et définissez les propriétés comme suit :
Name (Nom) : com.ibm.websphere.security.util.authCacheCustomKeySupport
Value (Valeur) : false
Cliquez sur **OK** pour ajouter la propriété ;
9. *L'étape suivante est obligatoire sur les plateformes non-Windows uniquement.*
Cliquez sur **Nouveau** et définissez les propriétés comme suit :
Name (Nom) : java.awt.headless
Value (Valeur) : true
Cliquez sur **OK** pour ajouter la propriété ;
10. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Configuration de votre 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 la section **Paramètres de conteneur**, développez **Paramètres de conteneur EJB** ;
4. Sélectionnez le lien **Paramètres du service de temporisation EJB** ;
5. Dans le panneau **Type de planificateur**, sélectionnez l'option **Utiliser l'instance du planificateur du service de temporisation EJB interne**.
6. Définissez les zones comme suit :
Nom JNDI de la source de données : jdbc/curamtimerdb
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 20 ;
7. Cliquez sur **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 section **Communications** ;
4. Cliquez sur le bouton **détails** ;
5. Cliquez sur **Nouveau** et définissez les zones suivantes pour le port TCP/IP client :
User-defined Port Name (Nom de port défini par l'utilisateur) :
CuramClientEndPoint
Hôte : *
Port : 9044
Cliquez sur **OK** pour appliquer les modifications ;
6. Cliquez sur **Nouveau** et définissez les zones suivantes pour le port TCP/IP WebServices :
User-defined Port Name (Nom de port défini par l'utilisateur) :
CuramWebServicesEndPoint
Hôte : *
Port : 9082
Cliquez sur **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 **Nouveau** et définissez les zones suivantes pour la chaîne de transport client :
Nom : CuramClientChain
Transport Chain Template (Modèle de chaîne de transport) :
WebContainer-Secure
Cliquez sur **Suivant**
Use Existing Port (Utiliser le port existant) : CuramClientEndPoint
Cliquez sur **Suivant** et **Terminer**
12. Cliquez sur **Nouveau** et définissez les zones suivantes pour la chaîne de transport WebServices :
Nom : CuramWebServicesChain
Transport Chain Template (Modèle de chaîne de transport) : WebContainer
Cliquez sur **Suivant**
Use Existing Port (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 l'option **Use persistent keep alive connections (Utiliser des connexions persistantes)** est sélectionnée ;
16. Cliquez sur **OK** pour confirmer l'ajout ;

17. Accédez à **Environnement > Virtual hosts (Hôtes virtuels)** ;
18. Cliquez sur **Nouveau** pour ajouter une 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)** de la section **Additional Properties (Propriétés supplémentaires)** ;
 Cliquez sur **Nouveau** pour ajouter un nouvel Alias en définissant les zones suivantes ;
Nom d'hôte = *
Port = 9044
 où 9044 correspond au port utilisé lors de l'étape 5. Répétez cette étape pour les autres hôte virtuel et port utilisés (par exemple, hôte_webservices, 9082) ;
20. Cliquez sur **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 26.

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 **Nouveau** et dans l'**Etape 1**, 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)** (Étape 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 section **Topologie** ;
7. Cliquez sur **Ajouter** pour ouvrir l'assistant **Add a New Bus Member (Ajouter un nouveau membre de bus)** ;
8. Sélectionnez le serveur à ajouter au bus et cliquez sur **Suivant** ;
9. Sélectionnez **Magasin de données** et cliquez sur **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 26.

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 **Connection factories (Fabriques de connexions)** dans la section **Additional Properties (Propriétés supplémentaires)** ;
5. Cliquez sur **Nouveau** et définissez les zones suivantes :
 - Nom** : CuramQueueConnectionFactory
 - Nom JNDI** : jms/CuramQueueConnectionFactory
 - Description** : la fabrique pour 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 : <NOMSERVEUR> /dbadmin)
 - Alias de configuration de mappage** : DefaultPrincipialMapping
 - 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 **OK** pour appliquer les modifications ;
6. Cliquez sur **Nouveau** et définissez les zones suivantes :
 - Nom** : CuramTopicConnectionFactory
 - Nom JNDI** : jms/CuramTopicConnectionFactory
 - Description** : la fabrique pour 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 : <NOMSERVEUR> /dbadmin)
 - Alias de configuration de mappage** : DefaultPrincipialMapping
 - Alias d'authentification géré par conteneur** : identique à la source de données jdbc/curamdb (par exemple : <NOMSERVEUR> /dbadmin)

Laissez toutes les autres valeurs par défaut et cliquez sur **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 26.

Résultats

Remarque : En suivant les étapes de configuration ci-dessus, il n'est pas possible de configurer correctement les paramètres de sécurité pour la file d'attente et les fabrique 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 de configuration de WebSphere Application Server resources.xml. Ce fichier est situé dans l'arborescence du système de fichiers %WAS_HOME%\profiles\\config en fonction de vos conventions d'attribution de noms et de la page 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 WebSphere wsadmin. 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 ces étapes pour `CuramTopicConnectionFactory`.

- g. Redémarrez le serveur d'applications.

Configuration des files d'attente obligatoires :

Pourquoi et quand exécuter cette tâche

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 **Intégration de services > Bus > CuramBus** ;
2. Sélectionnez le lien **Destinations** dans la section **Ressources de la destination** ;
3. Cliquez sur **Nouveau** pour ouvrir l'assistant «Création d'une destination» ;
4. Sélectionnez le type de destination **File d'attente** 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 **Suivant** ;
6. Utilisez l'élément **Selected Bus Member (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 2. 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 **OK** pour appliquer les modifications.
11. Accédez à **Ressources > JMS > JMS providers (Fournisseurs JMS)** ;
12. Sélectionnez le lien **Fournisseur de messagerie par défaut** ;
13. Sélectionnez le lien **Files d'attente** dans la section **Propriétés supplémentaires** ;
14. Cliquez sur **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 **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 26.

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 section **Additional Properties (Propriétés supplémentaires)** ;
4. Cliquez sur **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) : permanent
Laissez toutes les autres valeurs par défaut et cliquez sur **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 26.

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 section **Additional Properties (Propriétés supplémentaires)** ;
4. Créez de nouvelles spécifications en cliquant sur **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 26.

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 **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 26.

Configuration des fichiers journaux d'historique

Il est possible de configurer le nombre maximum de fichiers journaux d'historique conservés par un serveur spécifique. Pour ce faire :

1. Accédez à **Serveurs > Types de serveurs > Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste des serveurs ;
3. Sélectionnez **Logging and Tracing (Journalisation et suivi)** dans la section **Troubleshooting (Traitement des incidents)** ;
4. Sélectionnez **JVM Logs (Journaux JVM)** dans la liste **General Properties (Propriétés générales)** ;
5. Définissez la zone **Maximum Number of Historical Log Files (Nombre maximum de fichiers journaux d'historique)** sur 30 pour les fichiers System.out et System.err ;
6. Cliquez sur **OK** pour appliquer les modifications ;
7. Enregistrez les modifications apportées à la configuration principale.

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 fournit un utilitaire permettant de générer le langage SQL pour la création de ces tables, le générateur DLL SIB.

Le générateur peut être exécuté avec la commande suivante (par exemple pour Windows) :

```
%WAS_HOME%\bin\sibDDLGenerator.bat
-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 devant être utilisée, par exemple oracle ou db2 ;
- *plateforme* correspond au système d'exploitation, comme windows, unix ou 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.name du fichier Bootstrap.properties.

Par exemple :

```
c:/WebSphere/AppServer/bin/sibDDLGenerator.bat
-system db2 -platform windows
-schema db2admin -database curam -user db2admin
-statementend ; -create
```

Cette commande permet de générer des instructions SQL qui doivent ensuite être exécutées dans la base de données cible.

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 fournit le langage de définition de données pour ces tables dans son répertoire WAS_HOME /Scheduler.

Les fichiers DDL devant être exécutés sont *createTablespaceXXX.ddl* et *createSchemaXXX.ddl*, dans cet ordre, où XXX correspond au nom de votre produit de base de données cible.

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

Achèvement

Le serveur d'applications est à présent configuré et prêt pour l'installation d'une application IBM Cúram Social Program Management. Déconnectez-vous de la console d'administration et redémarrez le serveur d'applications WebSphere à l'aide des cibles décrites dans la rubrique «Démarrage et arrêt de serveurs WebSphere», à la page 14.

Déploiement d'application manuel

Pour installer une application d'entreprise dans WebSphere Application Server, il est possible d'utiliser la console d'administration. L'étape ci-après décrit l'installation d'une application d'un composant EJB ou d'un 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.

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, via le bouton **Parcourir** (facultatif), dans le panneau Chemin de la nouvelle application et cliquez sur **Suivant** ;
L'emplacement par défaut des fichiers EAR d'application est :
`%SERVER_DIR%/build/ear/WAS/Curam.ear`
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. A l'étape 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 le 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 26 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 16 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 prendre 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, à l'aide d'un navigateur Web, pointez vers l'adresse URL de l'application déployée, comme `https://localhost:9044/Curam`.

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. Vous pouvez également consulter le manuel *Cúram Third Party Tools Installation Guide* pour plus d'informations sur l'installation du déploiement réseau WebSphere.

Création de profils

Une fois le déploiement réseau WebSphere installé, il convient dans la majorité des cas de créer au moins deux profils. L'un est utilisé comme gestionnaire de déploiement pour le nœud et les autres comme serveurs fédérés.

Cette opération est effectuée à l'aide de l'assistant de création de profil, qui est démarré via le fichier `pct<hardware platform>` du répertoire `bin/ProfileCreator` de l'installation WebSphere Application Server.

Dans le cadre de cet assistant, vous devez tout d'abord choisir de créer :

1. Un profil de gestionnaire de déploiement ;
2. Un profil de serveur d'application.

Vous devez ensuite choisir d'activer ou non la sécurité administrative. Il est recommandé d'activer la sécurité administrative lors de la création du profil. Ces paramètres peuvent être modifiés ultérieurement.

Fédération d'un nœud

La fédération d'un profil de serveur d'application nécessite le démarrage du gestionnaire de déploiement ciblé.

Le gestionnaire de déploiement peut être démarré via l'exécution de la commande suivante à partir du répertoire `profiles/<nom de profil du gestionnaire de déploiement>/bin` de l'installation du déploiement réseau WebSphere :

startServer dmgr

Pour ajouter votre profil de serveur d'application au noeud du gestionnaire de déploiement, la commande suivante est utilisée à partir du répertoire `profiles/<nom du profil de serveur d'application>/bin` de l'installation WebSphere Application Server :

addNode <hôte gestdéploiement> <port gestdéploiement>

Où *<hôte gestdéploiement>* et *<port gestdéploiement>* correspondent aux port et hôte en mode écoute pour le connecteur SOAP du gestionnaire de déploiement. Les détails du connecteur SOAP sont disponibles dans la console d'administration du gestionnaire de déploiement sous :

1. Accédez à **Serveurs > Types de serveurs > Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste ;
3. Développez **Ports** dans la section **Communications** et appuyez sur le bouton **Détails (Détails)** ;
4. Les détails requis sont répertoriés en tant que **Hôte** et **Port** pour **SOAP_CONNECTOR_ADDRESS**.

Configuration du noeud

Avant de déployer une application sur le noeud enregistré, le serveur doit tout 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. Cette opération doit être effectuée via la commande `startNode.bat` ou `startNode.sh` dans le répertoire `profiles/<nom de profil fédéré>/bin` de l'installation WebSphere Application Server.

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 18 décrit la configuration manuelle de WebSphere Application Server pour une installation de base, et doit être suivie des différences identifiées ci-après. Lors de l'enregistrement de la configuration principale, vérifiez que vous avez forcé manuellement la synchronisation via la console d'administration :

1. Accédez à **Administration 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 **Sauvegarder**. La synchronisation peut prendre quelques minutes ;
4. Sélectionnez les journaux système et/ou WebSphere Application Server pour achever la synchronisation. Ces messages peuvent varier selon la version de WebSphere Application Server, cependant vous recherchez quelque chose comme :

ADMS0208I: La synchronisation de la configuration est terminée pour la cellule.

Une fois la synchronisation terminée, contrôlez le statut du serveur ainsi que les différents journaux WebSphere Application Server pour vérifier qu'elle a réussi ;

«Configuration de la sécurité de l'administration», à la page 26 détaille la configuration de sécurité nécessaire lors d'une configuration manuelle. Cette configuration nécessite de copier le fichier Registry.jar dans un répertoire situé dans l'installation WebSphere Application Server. 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 de la sécurité de l'administration», à la page 26 Cette configuration de sécurité requiert également la copie du fichier CryptoConfig.jar dans le répertoire java/jre/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 le fichier Curam.ear pour le déploiement, il convient de noter l'élément *BOOTSTRAP_ADDRESS* du serveur sur lequel ces éléments seront installés. 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. Cette modification affecte la valeur du port du fichier web.xml lors de la génération d'un fichier 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 40 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

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 sessions 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](http://www.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 États-Unis et/ou dans certains autres pays.

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

Oracle, 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.

