IBM Cúram Social Program Management
Version 6.0.5

Guide de déploiement de Cúram Portlet pour WebSphere Portal Server

Important

Avant d'utiliser ces informations et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 21

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.

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

Table des matières

Figures

Tableaux

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 de portlets sur IBM WebSphere Portal Server

Les portlets Cúram affichent des informations sur une application Cúram. Il existe un mappage un à un entre le contenu de certains pods Cúram et certains portlets Cúram. Plusieurs étapes sont requises pour déployer les portlets Cúram. Un fichier WAR de portlet est requis. Le contenu des portlets Cúram doit être configuré avant le déploiement.

Introduction

Introduction

Le présent guide décrit le processus de configuration des portlets Cúram et leur déploiement sur une page de portail, sur Portal Server.

Conditions préalables

Pour réussir à déployer et à administrer les portlets Cúram, le lecteur doit au préalable :

- savoir comment configurer IBM® WebSphere Application Server et/ou IBM WebSphere Portal Server ;
- avoir lu le document *Cúram Third-Party Tools Installation Guide for Windows (Outils tiers Cúram - Guide d'installation pour Windows)* pour savoir quels sont les logiciels nécessaires pour configurer les portlets Cúram ;
- maîtriser les notions de base concernant l'application Cúram et son développement.

Public concerné

Le présent document est un guide technique destiné aux individus chargés d'administrer les ressources sur un serveur d'application et/ou un serveur de portail.

Chapitres contenus dans ce guide

La liste suivante décrit les chapitres contenus dans le présent guide :

Présentation des portlets Cúram
Ce chapitre explique brièvement la composition d'un portlet Cúram.

Génération du fichier WAR de portlet
Ce chapitre décrit comment configurer les portlets Cúram et générer le fichier `CuramPortlets.war` avant le déploiement des portlets.

Déploiement des portlets Cúram
Ce chapitre décrit comment configurer le contenu des portlets Cúram et comment les déployer.

Configuration des portlets Cúram à connexion unique (Single Sign On)
Cette annexe décrit comment configurer manuellement le serveur de portail et comment déployer manuellement l'application Cúram de sorte qu'un utilisateur puisse activer les portlets à connexion unique (Single Sign On, soit SSO).

Présentation des portlets Cúram

Portlets Cúram

Les portlets Cúram affichent des informations relatives à une application Cúram. Il s'agit d'un mappage 1:1 entre le contenu de certaines capsules Cúram et celui de certains portlets Cúram à quelques différences près. Il existe donc une relation forte entre les contenus affichés dans les portlets et les capsules Cúram. Pour en savoir plus sur les capsules, consultez le manuel *Cúram Pod Developers Guide (Guide des développeurs de capsules Cúram)*. Les portlets Cúram ont été développés conformément à la spécification JSR 286. Toutefois, il est important de noter que cela ne signifie pas que les portlets Cúram interdisent aujourd'hui toute fonction JSR 286 (par exemple, la communication entre portlets).

Il est essentiel de comprendre que les portlets Cúram ne sont pas livrés prêts à l'emploi pour être déployés. Les quelques étapes importantes et obligatoires avant le déploiement de portlets Cúram sur une page de portail sont décrites dans les chapitres suivants. En outre, si les portlets Cúram doivent obligatoirement être à connexion unique (SSO) (comme décrit dans «Contrôle d'accès aux portlets Cúram»), vous devez suivre les instructions décrites dans «Configuration des portlets Cúram à connexion unique (Single Sign On)», à la page 6.

Contrôle d'accès aux portlets Cúram

A ce jour, il existe deux méthodes prises en charge pour contrôler l'accès aux portlets Cúram :

- **Portlets Cúram à connexion unique (Single Sign On, soit SSO)**

  Consultez la page Web Single Sign On pour en savoir plus sur la spécification SSO. En d'autres termes, une fois qu'un utilisateur a démarré une nouvelle session de portail (en se connectant), il n'est *pas* obligé de se connecter à chaque portlet Cúram sur une page de portail suite au chargement initial d'une page de portail contenant des portlets Cúram.
- **Portlets Cúram à connexion non unique (Non SSO)**

  En d'autres termes, une fois qu'un utilisateur a démarré une nouvelle session de portail (en se connectant), il *sera* obligé de se connecter à chaque portlet Cúram sur une page de portail suite au chargement initial de la page, s'il souhaite utiliser des portlets Cúram. Cela suppose qu'aucun utilisateur n'est déjà connecté à une application Cúram au sein de la même session de navigation. Consultez le chapitre relatif à la gestion des sessions dans le manuel de référence du client Web Cúram (*Web Client Reference Manual*), pour en savoir plus sur les sessions de navigation et la gestion des sessions de l'application Cúram.

Limitations actuelles des portlets Cúram

Voici les limitations actuelles des portlets Cúram :

- **Localisation**

  A ce jour, les portlets Cúram ne sont pris en charge que dans l'environnement local English (Anglais).
- **Prise en charge par le navigateur Web**

  A ce jour, les portlets Cúram ne sont pris en charge que par les navigateurs Web pris en charge par l'application Cúram. Consultez le document *Cúram v6 Supported Prerequisites (Conditions préalables de prise en charge de Cúram v6)* pour identifier les versions prises en charge par ces navigateurs.

Génération du fichier WAR de portlet

Configuration des portlets Cúram

Configuration des portlets Cúram à connexion unique (SSO) : Si des portlets Cúram SSO sont exigés, l'application Cúram (IBM Cúram Social Program Management) doit être configurée et déployée manuellement sur Portal Server. Pour ce faire, suivez les instructions décrites dans le manuel «Configuration des portlets Cúram à connexion unique (Single Sign On)», à la page 6. Autrement, une application Cúram déployée sur un serveur d'application suffit. Pour plus de détails à ce sujet, consultez le chapitre relatif au *déploiement* dans le manuel *Cúram Deployment Guide for WebSphere Application Server*.

les portlets Cúram doivent être configurés avant la génération du fichier `CuramPortlets.war`. Pour ce faire, mettez à jour les fichiers de propriétés pertinents dans le composant de base du client.[1]

Configuration des portlets Cúram

La valeur de la clé de la propriété portlet.ids dans le fichier `PortletConfig.properties` permet de définir quels portlets doivent être mis en package dans le fichier `CuramPortlets.war`. La valeur de cette propriété doit être formatée de façon à respecter les critères ci-après.

- **Il doit s'agir d'une chaîne délimitée par des virgules.**

  Cette valeur doit être délimitée par des virgules, et chaque partie de cette chaîne doit correspondre à l'ID (identificateur) d'une capsule Curam.
- **Ses sous-chaînes délimitées par des virgules doivent mapper à un fichier de propriétés.**

  La valeur de chacune de ces sous-chaînes délimitées par des virgules mappe à un fichier de propriétés dans le répertoire `PortletConfig/resources`.

Si la valeur de la propriété portlet.ids ne respecte pas ces critères, une erreur se produit lors de la génération du fichier `CuramPortlets.war`. Par défaut, la valeur de cette propriété contient la liste complète des portlets Cúram pris en charge. Il est recommandé de ne pas mettre à jour la valeur par défaut de cette propriété. Il est également recommandé de laisser en l'état les fichiers de propriétés dans le répertoire `resources` lors de l'installation, même si la valeur de la propriété portlet.ids a été modifiée.

Configuration de l'URL de base dans les portlets Cúram

L'URL (Uniform Resource Locator) de base est incluse dans l'URL absolue utilisée par chaque portlet pour accéder aux pages de l'application Cúram. L'URL de base est commune à tous les portlets Cúram. Consultez le manuel RFC 3986 pour en savoir plus sur la spécification d'URL. La valeur de la clé de la propriété base.url property dans le fichier `PortletConfig.properties` permet de configurer l'URL de base des portlets Cúram.

La valeur par défaut de la clé de la propriété base.url est **https://localhost:9044/Curam/**. La procédure suivante permet de configurer l'URL de base des portlets Cúram :

- **Schéma/Protocole**

1. La méthode actuellement prise en charge pour configurer des portlets Cúram consiste à mettre à jour les fichiers de propriétés dans le répertoire webclient/components/core/PortletConfig. Notez que cette mise à jour est en conflit avec la politique de personnalisation de fichiers dans le composant personnalisé. Cette limitation sera résolue dans une édition future.

Il s'agit de la première partie de la valeur de propriété, qui permet de configurer le protocole qui servira à accéder aux pages de l'application à partir d'un portlet Cúram. Comme vous pouvez le voir dans la valeur par défaut de la propriété, elle contient la valeur **https** qui configure un portlet pour pouvoir accéder à l'application Cúram en toute sécurité, à l'aide du protocole Hypertext Transfer Protocol et d'une couche Secure Socket Layer (HTTPS). Il est fortement recommandé de laisser cette valeur en l'état.

- **Domaine**

  Le domaine doit être utilisé pour configurer le nom d'hôte ou l'adresse IP du serveur où s'exécute le système WebSphere et où l'application Cúram a été déployée. Comme vu auparavant, le domaine par défaut est «localhost». Si la valeur par défaut n'est pas utilisée, il est préférable que le domaine soit qualifié complet. (Par exemple, serveur1.xxx.com.)

- **Numéro de port**

  Le numéro de port doit être configuré sur le numéro de port spécifié pour héberger l'application Cúram. Si cette partie de l'URL est omise de la valeur de propriété configurée, le nombre de port par défaut (`80`) est utilisé.

- **Nom d'application**

  Cette partie de l'URL de base est l'application telle qu'elle est spécifiée par la racine de contexte de l'application lors du déploiement de l'application Cúram sur un hôte.

Configuration des caractéristiques d'affichage de chaque portlet Cúram

Chaque fichier de propriétés inclus dans le répertoire `PortletConfig/resources` mappe à chaque portlet Cúram mis en package dans le fichier WAR. Ainsi, les propriétés au sein de n'importe lequel de ces fichiers de propriétés permettent de configurer l'affichage d'un portlet Cúram particulier. Les clés de propriété commençant par «javax» permettent de configurer le texte du titre et les étiquettes sur le portlet. Ces clés sont spécifiées dans la spécification du portlet. Pour en savoir plus, consultez le manuel JSR 286. La valeur de la clé de propriété portlet.height configure la hauteur d'un portlet Cúram. Toutes les propriétés au sein de chaque fichier de propriétés inclus dans le répertoire `PortletConfig/resources` sont obligatoires.

Génération du fichier WAR

Générez le fichier `CuramPortlets.war` en exécutant **`build portlet-war`** à partir du répertoire `installation_dir /webclient`.

Le fichier `CuramPortlets.war` est généré dans le répertoire `installation_dir /webclient/build/CuramPortlets`.

Déploiement des portlets Cúram

Configuration du contenu des portlets Cúram

Une fois le fichier `CuramPortlets.war` généré, le contenu des portlets Cúram doit être configuré avant d'être prêt à être déployé.

Le paragraphe suivant décrit comment configurer le contenu d'un portlet Cúram :

1. Connectez-vous à l'application Admin.
2. **Accédez aux pages de capsule personnalisées.**

Sélectionnez le lien «Pages Pod personnalisées» dans la catégorie «Interface utilisateur», à partir du panneau des raccourcis.

3. **Configurez une page personnelle.**

   Sélectionnez le contrôle d'action de page «Nouvelle page personnalisée» Une boîte de dialogue modale s'affiche alors, en même temps que la barre de progression de l'assistant.

   Dans cette barre de progression de l'assistant, sur la boîte de dialogue modale, un certain nombre d'étapes doivent être exécutées comme suit :

   - **ID page**

     La première étape de l'assistant consiste à entrer l'ID page défini pour le portlet Cúram en cours de configuration. Par exemple, si le contenu du portlet `QuickLinksPortlet` est en cours de configuration (tel que spécifié dans la valeur de clé de la propriété portlet.ids dans le fichier `PortletConfig.properties`), «QuickLinksPortlet» doit être entré dans la zone de saisie fournie. Consultez la liste d'ID des portlet Cúram dans le manuel tableau 1.

   - **Rôle utilisateur**

     La deuxième étape consiste à sélectionner l'option «SUPERROLE» à l'aide du bouton d'option.

   - **Capsules disponibles**

     La troisième étape consiste à sélectionner la capsule appropriée dans une liste (en cochant la case correspondante), pour que le contenu de la capsule appropriée s'affiche dans un portlet Cúram particulier. Le tableau suivant décrit les noms de capsule à sélectionner en fonction des portlets Cúram en cours de configuration (par ID) :

Tableau 1. Sélection d'une capsule Cúram

ID portlet Cúram	Nom de capsule Cúram
MyTasksPortlet	Mes tâches
QuickLinksPortlet	Liens rapides
MyAppointmentsPortlet	Mes rendez-vous
WorkQueuesPortlet	Files d'attente des travaux
RecentNotiPortlet	Notifications récentes
OrgSummaryPortlet	Récapitulatif de l'organisation
MyCurrentCasesPortlet	Mes dossiers en cours
MyTasksChartPortlet	Mes graphiques de tâche
CaseloadSummaryPortlet	Récapitulatif de mes dossiers

   - **Capsules par défaut**

     La quatrième étape consiste à sélectionner l'option présentée en cochant la case appropriée.

   - **Mise en page**

     La cinquième et dernière étape de l'assistant consiste à entrer le chiffre 1 dans la zone de saisie et à cliquer sur le bouton «Enregistrer» pour conclure la configuration du portlet.

     Anomalies liées à la mise en page : Si vous entrez un texte autre que 1 dans la zone de saisie fournie, des anomalies de mise en page se manifesteront lorsque les portlets Cúram seront déployés.

Configuration des utilisateurs et groupes d'utilisateurs pour les ressources de portail

Il est conseillé à l'administrateur de Portal Server de créer des groupes d'utilisateurs et des utilisateurs pour leur autoriser l'accès aux ressources de portail spécifiques à Cúram (à savoir, les portlets Cúram hébergeant des pages de portail). En outre, un mappage direct est recommandé entre les utilisateurs des ressources de portail et les utilisateurs de l'application Cúram (IBM Cúram Social Program Management) (à savoir, les `administrateurs` et les `travailleurs chargés de dossiers`). Consultez la section **Administering (Administration)** > **Users And Groups (Utilisateurs et groupes d'utilisateurs)** > **Creating new users and groups (Création de nouveaux utilisateurs et groupes)** de la documentation relative à WebSphere Portal Server pour en savoir plus sur la création d'utilisateurs et de groupes d'utilisateurs. Les utilisateurs peuvent être ajoutés au groupe `All Authenticated Portal Users (Tous les utilisateurs de portail authentifiés)` ou à un nouveau groupe dont les membres sont des utilisateurs de portlets Cúram.

Remarque : L'`ID utilisateur` et le `mot de passe` de ces utilisateurs doivent correspondre au `nom d'utilisateur` et au `mot de passe` des utilisateurs de l'application Cúram.

Déploiement de portlets sur les pages de portail

Deux étapes suffisent pour déployer un portlet Cúram sur une page de portail. Elles sont décrites dans la section **Administering (Administration)** > **Managing portlets and portlet applications (Gestion des portlets et des collections de portlets)** > **Installing a portlet (Installation d'un portlet)** de la documentation relative à WebSphere Portal Server :

- Installation du fichier `CuramPortlets.war` contenant les portlets Cúram, dans le référentiel de modules Web sur Portal Server
- Création d'une instance de portlet Cúram sur une page de portail

L'utilisateur approprié peut ouvrir une page de portail avec des portlets Cúram, en ouvrant une instance de navigateur Web et en la pointant vers : `http://domain:WpsHostPort/WpsContextRoot/MyPortalPage"/>`.

Par exemple, si les valeurs par défaut de l'installation de serveur de portail et les valeurs par défaut de la configuration de portlet Cúram sont utilisées (en supposant qu'il existe une page de portail nommée `MaPagePortail` dotée de portlets Cúram), le navigateur pointe vers : `http://localhost:10039/wps/monportail/MaPagePortail"/>`.

Configuration des portlets Cúram à connexion unique (Single Sign On)

Introduction

Les sections de la présente annexe décrivent les étapes manuelles nécessaires pour configurer les portlets Cúram à connexion unique (Single Sign On) sur Portal Server. Au préalable, Portal Server doit être configuré manuellement, et les fichiers EAR de l'application doivent avoir été déployés manuellement sur le serveur.

Configuration manuelle de WebSphere Portal Server

Démarrage de Portal Server

Pour démarrer `WebSphere_Portal`, vous devez utiliser le fichier `startServer.bat`, qui se trouve dans le répertoire `wp_profile/bin` de l'installation WebSphere :

<WEBSPHERE PORTAL INSTALL DIR>/wp_profile/bin/startServer WebSphere_Portal. Au cours de cette installation, le profil par défaut se nomme «wp_profile» (si vous avez personnalisé le nom de profil, c'est ce nom qui doit être utilisé à la place de «wp_profile», prémentionné).

Alternativement, la console d'administration peut être démarrée depuis **Démarrer** > **Programmes** > **IBM WebSphere** > **Portal Server** *Version* > **Start the Server (Démarrer le serveur)**.

Console d'administration

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

```
https://domain:10032/ibm/console"/>
```

Alternativement, la console d'administration peut être démarrée depuis **Démarrer** > **Programmes** > **IBM WebSphere** > **Application Server Network Deployment** *Version* > **Profiles (Profils)** > **wp_profile** > **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.

Chaque fois que la console d'administration est ouverte, un nom d'utilisateur et un mot de passe sont demandés pour se connecter. Ces données d'identification seront celles utilisées lors de l'installation de Portal Server. 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.

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

La console d'administration permet de configurer un alias de connexion pour DB2 et les sources de données. Pour ce faire, procédez comme suit.

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 :

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 :

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

1. Sélectionnez le `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 ;

   Database name (Nom de base de données) : nom de la base de données DB2 (qui doit être équivalent à la propriété curam.db.name dans le fichier `Bootstrap.properties`).

Server name (Nom de serveur) : nom du serveur de la base de données DB2 (qui doit être équivalent à la propriété curam.db.servername dans le fichier `Bootstrap.properties`).

Port number (Numéro de port) : port du serveur de la base de données DB2 (qui doit être équivalent à la propriété curam.db.serverport dans le fichier `Bootstrap.properties`).

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_base_données>*.

   Définissez la valeur **Mapping-configuration alias (Alias de mappage-configuration)** sur : DefaultPrinicipalMapping ;

   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_base_données>* utilisé correspond à celui défini dans «Création de l'alias de connexion à la source de données», à la page 7.

   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.

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

Le registre d'utilisateurs par défaut utilisé par l'application est le registre d'utilisateurs basé sur les fichiers WebSphere par défaut.

1. Accédez à **Sécurité** > **Sécurité globale** ;
2. Définissez **Available realm definitions (Définitions de domaines disponibles)** sur **Référentiels fédérés** et cliquez sur le bouton **Configurer** ;
3. Définissez **Primary administrative username (Nom d'administrateur principal)** sur `websphere` ;
4. Sélectionnez le bouton d'option **Automatically generated server identity (Identité de serveur générée automatiquement)** ;
5. Sélectionnez **Ignore case for authorization (Ignorer la casse 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 **Available realm definitions (Définitions de domaines disponibles)** sur **Référentiels fédérés** et cliquez sur le bouton **Set as current (Définir comme valeur actuelle** ;

8. Sélectionnez **Enable administrative security (Activer la sécurité administrative)** ;
9. Sélectionnez **Enable application security (Activer la sécurité d'application)** ;
10. Sélectionnez **Use Java 2 security to restrict application access to local resources (Utiliser la sécurité Java 2 pour limiter l'accès de l'application aux ressources locales)** et **Warn if applications are granted custom permissions (Prévenir si des autorisations personnalisées sont accordées à des applications)** ;
11. Cliquez sur le bouton **Appliquer** pour confirmer les modifications ;
12. Accédez à **Sécurité** > **Sécurité globale** ;
13. Sélectionnez le lien **Custom Properties (Propriétés personnalisées)** ;
14. Cliquez sur **Nouveau**, puis définissez le nom et la valeur comme suit :

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

    Valeur = `true`
15. Cliquez sur **OK** pour ajouter la nouvelle propriété.
16. Accédez à **Sécurité** > **Sécurité globale** ;
17. Sélectionnez **Web and SIP Security (Sécurité SIP et WEB)** > **Single sign-on (SSO) (Connexion unique)** ;
18. Le cas échéant, décochez la case **Requires SSL (SSL requis)**.
19. Assurez-vous que la zone **Nom de domaine** est définie sur le nom de domaine complet qui sera utilisé pour accéder à l'application (par exemple, xxx.com). Cette valeur devrait être similaire à celle spécifiée dans «Configuration de l'URL de base dans les portlets Cúram», à la page 3.
20. Cliquez sur **OK** pour confirmer les modifications.
21. Accédez à **Sécurité** > **Sécurité globale** ;
22. Sélectionnez**Custom properties (Propriétés personnalisées)** ;
23. Ajoutez la valeur `true` à com.ibm.ws.security.addHttpOnlyAttributeToCookies ;
24. Cliquez sur **OK** pour confirmer les modifications.
25. Enregistrez les modifications apportées à la configuration principale.

Configuration des utilisateurs

Le registre d'utilisateurs WebSphere Portal Server configuré permet d'authentifier les administrateurs et les utilisateurs de base de données. Les administrateurs et les utilisateurs de base de données WebSphere Portal Server doivent être ajoutés manuellement au registre d'utilisateurs, comme suit :

- Accédez à **Utilisateurs et groupes** > **Gérer les utilisateurs** ;
- Cliquez sur le bouton **Créer** ;
- Complétez les informations concernant l'administrateur Portal Server, puis cliquez sur le bouton **Créer**.
- Répétez ces étapes pour l'utilisateur de base de données.
- Pour chaque utilisateur d'une application Cúram (par exemple, l'application Admin), l'utilisateur équivalent doit être configuré en tant qu'utilisateur de Portal Server. Au minimum, les administrateurs et les utilisateurs chargés de dossier doivent être configurés. L'administrateur doit être configuré comme suit :
  - La zone `User ID (ID utilisateur)` doit être définie sur `admin`.
  - La zone `Prénom` doit être définie sur `admin`.
  - La zone `Prénom` doit être définie sur `worker (travailleur)`.

– Les zones `Mot de passe` et `Confirm password (Confirmation du mot de passe)` doivent être définies sur le mot de passe qui sera utilisé pour accéder à l'application admin.

Remarque : si la sécurité administrative Portal Server a été activée lors de la création du profil, il se peut que l'administrateur soit déjà défini dans le registre.

Désactivation de l'authentification entre les clusters

Cette propriété détermine le comportement d'une connexion Token2 avec authentification LTPA à connexion unique. La propriété com.ibm.ws.security.webChallengeIfCustomSubjectNotFound est définie sur 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.

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 «Enregistrement de la configuration principale», à la page 9.

Configuration d'un serveur spécifique

La présente section décrit comment configurer la cible spécifique conformément à la portée du serveur (à savoir, WebSphere_Portal).

Configuration de votre port de recherche JNDI

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste (par exemple, WebSphere).
3. Développez **Ports** dans la section **Communications**, puis cliquez sur le bouton **Details (Détails)** ;
4. Sélectionnez l'entrée **BOOTSTRAP_ADDRESS** et définissez le **Port** afin de correspondre à la valeur de la propriété curam.server.port dans votre fichier `AppServer.properties` ;
5. Cliquez sur **OK** pour appliquer les modifications ;
6. Enregistrez les modifications apportées à la configuration principale à l'aide de l'option **Enregistrer**, comme indiqué précédemment.

Configuration de votre référence pass by ORB

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste (par exemple, WebSphere).
3. Développez **Container Services (Services de conteneur)** dans la section **Container Settings (Paramètres du conteneur)**, puis cliquez sur le lien **ORB service (Service ORB)** ;
4. Sélectionnez l'option **Pass by reference (Référence pass by)** dans la section **General Properties (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

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste (par exemple, WebSphere_Portal).
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 de segment de mémoire initiale) : `512`

   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 uniquement obligatoire sur les plateformes non Windows.*

   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

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

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

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

où l'alias utilisé correspond à celui défini dans «Création de l'alias de connexion à la source de données», à la page 7.

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

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur approprié dans la liste (par exemple, WebSphere_Portal).
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 pertinent dans la liste (par exemple, WebSphere_Portal).
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**, puis 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 un nouvel `hôte virtuel` en définissant les zones ci-après.

    Nom = *hôte_client*

    Répétez cette étape en remplaçant *hôte_client* par *hôte_webservices* ;
19. Sélectionnez le lien **client_host (hôte_client)** dans 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 «Enregistrement de la configuration principale», à la page 9.

Configuration de l'intégration de la sécurité de session

1. Accédez à **Serveurs** > **Types de serveurs** > **Serveurs d'applications WebSphere** ;
2. Sélectionnez le serveur pertinent dans la liste (par exemple, WebSphere_Portal).
3. Cliquez sur **Session management (Gestion de session)** dans la section **Container Settings (Paramètres du conteneur)** ;
4. Sélectionnez **Security integration (Intégration de la sécurité)**, *décocher*. *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.
7.

   Remarque : Le paramètre ci-dessus est obligatoire pour les applications Web.

Configuration du bus

Configuration du bus d'intégration de services

1. Accédez à **Service integration (Intégration de service)** > **Buses (Bus)** ;
2. Cliquez sur **Nouveau** et lors de l'**étape 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 la sécurité de 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 «Enregistrement de la configuration principale», à la page 9.

Configuration JMS

Configuration des fabriques de connexions JMS

1. Accédez à **Ressources** > **JMS** > **JMS providers (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 **Default messaging provider (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.

   Bus Name (Nom de bus) : CuramBus

   Authentication alias for XA recovery (Alias d'authentification pour la récupération XA) : identique à la source de données `jdbc/curamdb` (par exemple : <*SERVERNAME*> /dbadmin)

   Mapping-configuration alias (Alias de mappage-configuration) : DefaultPrinicipalMapping

   Container-managed authentication alias (Alias d'authentification géré par des conteneurs) : 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.

   Bus Name (Nom de bus) : CuramBus

   Authentication alias for XA recovery (Alias d'authentification pour la récupération XA) : identique à la source de données `jdbc/curamdb` (par exemple : <*SERVERNAME*> /dbadmin)

   Mapping-configuration alias (Alias de mappage-configuration) : DefaultPrinicipalMapping

   Container-managed authentication alias (Alias d'authentification géré par des conteneurs) : identique à la source de données `jdbc/curamdb` (par exemple : <*SERVERNAME*> /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 «Enregistrement de la configuration principale», à la page 9.

Configuration des files d'attente d'application

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.

1. Accédez à **Service integration (Intégration de service)** > **Buses (Bus)** > **CuramBus** ;
2. Sélectionnez le lien **Destinations** dans la section **Destination resources (Ressources de destination)** ;

3. Cliquez sur **Nouveau** pour ouvrir l'assistant «Create new destination (Créer une nouvelle 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_d'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. Le tableau suivant permet de définir la destination d'exception via le bouton d'option **Specify (Indiquer)** et le texte associé et archivé.

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 **Default messaging provider (Fournisseur de messagerie par défaut)** ;
13. Sélectionnez le lien **Queues (Files d'attente)** dans la section **Additional Properties (Propriétés supplémentaires)** ;
14. Cliquez sur **Nouveau** et définissez les zones suivantes :

    Nom : *<nom_file_d'attente>*

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

    Bus Name (Nom de bus) : CuramBus

    Queue Name (Nom de file d'attente) : SIB_ *<nom_file_d'attente>*

    Delivery Mode (Mode de livraison) : permanent

    Laissez toutes les autres valeurs par défaut et cliquez sur **OK** pour appliquer les modifications.

Enregistrez les modifications apportées à la configuration principale, comme indiqué dans «Enregistrement de la configuration principale», à la page 9.

Configuration des rubriques d'application

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 «Enregistrement de la configuration principale», à la page 9.

Configuration des fichiers journaux d'historique

Cette étape est facultative. 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.

Achèvement

Portal Server est désormais configuré et prêt à installer une application. Déconnectez-vous de la console d'administration, puis redémarrez Portal Server.

Configuration de Portal Server de façon à réutiliser JSESSIONID

Pour activer la fonction Single Sign on (Connexion unique) entre l'application Cúram et les portlets Cúram, l'information `JSESSIONID` doit être conservée. Pour ce faire, procédez comme suit.

- Accédez à **Servers (Serveurs)** > **Server Types (Types de serveur)** > **Websphere application servers (Serveurs d'application Websphere)** > **WebSphere_Portal** > **Server Infrastructure (Infrastructure de serveur)** > **Java and Process Management (Gestion de processus et Java)** > **Process Definition (Définition de processus)** > **Java Virtual Machine (Machine virtuelle Java)** > **Custom Properties (Propriétés personnalisées)** > **Nouveau**.
- Définissez `HttpSessionIdReuse` sur la même valeur que la zone `Nom`, et définissez `Valeur` sur `true`.
- Cliquez sur **OK** pour appliquer les modifications.
- Enregistrez les modifications apportées à la configuration principale.

Déploiement d'application manuel

La console d'administration permet d'installer une application d'entreprise dans WebSphere. 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. Cliquez sur **Suivant** puis sur **Terminer** pour terminer l'installation. Cette étape peut prendre quelques minutes et doit se terminer avec un message indiquant que *l'installation de l'application Curam a abouti*.
8. Enregistrez les modifications apportées à la configuration principale. (Voir «Enregistrement de la configuration principale», à la page 9 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. 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 à un mot de passe en procédant comme suit.

    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, puis 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**.

15. 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**.
16. 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**.
17. Cliquez sur **OK**.
18. Enregistrez les modifications apportées à la configuration principale.
19. Une fois le déploiement effectué, il convient de démarrer l'application avant toute utilisation. Accédez à **Applications** > **Types d'application** > **Applications d'entreprise WebSphere**, cochez la case située en regard de l'application nouvellement installée, puis cliquez sur le bouton **Démarrer**. Cette étape peut prend quelques minutes et doit se terminer par le changement du statut de l'application pour indiquer qu'elle a été démarrée.
20. 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`.

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 session et d'authentification, pour faciliter l'utilisation des produits, pour la configuration de la connexion unique et/ou pour d'autres fonctions de suivi ou buts fonctionnels. Ces cookies ou d'autres technologies similaires ne peuvent pas être désactivés.

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

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

Marques

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

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.