IBM Cúram Social Program Management
Versión 6.0.5

Cúram - Guía de despliegue para WebSphere Application Server

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en el apartado "Avisos" en la página 45

Revisado: marzo de 2014

Esta edición se aplica a IBM Cúram Social Program Management v6.0.5 y a todos los releases posteriores mientras no se indique lo contrario en nuevas ediciones.

Contenido

Figuras

Tablas

Despliegue en IBM WebSphere Application Server

Los archivos ear de aplicación y servidor de Webclient son necesarios para compilar una aplicación de IBM Cúram Social Program Management y desplegarla en IBM WebSphere Application Server. También son necesarios una serie de valores de configuración para el despliegue.

Introducción

Guía de despliegue

Esta guía describe los pasos necesarios para construir una aplicación IBM® Cúram Social Program Management para el despliegue en la versión básica de IBM WebSphere Application Server[1]. La guía también detalla el soporte proporcionado para configurarlo y desplegarlo en WebSphere Application Server, y cuando es necesario proporciona los pasos manuales necesarios.

Es un requisito previo que el lector tenga conocimientos del entorno de desarrollo de IBM Cúram Social Program Management. En otras palabras, que sepa cómo desarrollar y construir una aplicación de servidor y un cliente web. La guía también supone que WebSphere Application Server está instalado. Para obtener más detalles sobre esta instalación, consulte la publicación *Cúram Third Party Guía de instalación de Herramientas*[2].

Creación de archivos EAR

Introducción

El paso principal antes del despliegue de una aplicación de IBM Cúram Social Program Management es empaquetarla en los archivos EAR (archivos Enterprise). La aplicación del servidor (que incorpora el cliente Web y el servidor) y los servicios se empaquetan en archivos EAR de aplicación web independiente, y el servidor de Development Environment (SDEJ) proporciona destinos de construcción que realizan esta tarea.

Antes de ejecutar los destinos en la sección siguiente, asegúrese de que se haya establecido la variable de entorno siguiente:

- WAS_HOME

  Esto debería apuntar al directorio base de la instalación básica de WebSphere Application Server. Por ejemplo: `d:\WebSphere\AppServer` o `/opt/WebSphere/AppServer`.

1. Para obtener más información sobre la utilización de la aplicación con la edición de despliegue de red de WebSphere Application Server consulte "Configuración manual de WebSphere Application Server" en la página 18.
2. Consulte la guía de instalación que corresponda a la plataforma, es decir Microsoft Windows o **UNIX**.

La aplicación empresarial

Creación del archivo EAR de la aplicación

El siguiente destino debe ejecutarse desde el directorio raíz del proyecto de servidor para crear el archivo EAR de la aplicación para WebSphere Application Server:

```
build websphereEAR
```

Este destino creará un archivo EAR preparado para instalar, `<SERVER_MODEL_NAME>.ear`, ubicado en `<SERVER_DIR>/build/ear/WAS`[3].

Antes de ejecutar este destino debe haber disponible una aplicación totalmente generada. Para obtener más detalles sobre cómo generar una aplicación IBM Cúram Social Program Managemen, consulte la publicación *Cúram Server Guía del desarrollador*.

Nota: No se puede crear un archivo EAR para la base de datos H2.[4]

En segundo plano

El destino **websphereEAR** toma varios archivos Java y descriptores de despliegue previamente generados y los empaqueta en un archivo EAR.

Los archivos Java y los descriptores de despliegue se generan durante el proceso de construcción basándose en la existencia de clases de Business Process Object (*BPO*), es decir, los métodos de las clases o las clases WebService *de fachada*, y los pueden llamar los clientes remotos.

De forma predeterminada todas las llamadas remotas al servidor son manejadas por la sesión bean `curam.util.invoke.EJBMethod`, en lugar de un bean de sesión por interfaz disponibles públicamente. Este bean proporciona soporte para funciones de gestión de IBM Cúram Social Program como autorizaciones, auditorías y rastreos. Si es necesario, también es posible generar una interfaz de fachada[5].

Contenido del archivo EAR de la aplicación

El archivo EAR que se genera tiene la siguiente estructura y contenido:

- Directorio META-INF
  - `application.xml`

    Este archivo se genera automáticamente y muestra la correlación de módulos EJB con los archivos JAR que contiene la aplicación.
  - `ibm-application-bnd.xmi`

    Un archivo de extensión específica WebSphere Application Server generado.
  - `ibm-application-ext.xmi`

    Un archivo de extensión específica WebSphere Application Server generado.
  - `was.policy`

3. SERVER_MODEL_NAME y SERVER_DIR son variables de entorno que especifican el nombre del modelo en el proyecto y el directorio raíz del proyecto respectivamente.

4. Para obtener más información sobre la base de datos H2 consulte la publicación *Cúram Third-Party Tools Guía de instalación para Windows*.

5. El parámetro opcional`-Denablefacade=true` activa la generación de código de fachada.

Archivo de políticas de seguridad WebSphere Application Server que otorga a la aplicación el permiso Javajava.security.AllPermission.

– MANIFEST.MF

El archivo manifest que detalla el contenido del archivo EAR.

- **Archivos JAR principales**

  Los archivos JAR principales incluyen[6]:

  – 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

- **Archivos JAR de fachada**

  Sólo está presente si se ha habilitado la generación de fachadas. Todas las fachadas definidas en la aplicación se empaquetan en un archivo JAR, FacadeModule.jar. Este archivo JAR contiene las clases de implementación de bean para los módulos EJB que representan las fachadas. El archivo JAR contiene los archivos siguientes en el directorio META-INF:

  – ejb-jar.xml

    Este archivo se genera automáticamente y contiene la definición de cada módulo EJB en el archivo JAR. Se muestran todos los métodos públicamente disponibles, así como los detalles de los recursos disponibles para los módulos EJB.

  – ibm-ejb-jar-bnd.xmi

    Un archivo de extensión específica WebSphere Application Server generado.

  – ibm-ejb-jar-ext.xmi

    Un archivo de extensión específica WebSphere Application Server generado.

  – Manifest.mf

    El archivo manifest, que detalla la vía de acceso de clases para el EJB.

- **Otros archivos JAR**

6. Los números de versión no aparecen para los archivos JAR detallados.

Los otros archivos JAR contienen el código generado y elaborado desde la aplicación. Estos incluyen `aplicación.jar`, `codetable.jar`, `events.jar`, `struct.jar`, `messages.jar`, `implementation.jar` y `properties.jar`. El archivo `properties.jar` contiene el archivo `bootstrap.properties`. Es el archivo que contiene las propiedades de configuración específicas de máquina para obtener inicialmente una conexión con la base de datos.

Aplicación de servicios web

Hay soporte disponible para la generación automática de servicios web definidos de Web Service Definition Language (WSDL). De este modo, los desarrolladores de aplicaciones pueden combinar la potencia del modelo de IBM Cúram Social Program Management con la accesibilidad de los servicios web para producir componentes de software realmente reutilizables.

Creación del archivo EAR de servicios web

Debe ejecutarse el siguiente destino desde el directorio raíz del proyecto para crear el archivo EAR para los servicios web:

```
build websphereWebServices
```

Otras opciones alternativas son estas:

- `prp.webipaddress` es la dirección IP en la que escucha el servidor que aloja los servicios web. El valor predeterminado es `http://localhost:2809`;
- `prp.contextproviderurl` es el URL del proveedor de contexto JNDI. Esta es la dirección del servidor que aloja los componentes de IBM Cúram Social Program Management mediante los componentes de servicios web. El valor predeterminado es `iiop://localhost:2809`;
- `prp.contextfactoryname` es el nombre de fábrica de contextos JNDI. El valor predeterminado para esto es `com.ibm.websphere.naming.WsnInitialContextFactory`, y debe rara vez es necesario cambiarlo.

Este destino creará un archivo EAR preparado para instalar, `<SERVER_MODEL_NAME>WebServices.ear`, ubicado en `<SERVER_DIR>/build/ear/WAS`.

Antes de ejecutar este destino debe existir una aplicación IBM Cúram Social Program Management totalmente generada y lista para el despliegue.

En segundo plano

El destino **websphereWebServices** toma varios archivos Java y descriptores de despliegue previamente generados y los empaqueta en un archivo EAR.

Los archivos Java y los descriptores de despliegue se generan durante el proceso de generación (consulte la publicación *Cúram Server Guía del desarrollador*) basándose en los *componentes de servicios web* que se han definido en el modelo. Las clases de BPO deben correlacionarse con los componentes del servidor con un estereotipo de servicio web para que esta generación se produzca[7]. Cualquier componente de servidor con un estereotipo de servicio web se tratará como si también tuviese un estereotipo de ejb. Esto es porque las interfaces de servicios web son contenedores en BPO disponibles públicamente.

7. Consulte la publicación *Cúram Server Guía de modelación* para obtener detalles sobre cómo asignar BPO a los componentes del servidor.

Contenido del archivo EAR de servicios web

El archivo EAR que se genera tiene la siguiente estructura y contenido:

- Directorio META-INF
  - `application.xml`

    Este archivo detalla del módulo principal para la aplicación de servicios web, que es el archivo `webservices.war`.
  - `ibm-application-bnd.xmi`

    Un archivo de extensión específica WAS generado.
  - `ibm-application-ext.xmi`

    Un archivo de extensión específica WAS generado.
  - `was.policy`

    Archivo de políticas de seguridad WAS que otorga a la aplicación el permiso Javajava.security.AllPermission.
  - `MANIFEST.MF`

    El archivo manifest que detalla el contenido del archivo EAR.
- **Archivo WAR del servicio web**

  Este archivo contiene los archivos JAR del directorio `WEB-INF/lib`, incluyendo:
  - `coreinf.jar`

    Este archivo JAR contiene los métodos de conversión que se utilizan para dar soporte a la serialización de los tipos complejos que se utilizan en la interfaz.
  - `axis.jar`

    Este archivo JAR contiene el motor de servicios web Axis.
  - `appwebservices.jar`

    Este archivo JAR contiene las clases de contenedor que permiten a los servicios web Axis conectarse al servidor de aplicaciones de IBM Cúram Social Program Management de los beans de la sesión y las clases para los tipos complejos que se utilizan en la interfaz de servicios web.
  - `server-config.wsdd`

    Este archivo `wsdd` se encuentra en el directorio `WEB-INF` y contiene la configuración del motor de servicios web que correlaciona los BPO de IBM Cúram Social Program Management con los servicios web.

WSDL de servicio web

Un servicio web de IBM Cúram Social Program Management expone su propio WSDL una vez se despliega.

Por ejemplo, si hay un servicio en el URL:

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

La descripción WSDL estará en el URL:

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

El URL

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

devolverá una página web que muestra todos los servicios web desplegados y un enlace a sus archivos WSDL.

El formato de URL general de las ubicaciones anteriores es este:

`http://<web-server>:<port-number>/<ServerModelName>WS/services/<BPO-name>`.

Varios archivos EAR

Para la creación de una aplicación EAR también es necesario un archivo opcional para permitir la división de los componentes de cliente en distintos archivos WAR y EAR, y también para permitir un mayor control de una parte de la configuración EAR y de los módulos incluidos. Este archivo se denomina `deployment_packaging.xml` y debe colocarse en el directorio `SERVER_DIR/project/config`.

El formato del archivo `deployment_packaging.xml` es el siguiente:

```
<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>
```

Figura 1. deployment_packaging.xml sample

Cada archivo puede tener varios elementos `ear` y da como resultado un archivo EAR que se genera en el directorio `SERVER_DIR/build/ear/WAS`. Las opciones para cada elemento son:

- `name`

  Esta opción controla el nombre del EAR creado a partir del proceso.

- `requireServer`

  Este atributo opcional controla si el módulo de servidor está incluido en el archivo EAR. Las entradas válidas son `true` o `false`. El valor predeterminado es `false`. Si se despliegan varios archivos EAR en un servidor de aplicaciones, este atributo debe establecerse en `true` sólo para un archivo EAR, ya que sólo se puede desplegar un módulo de servidor IBM Cúram Social Program Management por cada clúster. Si se establece `requireServer` en `true` para varios archivos EAR, los demás archivos EAR deben desplegarse en un clúster EAR para evitar conflictos.

- `components`

  Esta opción controla qué componentes de cliente se colocan en el archivo EAR. También controla el orden de los componentes para la nueva creación del cliente que deberá tener lugar. Normalmente, el directorio principal no forma parte del orden de los componentes, pero en esta ocasión es importante añadir esta opción para indicar si debe incluirse en un archivo WAR determinado. Estas entradas deben seguir el orden habitual de los componentes definidos en la publicación *Cúram Server Guía del desarrollador* y deben estar separadas por comas.

- `context-root`

  Esta opción forma la raíz de contexto del módulo WAR en el descriptor de despliegue `application.xml`. Estas entradas deben empezar con una barra inclinada.

- `custom-web-xml`

Este elemento opcional controla si un archivo `web.xml` debe sobrescribir la versión estándar en el archivo WAR. Estas entradas deben ser una vía de acceso de Apache Ant que lleve al directorio que contiene el archivo `web.xml`.

Es posible utilizar referencias a variables de entorno como parte de esta vía de acceso. Por ejemplo, puede utilizarse `${client.dir}` para que apunte al directorio del cliente web y `${SERVER_DIR}` para que apunte al directorio del servidor.

- `requireSearchServer`

  Consulte *Servidor de búsquedas genérico de Cúram* para obtener información adicional.

Para cada cliente web (por ejemplo, un archivo WAR) se necesita un componente de cliente web independiente para que contengasus personalizaciones. En el caso de varios clientes web, la variable de entorno CLIENT_COMPONENT_ORDER incluirá todos los componentes personalizados; pero serán necesarios los elementos <ear> separados, uno para cada componente web personalizado (y otros componentes, según sea necesario).

Al igual que con el destino estándar, debe haber disponible una aplicación IBM Cúram Social Program Management generado totalmente. Para obtener más detalles sobre cómo generar una aplicación, consulte la publicación *Cúram Server Guía del desarrollador*.

Destinos alternativos

El destino **`websphereEAR`** generará un archivo `.ear` de la aplicación IBM Cúram Social Program Management que contiene tanto el cliente web como una aplicación. Se proporciona soporte para crear un archivo `.ear` de la aplicación que contiene sólo la aplicación web o sólo la aplicación de servidor.

Estos objetivos pueden ser necesarios cuando es necesario instalar el cliente web y la aplicación de servidor en servidores distintos. Por ejemplo, para dar soporte al acceso seguro a la aplicación de Cúram para los usuarios externos se puede desarrollar una aplicación cliente web nueva. Esta aplicación web puede desplegarse por sí misma y utilizar una aplicación del servidor existente.[8]

Para crear un archivo `oreja` que contenga sólo debe usarse la aplicación de cliente web mediante el mandato siguiente:

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

Para crear un archivo `.ear` que contenga sólo debe usarse la aplicación de servidor mediante el mandato siguiente:

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

8. Para obtener más información sobre la seguridad de acceso externo, consulte la publicación *Cúram Server Guía del desarrollador*.

Configuración del servidor de aplicaciones

Introducción

Este capítulo presupone que WebSphere ya se ha instalado. Consulte la publicación *Cúram Third Party Guía de instalación de Herramientas*[9]para obtener detalles sobre la instalación.

La configuración de WebSphere Application Server es similar en todas las plataformas, y el entorno de desarrollo de Java Server (SDEJ) proporciona un número de destinos Ant para facilitar la configuración y la gestión de la instalación. Para los interesados, "Configuración manual de WebSphere Application Server" en la página 18 detalla los pasos manuales realizadas por los scripts de configuración.

El destino de configuración proporcionado por SDEJ es una configuración predeterminada simple y puede no ser adecuado para un entorno de producción.

Nota: El destino de **configuración** sobrescribirá el perfil *predeterminado* creado por WebSphere Application Server a menos que -Dkeep.profile=true se pase al destino.

Configuración de WebSphere Application Server

La configuración de WebSphere Application Server implica la creación de un perfil, un origen de datos, un número de servidores y la configuración de los valores JMS y de seguridad. Todas estas tareas pueden realizarse mediante la ejecución del destino **configurar** proporcionado por SDEJ.

El perfil creado por el destino **configurar** tomará el valor por omisión siguiente a menos que se sustituya específicamente al llamar al destino.

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

El mandato **build configure** debe ejecutarse desde el directorio `<SERVER_DIR>` para invocar la configuración automática. Este destino requiere que existan los archivos `AppServer.properties` y `bootstrap.properties` en `<SERVER_DIR>/project/properties`[10]directorio. Consulte *Cúram Server Developer's Guide* para obtener más información sobre la configuración de un `Bootstrap.properties`. "Configuración de WebSphere Application Server" muestra ejemplos de contenido del archivo `AppServer.properties`.

9. Consulte la guía de instalación que sea relevante para la plataforma, por ejemplo Windows o **UNIX**.

10. Es posible sustituir esta ubicación predeterminada para el archivo de propiedades especificando -Dprop.file.location=<new location> cuando se ejecuta el destino **configure**.

```
## APPLICATION SERVER PROPERTIES

# Propiedad que indica que WebSphere está instalado.
as.vendor=IBM

# El nombre de usuario y contraseña cifrada del servidor admin.
security.username=<e.g. websphere>
security.password=<encrypted password>

# El nombre del nodo de WebSphere
node.name=MyNode

# El nombre del servidor en el que la aplicación se alojará.
curam.server.name=CuramServer
curam.server.port=2809

################################################
## LAS PROPIEDADES SIGUIENTES SON SÓLO PARA WebSphere##
################################################
# El alias que se debe usar para la autorización de la base de datos
curam.db.auth.alias=databaseAlias

# Puerto HTTP para el servidor en el que se
# accederá al cliente
curam.client.httpport=9044

# Puerto HTTP para el servidor en el que se
# accederá a los servicios web
curam.webservices.httpport=9082

# Propiedad para establecer el tamaño de almacenamiento dinámico inicial y máximo de la JVM.
curam.server.jvm.heap.size=1024
```

Figura 2. Ejemplo de propiedades de AppServer

De forma predeterminada, el destino **configure** establece un origen de datos de controlador Universal de tipo 4 (XA). Sin embargo, puede configurar un origen de datos de controlador universal de tipo de 2 (XA) estableciendo la propiedad curam.db.type2.required en el archivo `AppServer.properties`.

También de forma predeterminada el destino **configure** establece la el tamaño de almacenamiento dinámico inicial y máximo de la JVM en "1024" MB. Sin embargo, puede sustituir el tamaño del almacenamiento dinámico inicial y máximo de la JVM por omisión estableciendo la propiedad curam.server.jvm.heap.size en el archivo `AppServer.properties`.

Nota:

1. El valor del almacenamiento dinámico de Java descrito en el ejemplo “Configuración de WebSphere Application Server” en la página 8 y establecido por los scripts de configuración tiene fines ilustrativos. Según el tamaño de la aplicación personalizada, la estrategia de despliegue, etc. estos valores pueden ser demasiado bajos o demasiado altos. El valor óptimo debe ser determinado por la supervisión del rendimiento de la memoria del servidor.
2. Se han observado problemas de memoria con los controladores de bases de datos envueltos de WebSphere Application Server durante la recuperación de CLOB y BLOB grandes (3MB+) de la base de datos. Estos problemas pueden solucionarse aumentando el tamaño máximo de almacenamiento dinámico JVM como parámetro apropiado en el servidor desplegado.

3. El destino **configure** no se puede ejecutar cuando la base de datos H2 está en uso.[11]

Configuración de la seguridad

La configuración de seguridad por omisión de IBM Cúram Social Program Management dentro de WebSphere Application Server implica la omisión de archivos basada en el registro de usuario y un módulo de inicio de sesión JAAS. El apartado *Configuración predeterminada para IBM WebSphere Application Server* de la publicación *Cúram Security Handbook* debe consultarse para obtener más detalles sobre esto.

Hay diversas configuraciones de seguridad alternativas que pueden utilizarse con WebSphere Application Server. Las configuraciones están disponibles para dar soporte a la utilización de mecanismos de autenticación alternativos, como por ejemplo un servidor de directorios LDAP o una solución de inicio de sesión único.

Para beneficiarse de una configuración diferente deben definirse las propiedades detalladas en las secciones siguientes en el archivo `AppServer.properties` antes de ejecutar el destino `configure`. Los mecanismos de autenticación alternativos deben configurarse manualmente después de ejecutar el destino `configure` con el conjunto de propiedades correspondientes. Para configurar el módulo de inicio se sesión para la autenticación sólo por identitidad, la propiedad curam.security.check.identity.only debe establecerse en `true`. De este modo se garantiza que se utilice el mecanismo de autenticación alternativo configurado.

El apartado *Autenticación sólo por identidad* de la publicación *Cúram Security Handbook* contiene más detalles.

Pasos de configuración especiales al usar sólo identidad y LDAP

Cuando se utiliza sólo la identidad en combinación con WebSphere Application Server y LDAP, es posible que se deban realizar pasos adicionales de configuración manual; es decir, independientemente de si la configuración se realiza a través de la consola administrativa de WebSphere Application Server o el destino `configure`. Con esta combinación, puede ver que WebSphere Application Server no se puede iniciar correctamente debido a la necesidad de añadir un nombre de usuario generado por WebSphere Application Server a la propiedad de la lista de exclusión del módulo de inicio de sesión (exclude_usernames) descrita en el apartado "Añadir el módulo de inicio de sesión" en la página 27. En este caso de incapacidad de WebSphere Application Server de iniciarse se producirá un mensaje de error SECJ0270E en el archivo `SystemOut.log` antes del fallo.

Estos son los pasos necesarios para resolver este error:

1. Identifique el nombre de usuario que está provocando que WebSphere Application Server empiece a fallar. Configure el rastreo del módulo de inicio de sesión como se describe en el apartado "Registro del proceso de autenticación" en la página 12 (en relación con el destino `configure`) o "Añadir el módulo de inicio de sesión" en la página 27 (en relación con la configuración a través de la consola administrativa) y reinicie WebSphere Application Server. Con el rastreo del módulo de inicio de sesión en ejecución, antes del error de SECJ0270E en el archivo `SystemOut.log`, los datos de rastreo identificarán el

11. Para obtener más información sobre la base de datos H2 consulte la publicación *Cúram Third-Party Tools Guía de instalación para Windows*.

nombre de usuario fallido con un registro como el siguiente:

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

Donde "MyNode" es el nombre del nodo, "MyNodeCell" es el nombre de la celda y "CuramServer" es el nombre del servidor de WebSphere. Después de los datos de rastreo de módulo de inicio de sesión aparecerá el error, que será similar al siguiente:

```
SECJ0270E: No se han podido obtener las credenciales reales.
   La excepción es javax.security.auth.login.LoginException:
   Contexto: MyNodeCell/nodes/MyNode/servers/CuramServer,
   Nombre: curamejb/LoginHome:
   No se ha encontrado el primer componente en el nombre curamejb/LoginHome.
```

2. Especifique el nombre de usuario erróneo en la propiedad exclude_usernames del módulo de inicio de sesión en la configuración de WebSphere Application Server. Puesto que WebSphere Application Server no consigue iniciarse, realice este cambio a través de la consola administrativa y edite directarmentre el archivo de configuración de WebSphere Application Server. En el sistema de archivos de configuración de WebSphere Application Server edite `config\cells\MyNodeCell\security.xml`, que tendrá tres apariciones de la propiedad exclude_usernames (una para cada alias); por ejemplo:

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

Debe modificar las tres apariciones para que incluyan el nombre de usuario recién identificado a partir de la entrada de rastreo anterior; por ejemplo:

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

Tenga en cuenta que en las apariciones de exclude_usernames el atributo de ID variará según la configuración del sistema y el separador de coma en el atributo del valor de ejemplo representa el valor curam.security.usernames.delimiter predeterminado, que puede ser diferente en su caso.

3. Reinicie WebSphere Application Server.

Registro de usuarios de WebSphere Application Server

De forma predeterminada, el registro de usuario de WebSphere Application Server no es consultado como parte de la autenticación. Cuando el módulo de inicio de sesión se ha configurado sólo para la identidad, el registro de usuarios es consultado. Es posible sustituir este comportamiento por omisión estableciendo la propiedad curam.security.user.registry.enabled. Si esta propiedad se establece en `true`, el registro de usuario de WebSphere Application Server será consultado durante el proceso de autenticación, independientemente de si está habilitada o inhabilitada la autenticación sólo con identidad. Si esta propiedad se establece en `false`, el registro de usuario de WebSphere Application Server no se consulta. Por ejemplo, si curam.security.check.identity.only está establecido en `true` y curam.security.user.registry.enabled se establece en `false`, ni la verificaciones de

autenticación de IBM Cúram Social Program Management ni el registro de usuario de WebSphere Application Server se utilizará como parte del proceso de autenticación.

También puede controlar la autenticación de tipos de usuarios externos (es decir, los usuarios no internos) con el registro de usuarios de WebSphere Application Server mediante el uso de las propiedades curam.security.user.registry.enabled.types y/o curam.security.user.registry.disabled.types. Estas propiedades especifican una lista delimitada por comas de tipos de usuario externos que se autenticarán, o no, mediante el registro de usuario de WebSphere Application Server:

- Los tipos de usuario especificados en la lista de curam.security.user.registry.enabled.types serán procesados en el registro de usuario de WebSphere Application Server (por ej. LDAP) y la implementación de `ExternalAccessSecurity`.
- Los tipos de usuario especificados en la lista curam.security.user.registry.disabled.types no se procesarán en el registro de usuario de WebSphere Application Server y el procesamiento de la implementación de `ExternalAccessSecurity` será la autorización para realizar la autenticación.

El orden de prioridad en el proceso de estas tres propiedades y el usuario WebSphere Application Server o el registro externo (por ej. LDAP) es el siguiente:

- De forma predeterminada, el registro de usuario de WebSphere Application Server no está marcado y se utiliza la autenticación de la aplicación.
- El establecimiento de la propiedad curam.security.user.registry.enabled en `true` requiere la autenticación mediante el servidor de Application Server o externa (por ej. LDAP), el registro de usuarios y la seguridad de aplicaciones (para usuarios internos) o la aplicación `ExternalAccessSecurity` (para los usuarios externos).
- Un usuario externo de un tipo especificado en la lista de curam.security.user.registry.enabled.types debe ser autentificado por el servidor de Application Server, o mediante el registro de usuarios externo y la implementación de `ExternalAccessSecurity`.
- Un usuario externo de un tipo especificado en la lista de curam.security.user.registry.disabled.types no es autentificado por el servidor de Application Server, o mediante el registro de usuarios externo y la implementación de `ExternalAccessSecurity` es la autorización.

Consulte el apartado “Configurar el módulo de inicio de sesión JAAS del sistema” en la página 27 para obtener más información sobre cómo establecer las propiedades resultantes en la configuración de `CuramLoginModule`.

Registro del proceso de autenticación

curam.security.login.trace es una propiedad opcional que permita el registro cronológico para el módulo de inicio de sesión. Cuando se establece en `true`, esta propiedad añade información de rastreo al archivo `SystemOut.log` de WebSphere Application Server durante el proceso de autenticación.

Establecimiento de un delimitador de nombre de usuario de exclusión alternativo

curam.security.usernames.delimiter es una propiedad opcional que permitirá establecer un delimitador alternativo para la lista de nombres de usuario de la propiedad exclude_usernames. La propiedad se puede establecer en un carácter que permitirá incorporar nombres con comas como con LDAP.

Comportamiento de almacenamiento intermedio de WebSphere Application Server

WebSphere Application Server almacena la información de usuario y las credenciales en una memoria caché de seguridad y el módulo de inicio de sesión no se invocará mientras una entrada de usuario sea válida en esta memoria caché. El tiempo de invalidación predeterminado para esta memoria caché de seguridad es diez minutos, cuando el usuario ha estado inactivo durante diez minutos. La sección *Comportamiento de almacenamiento en caché de WebSphere* de la publicación *Cúram Security Handbook* debe ser consultarse para obtener más detalles sobre este tema.

Propiedades personalizadas de seguridad

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

  Esta propiedad determina el comportamiento de un inicio de sesión de LTPA Token2 de inicio de sesión exclusivo.

  Cuando el valor de esta propiedad se establecer en `true`, el símbolo contiene una clave de antememoria personalizada y no se encuentra el sujeto personalizado, se utiliza el símbolo para efectuar un inicio de sesión directamente a medida que la información personalizada necesita volver a reunirse. Se produce un desafío por lo que el usuario debe volver a iniciar la sesión. Cuando este valor de propiedad se establece en `false` y el sujeto personalizado no se encuentra, se utiliza el símbolo 2 de LTPA para iniciar la sesión y reunir todos los atributos del registro. Sin embargo, es posible que el símbolo no obtenga ninguno de los atributos especiales que esperan las aplicaciones en sentido descendente.

  Por omisión, el script de configuración establece una propiedad de WebSphere Application Server, com.ibm.ws.security.webChallengeIfCustomSubjectNotFound, en `false` para garantizar que las sesiones web puedan transferirse sin interrupciones entre dos servidores de un clúster (por ejemplo, en un caso de migración tras error) sin que se pidan credenciales de seguridad. Este valor permite validar correctamente la señal de seguridad utilizada por WebSphere Application Server, sin que el usuario tenga que hacer nada.

  Si este comportamiento no es necesario, es posible cambiar esta propiedad por true. Consulte el apartado “Configurar el módulo de inicio de sesión JAAS del sistema” en la página 27 para obtener más información sobre el establecimiento de *propiedades personalizadas de seguridad*. Si la propiedad se establece en `true`, cuando una sesión web pasa de un servidor de la agrupación a otro, quizás debido a que el servidor original falla, se solicitará al usuario información de seguridad antes de poder continuar.

Medidas de endurecimento de la seguridad

Cuando un usuario inicia la sesión en la aplicación, se proporciona un nombre de usuario y una contraseña. Estos se envían al servidor y, si se autentifica satisfactoriamente, el servidor responde con un símbolo exclusivo. En este caso, el símbolo es 'símbolo LTPA'. Este símbolo se utiliza en todas las solicitudes posteriores para reconocer el usuario y luego sirve contenido privilegiado. Cuando el usuario finaliza la sesión, en principio este símbolo podría convertirse en no válido. Sin embargo, éste no es el caso, y no hay ninguna forma de invalidar el símbolo LTPA, que ha sido confirmado por IBM. **la recomendación de IBM es utilizar dos "medidas de endurecimiento de seguridad" de:**

1. La configuración de la seguridad requiere la opción SSL;
2. Configuración de una propiedad personalizada para limitar las cookies LTPA sólo a SSL.

Los scripts de configuración predeterminados realizan este cambio y los pasos se documentan “Configurar la seguridad de administración” en la página 25.

Para más información, consulte:

- 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

Cifrado de Cúram

La codificación de Cúram trata la funcionalidad para la gestión de contraseñas, la cual se explica en detalle en la publicación *Cúram Security Handbook*. Cuando la consulte, tenga en cuenta lo siguiente:

- En entornos de producción se recomienda modificar los valores predeterminados.
- En entornos de desarrollo y prueba, debe considerar si los valores predeterminados son suficientes para proteger el entorno particular.
- Para los usuarios que vayan a actualizar desde una versión anterior de IBM Cúram Social Program Management, las contraseñas no funcionan directamente. Si no le importar obtener un nivel de seguridad menor, puede elegir, bajo su responsabilidad, seguir los pasos par a dejar el sistema existente y las contraseñas de usuario como está, pero no se recomienda. Puede encontrar más información sobre la actualización en *Cúram Upgrade Guide*.

Configuración de huso horario

Si se utilizan varias máquinas de servidor, todos ellas deben tener los relojes en sincronización y estar en el mismo huso horario para que el orden "natural" de fecha/horas en la base de datos refleje de manera precisa el orden en el que se han producido los sucesos en el mundo real. Por ejemplo, si en el registro de base de datos *A* tiene un campo de fecha/hora de creación anterior a la que tiene en el registro *B* podemos decir con seguridad que *A* se ha creado antes que *B*, independientemente de qué servidor haya creado el registro.

El huso horario del servidor o los servidores no debe cambiar nunca durante el tiempo de vida de la aplicación, La razón de esto es que el huso horario tomado al almacenar fechas en la base de datos es el huso horario del servidor actual; por lo tanto, si cambia el huso horario del servidor, todas las fechas entradas antes del cambio de huso horario estarán desincronizadas en el número de horas igual a la diferencia entre los husos horarios antiguo y nuevo.

Inicio y detención de servidores WebSphere

Se proporciona un gran número de destinos Ant para ayudar en el inicio y la detención de servidores WebSphere. Estos destinos deben ejecutarse desde el directorio `<SERVER_DIR>` y, en cuanto al destino **`configure`**, es necesario que el archivo `AppServer.properties` se configure correctamente (“Configuración de WebSphere Application Server” en la página 8). También requieren un número de opciones extra que especificar, que se detallan a continuación.

Iniciar un servidor WebSphere

El destino para iniciar un servidor WebSphere es **`startserver`** y requiere las siguientes opciones:

- `-Dserver.name`

  El nombre del servidor que se va a iniciar.

Importante: Antes de iniciar el servidor de aplicaciones por primera vez debe haber ejecutado el destino **database** seguido del destino **prepare.application.data**. Si no se ejecuta esta secuencia probablemente hará que se excedan los tiempos de espera de transacciones durante el primer inicio de sesión y provocará un error al inicializar y acceder a la aplicación. Siempre que se vuelve a ejecutar el destino **database** (por ejemplo en un entorno de desarrollo) también se debe ejecutar el destino **prepare.application.data**.

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

Figura 3. Ejemplo de uso

Detener un servidor WebSphere

El destino para detener un servidor WebSphere es **stopserver** y requiere las siguientes opciones:

- `-Dserver.name`

  El nombre del servidor que se va a detener.

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

Figura 4. Ejemplo de uso

Reiniciar un servidor WebSphere

El destino para el reinicio de un servidor WebSphere es **restartserver** y las opciones son las mismas que para el destino **startserver**. Consulte el apartado "Iniciar un servidor WebSphere" en la página 14 para obtener un ejemplo de uso.

Nota: Si el servidor no se ha iniciado ya al intentar reiniciarlo, la parte de detención del destino no hace que el destino vuelva a fallar.

Despliegue

Introducción

El paso final después de empaquetar la aplicación IBM Cúram Social Program Management y la aplicación de servicios web en los archivos EAR consiste en desplegarlos en el servidor de aplicaciones.

Antes del despliegue, es importante tener en cuenta que en WebSphere Application Server los scripts de configuración proporcionados soportan una configuración sencilla en el único servidor en las ediciones Express o Base de WebSphere Application Server.

Despliegue

El SDEJ proporciona destinos para instalar y desinstalar aplicaciones en un servidor WebSphere. Al igual que con los destinos **startserver** / **stopserver**, los destinos **installapp** / **uninstallapp** requieren que el archivo `AppServer.properties` se haya configurado correctamente (consulte el apartado "Configuración de WebSphere Application Server" en la página 8). Los objetivos también requieren un número de opciones que especificar y éstas se detallan a continuación.

Asegúrese de que el servidor se haya iniciado antes de instalar una aplicación. No hay ninguna necesidad de reiniciar el servidor después de la instalación, ya que el destino de instalación iniciará automáticamente la aplicación.

Instalar una aplicación

El destino Ant para instalar una aplicación (en forma de un archivo EAR) es **installapp** y requiere las siguientes opciones:

- `-Dserver.name`

  El nombre del servidor en el que instalar la aplicación.
- `-Dear.file`

  El nombre completo del archivo EAR que se va a instalar.
- `-Dapplication.name`

  El nombre de la aplicación.

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

Figura 5. Ejemplo de uso

Nota: El archivo EAR que contiene el módulo de servidor debe ser desplegado antes de instalar otros archivos EAR (sólo cliente).

Hay una propiedad Ant opcional disponible para pasar argumentos adicionales al wsadmin de WebSphere: `wsadmin.extra.args`. Por ejemplo, lo siguiente define tamaños de almacenamiento intermedio Java™ y pasa la opción para unir el rastreo de wsadmin:

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

No debería utilizar esta propiedad para definir argumentos ya pasados a través de los scritps de Curam Ant y puede observarlos al ejecutar Ant y especificar la opción verbose: `-v`.

Cambiar el nombre de usuario SYSTEM

Es muy recomendable cambiar el nombre de usuario para la invocación JMS al desplegar la aplicación. Las siguientes propiedades deben establecerse en el archivo `AppServer.properties` antes del despliegue para modificar este nombre de usuario:

- curam.security.credentials.async.username

  El nombre de usuario bajo el cual deben ejecutarse las invocaciones de JMS.
- curam.security.credentials.async.password

  La contraseña cifrada asociada al nombre de usuario. La contraseña debe cifrarse utilizando el destino Ant **encrypt**. Consulte la publicación *Cúram Server Guía del desarrollador* para obtener más información.

También es posible cambiar el nombre de usuario una vez que la aplicación se ha desplegado utilizando la consola administrativa de WebSphere Application Server. Vaya a **Aplicaciones** > **Tipos de aplicación** > **Aplicaciones empresariales de WebSphere** y seleccione la aplicación IBM Cúram Social Program Management. Seleccione el enlace **Ejecutar usuario como rol**. Marque el papel `todo el mundo`, escriba un nuevo nombre de usuario y la contraseña (tenga en cuenta que la contraseña debe indicarse aquí en el formato cifrado) y pulse en el botón **Aplicar**. Guarde los cambios tal como se detalla en el apartado "Guardar la configuración maestra" en la página 25.

Tenga en cuenta que si el nombre de usuario se cambia, el nuevo nombre de usuario debe existir en la tabla de base de datos de usuarios y este usuario debe tener un rol de 'SUPERROLE'.

El usuario SYSTEM es el usuario bajo el que se ejecutan los mensajes de JMS.

Desinstalar una aplicación

El destino Ant para desinstalar una aplicación es **uninstall** y requiere las siguientes opciones:

- `-Dserver.name`

  El nombre del servidor en el que se instala la aplicación.

- `-Dapplication.name`

  El nombre de la aplicación que se va a desinstalar (tal como se ha configurado durante la instalación).

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

Figura 6. Ejemplo de uso

Pre-compilación de JSP

Hay un destino adicional disponible durante el despliegue, **precompilejsp**, que permite precompilar JSP de un EAR de cliente *antes de* instalar el archivo EAR. Pre-compilar los JSP antes de realizar la instalación acelerará la visualización de una página determinada en el navegador web la primera vez que se acceda a ella.

Las opciones para el destino **precompilejsp** son:

- `-Dear.file`

  El nombre completo del archivo EAR para ser precompilarlo.

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

Figura 7. Ejemplo de uso

Nota: Mientras se ejecuta el destino **precompilejsp** para el servidor de aplicación WebSphere se puede producir una excepción de memoria (o se pueden omitir y no pre-compilar algunos JSP de forma silenciosa). Para solucionar esto el script `JspBatchCompiler.bat` del directorio `%WAS_HOME%\bin` debe ser modificado para aumentar el tamaño máximo de la memoria. Cambie el consumo de memoria de `-Xmx256m` por al menos `-Xmx1024m`.

Prueba del despliegue

Cuando se instala la aplicación[12]en la instalación de un servidor WebSphere Application Server el paso siguiente es iniciar y probar la aplicación.

Asegúrese de que se inicie el servidor que corresponda[13]y abra la página siguiente en un navegador web:

`https://<alguna. máquina.com>:<puerto>/<raíz-contexto>`

donde,

12. La instalación de una aplicación de servicios web también puede ser necesaria.

13. No hay necesidad de reiniciar el servidor después de desplegar una aplicación.

<*some.machine.com*> identifica el nombre de sistema principal o la dirección IP donde WebSphere Application Server se está ejecutando, <*port*> identifica el puerto del servidor en el que la aplicación cliente se despliega y <*context-root*> identifica la raíz de contexto del módulo WAR (consulte el apartado "Varios archivos EAR" en la página 6 para obtener más detalles).

Para que se pueda abrir la página, el navegador se dirigirá a la página de inicio de sesión. Inicie sesión con un nombre de usuario y una contraseña válida de Cúram y el navegador se redirigirá a la página solicitada.

Nota: El uso del nombre de archivo EAR `Curam.ear` para la opción `-Dear.file` y el uso del nombre del servidor de aplicaciones `Curam` para la opción `-Dapplication.name` en los ejemplos de este capítulo son sólo ilustrativos. Estos valores pueden cambiar en función de la estrategia de despliegue y la aplicación personalizada.

Utilización de IBM WebSphere Application Server con USGCB

La United States Government Configuration Baseline (Línea base de configuración del Gobierno de EEUU, USGCB) es una iniciativa federal a nivel de gobierno que proporciona pautas para mejorar las configuraciones, centrándose sobre todo en la seguridad. Cuando se ejecute la aplicación IBM Cúram Social Program Management, si se utiliza IBM WebSphere Application Server v7 (consulte la guía *Requisitos previos soportados de IBM Cúram Social Program Management v6* para obtener las versiones soportadas de IBM WebSphere Application Server v7) con una configuración USGCB, es posible que falten imágenes. Si se produce este problema, es señal de que that IBM WebSphere Application Server no reconoce los archivos .png. Para resolver este problema, deberá actualizarse IBM WebSphere Application Server para que soporte el tipo MIME PNG. Para obtener los detalles, consulte el *Information Center de WebSphere Application Server*.

Puede obtener información adicional relativa a USGCB consultando el sitio web siguiente: http://usgcb.nist.gov/

Configuración manual de WebSphere Application Server

Introducción

En los apartados de este capítulo cubren los pasos manuales necesarios para configurar y desplegar la edición Base o Express de WebSphere Application Server. Tendrá que modificar estos pasos adecuadamente para desplegarlos en una instalación de despliegue de red de WebSphere Application Server. Consulte el apartado "Despliegue de la red WebSphere" en la página 41 para obtener más información en esta área.

Configuración manual de WebSphere Application Server

La instalación de IBM WebSphere Application Server puede configurarse manualmente si es necesario, pero esto no es recomendable. Esta sección detalla los pasos manuales necesarios para configurar WebSphere Application Server sólo para fines informativos.

Vale la pena tener en cuenta que los valores especificados en el apartado **Recursos** de la consola administrativa de Application Server se pueden configurar en varios niveles que controlan el ámbito JNDI. Estos incluyen celda, nodo o servidor. Al seleccionar un **recurso**, en la parte superior de la ventana del navegador principal se muestra este ámbito y se permite ver los distintos recursos en el ámbito actual.

El ámbito y, a su vez, la ubicación de los recursos establecidos, deben basarse en el uso planificado, es decir, si se trabaja en un clúster es posible que no sea necesario establecer la misma configuración en cada servidor, así que el ámbito puede establecerse como celda o nodo.

La consola administrativa

La mayor parte de la configuración de WebSphere Application Server se realiza utilizando la consola administrativa. Para ejecutar la consola administrativa, el servidor predeterminado, por ejemplo,`server1`, debe ser iniciado, ya que la consola administrativa se instala como una aplicación Web en este servidor.

Para iniciar `server1`, debe utilizarse `startServer.bat`, que se encuentra en el directorio `profiles/AppSvr01/bin` de la instalación de WebSphere Application Server:

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

Para abrir la consola de administración, se debe apuntar a un navegador web a:
`http://localhost:9060/ibm/console"/>`

De forma alternativa, la consola administrativa puede iniciarse desde **Iniciar** > **Programas** > **IBM WebSphere** > **Application Server V7.0** > **Perfiles** > **AppSvr01** > **de la consola de administración**. TAmbién se pueden utilizar **Iniciar el servidor** y **Detener el servidor de mandatos de** desde este menú para iniciar y detener los servidores.

La primera vez que se abre la consola de administración se solicitará un usuario para el inicio de sesión. Este nombre de usuario puede ser cualquier cosa. La consola de administración está dividida en dos secciones. La parte izquierda contiene una jerarquía de árbol para navegar por la consola y el lado derecho muestra la información relacionada con el nodo actual seleccionado en el árbol. Cuando se le indique que `vaya a`, se recorre la jerarquía de árbol hasta el nodo correspondiente.

Soporte para scripts

Para dar soporte a la ejecución de scripts Ant proporcionados es necesario cambiar los archivos de propiedades de WebSphere Application Server.

sas.client.props: Abra el archivo `sas.client.props`, que se encuentran en el directorio `profiles/AppSvr01/properties` de la instalación de WebSphere Application Server. Es necesario establecer el origen de inicio de sesión para recuperar el nombre de usuario y la contraseña de un archivo de propiedades en lugar de tener que escribirlos cada vez que los scripts se ejecuten. Establezca o cuando sea necesario añada las propiedades siguientes:

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

donde *websphere* es el nombre de usuario y la contraseña para la consola administrativa.

soap.client.props: Abra el archivo `soap.client.props`, que también se encuentran en el directorio `profiles/AppSvr01/properties` de la instalación de WebSphere Application Server. Es necesario establecer el origen de inicio de sesión para recuperar el nombre de usuario y la contraseña de un archivo de propiedades en

lugar de tener que escribirlos cada vez que los scripts se ejecuten. Defina las propiedades siguientes de manera que coincidan con las credenciales que ha configurado para WebSphere en "Configuración de WebSphere Application Server" en la página 8. En el ejemplo siguiente, los valores son solo ejemplos y la contraseña que se especifica en este archivo no se puede cifrar:

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

donde *websphere* es el nombre de usuario y la contraseña para la consola administrativa.

Para evitar tiempos de espera excedidos al instalar los archivos EAR asegúrese de que se establezca lo siguiente como mínimo:

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

server.policy: Abra el archivo `server.policy`, que se encuentran en el directorio `profiles/AppSvr01/properties` de la instalación de WebSphere Application Server. Agregue las líneas siguientes al final de este archivo:

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

donde <*CURAMSDEJ*> es el directorio de instalación de SDEJ.

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

donde <*profile.name*> es el nombre del perfil de WebSphere Application Server de destino;

donde <*cell.name*> es el nombre de la celda de WebSphere Application Server de destino;

donde <*SERVER_MODEL_NAME*> es el nombre de la aplicación (nombre de base del archivo EAR).

Creación del alias de inicio de sesión del origen de la base de datos

Acerca de esta tarea

Las bases de datos soportadas son IBM DB2, IBM DB2 for z/OS y Oracle. La consola administrativa puede utilizarse para configurar un alias de inicio de sesión de DB2 y los orígenes de datos de Oracle como se indica a continuación:

Procedimiento

1. Vaya a **Seguridad** > **Seguridad global**;
2. Expanda la opción **Servicio de autenticación y autorización de Java** en el apartado **Autenticación** y seleccione la opción **Datos de autenticación J2C**;
3. Pulse **Nuevo** para abrir la pantalla de configuración;
4. Establezca los campos siguientes:

Alias = dbadmin

ID de usuario = <*database username*>

Contraseña = <*database password*>

Descripción = alias de seguridad de datos

donde en <*database username*> y <*database password*> se establece el nombre de usuario y la contraseña que se utilizan para iniciar la sesión en la base de datos;

5. Pulse **Aceptar** para confirmar los cambios.

Configurar orígenes de datos DB2

Configurar una variable de entorno DB2:
Procedimiento

1. Vaya a **Entorno** > **Variables de WebSphere**;
2. Seleccione el enlace DB2UNIVERSAL_JDBC_DRIVER_PATH de la lista de variables de entorno. Esto abrirá la pantalla de configuración de esta variable;
3. Establecer el campo **Valor** para que apunte al directorio que contiene los controlador de tipo 4/tipo 2. Este es normalmente el directorio `drivers` de la instalación de SDEJ, por ejemplo `D:\Curam\CuramSDEJ\drivers`;
4. Pulse **Aceptar** para confirmar los cambios.

Establecer el proveedor de controlador de base de datos:
Procedimiento

1. Vaya a **Recursos** > **JDBC** > **Proveedores JDBC**;
2. *Nota:* En este punto de debería seleccionar el ámbito adecuado donde se debe definir el origen de datos.
3. Pulse **Nuevo** para añadir un nuevo controlador. Se abrirá una pantalla de configuración;
4. Seleccione **DB2** en la lista desplegable de **tipo de base de datos** proporcionada;
5. Seleccione el **Proveedor de controlador JDBC universal de DB2** en la lista desplegable de **Tipo de proveedor** proporcionada;
6. Seleccione **Origen de datos XA** en la lista desplegable **Tipo de implementación** proporcionada;
7. Pulse **Siguiente** para continuar;
8. Revise las propiedades en la pantalla de configuración que se abre. No debe haber ninguna necesidad de cambiar ninguna a menos que se plantee conectarse a una base de datos **zOS**. Si es así, verifique que el campo `${DB2UNIVERSAL_JDBC_DRIVER_PATH}` esté apuntando al directorio correcto para su sistema. Por ejemplo, debe apuntar al directorio que contiene el archivo jar de licencia de DB2 Connect, `db2jcc_license_cisuz.jar` proporcionado por IBM para la conectividad de **zOS**;
9. Pulse **Siguiente** y, a continuación **Finalizar** para confirmar los cambios.

Configurar el origen de datos del controlador de base de datos:
Acerca de esta tarea

Los pasos siguientes deben repetirse para cada origen de datos, sustituyendo `curamdb`,`curamsibdb` y `curamtimerdb` con <*DatasourceName*> (sin los corchetes):

Procedimiento

1. Seleccione el `Proveedor de controlador JDBC universal DB2 (XA)` que ahora aparece en la lista de **Proveedores JDBC**. Esto abrirá la pantalla de configuración del proveedor;
2. Seleccione el enlace **Orígenes de datos** en **Propiedades adicionales**;
3. Pulse **Nuevo** para añadir un nuevo origen de datos;
4. Establezca los campos como se indica a continuación:

   Nombre de origen de datos: *<DatasourceName>*

   Nombre JNDI: *jdbc/<DatasourceName>*
5. Pulse **Siguiente** para continuar;
6. Establezca los campos como se indica a continuación:

   Tipo de controlador: 2 ó 4, según corresponda;

   Nombre de base de datos: el nombre de la base de datos DB2;

   Nombre de servidor: el nombre del servidor de la base de datos DB2;

   Número de puerto: el puerto del servidor de bases de datos DB2;

   Deje todos los demás campos sin tocar, a menos que se requiera un cambio específico, y pulse **Siguiente**;
7. Establezca el valor de desglose de **Alias de autenticación gestionado por componentes**en: *<válido para la base de datos>*;

   Establezca el valor de la lista desplegable **Alias de configuración de correlaciones** en: DefaultPrinicipalMapping

   Establezca el valor de desglose de **Alias de autenticación gestionado por contenedores**en: *<válido para la base de datos>*;

   donde el alias *<válido para la base de datos>* utilizado es el establecido en el apartado "Creación del alias de inicio de sesión del origen de la base de datos" en la página 20;

   Deje todos los demás campos sin tocar, a menos que se requiera un cambio específico, y pulse **Siguiente** para continuar;
8. Pulse **Finalizar** para confirmar los cambios y continuar;
9. Seleccione el origen de datos *nombreOrigenDatos* recién creado en la lista visualizada;
10. Seleccione el enlace **Propiedades personalizadas** en **Propiedades adicionales**;
11. Seleccione la entrada `fullyMaterializeLobData`;
12. Establezca el `valor` en `false`;
13. Pulse **Aceptar** para confirmar el cambio.

Configurar un origen de datos Oracle

Configurar una variable de entorno de Oracle:
Procedimiento

1. Vaya a **Entorno** > **Variables de WebSphere**;
2. Seleccione el enlace ORACLE_JDBC_DRIVER_PATH de la lista de variables de entorno. Esto abrirá la pantalla de configuración de esta variable;
3. Establecer el campo **Valor** para que apunte al directorio que contiene el controlador de tipo 4. Este es el directorio `drivers` de la instalación de SDEJ, por ejemplo `D:\Curam\CuramSDEJ\drivers`;
4. Pulse **Aceptar** para confirmar los cambios.

Instalación del controlador de bases de datos XA:

Procedimiento

1. Vaya a **Recursos** > **JDBC** > **Proveedores JDBC**;
2. *Nota:* el ámbito adecuado en el que se define el origen de datos debe seleccionarse en este punto.
3. Pulse **Nuevo** para añadir un nuevo controlador. Esto abrirá una pantalla de configuración;
4. Seleccione **Oracle** en la lista desplegable de **tipo de base de datos** proporcionada;
5. Seleccione el **Controlador JDBC de Oracle** en la lista desplegable **Tipo de proveedor** proporcionada;
6. Seleccione **Origen de datos XA** en la lista desplegable **Tipo de implementación** proporcionada;
7. Establezca el campo **Nombre** para que sea el controlador JDBC de Oracle (XA), si no se ha rellenado automáticamente;
8. Pulse **Siguiente** para continuar;
9. Revise la **Vía de acceso de clase** y asegúrese de que la variable de entorno `ORACLE_JDBC_DRIVER_PATH` sea correcta. Pulse **Siguiente** para continuar;
10. Revise las propiedades en la pantalla de configuración que se abre. No debe haber ninguna necesidad de cambiar ninguna;
11. Pulse **Finalizar** para confirmar los cambios.

Instalación del controlador de bases de datos no XA:
Procedimiento

1. Vaya a **Recursos** > **JDBC** > **Proveedores JDBC**;
2. Pulse **Nuevo** para añadir un nuevo controlador. Esto abrirá una pantalla de configuración;
3. Seleccione **Oracle** en la lista desplegable de **tipo de base de datos** proporcionada;
4. Seleccione el **Controlador JDBC de Oracle** en la lista desplegable **Tipo de proveedor** proporcionada;
5. Seleccione **Origen de datos de la agrupación de conexiones** en la lista desplegable **Tipo de implementación** proporcionada;
6. Establezca el campo **Nombre** para que sea el controlador JDBC de Oracle, si no se ha rellenado automáticamente;
7. Pulse **Siguiente** para continuar;
8. Revise la **Vía de acceso de clase** y asegúrese de que la variable de entorno `ORACLE_JDBC_DRIVER_PATH` sea correcta. Pulse **Siguiente** para continuar;
9. Revise las propiedades en la pantalla de configuración que se abre. No debe haber ninguna necesidad de cambiar ninguna;
10. Pulse **Finalizar** para confirmar los cambios.

Instalación de los orígenes de datos del controlador de bases de datos XA:
Acerca de esta tarea

Los pasos siguientes deben repetirse dos veces, sustituyendo *<DatasourceName>* (sin los corchetes) con `curamdb` y `curamsibdb`.

Procedimiento

1. Seleccione la `unidad de Oracle de JDBC (XA)` que aparece ahora en la lista de proveedores existentes. Se volverá a abrir la pantalla de configuración;

2. Seleccione el enlace **Orígenes de datos** en **Propiedades adicionales**;
3. Pulse **Nuevo** para añadir un nuevo origen de datos;
4. Establezca los campos como se indica a continuación:

   Nombre del origen de datos : *<NombreOrigenDeDatos>*

   Nombre JNDI: *jdbc/<DatasourceName>*

   Pulse **Siguiente**;
5. Establezca el campo Valor en: **URL**

   `jdbc:oracle:thin:@//serverName:port/databaseServiceName`, para conectarse a la base de datos utilizando el nombre de servicio Oracle.

   o

   `jdbc:oracle:thin:@serverName:port:databaseName`, para conectarse con la base de datos usando el nombre SID de Oracle.

   Donde

   serverName es el nombre del servidor que aloja la base de datos;

   puerto es el número de puerto al que la base de datos escucha;

   databaseName es el SID de la base de datos; y

   databaseServiceName es el nombre de servicio de la base de datos.

   Establezca el **Nombre de clase del ayudante de almacenamiento de datos** para que sea el `Ayudante de almacenamiento de datos Oracle 11g`;

   Deje todos los demás campos igual, a menos que sea necesario algún cambio específico y pulse **Siguiente**;

   Nota: Oracle recomienda usar el formato **URL** `jdbc:oracle:thin:/@//serverName:port/databaseServiceName` para conectarse con la base de datos Oracle con el nombre de servicio. Pero este formato de **URL** ('/' extra antes de la '@' en la **URL**) no es soportado por la consola administrativa de WebSphere Application Server. Por lo tanto, de usarse el nombre de servicio Oracle **URL** descrito anteriormente (sin '/' extra antes de la '@' en la URL) al configurar el origen de datos Oracle desde la consola de administración, para conectarse con la base de datos de Oracle utilizando el nombre de servicio.
6. Establezca el **Alias de autenticación para recuperación de XA**: *<válido para la base de datos>*

   Establezca el valor de desglose de **Alias de autenticación gestionado por componentes**en: *<válido para la base de datos>*;

   donde el alias *<válido para la base de datos>* utilizado es el establecido en el apartado "Creación del alias de inicio de sesión del origen de la base de datos" en la página 20;

   Deje todos los demás campos igual, a menos que sea necesario algún cambio específico y pulse **Siguiente**;
7. Pulse **Finalizar** para confirmar los cambios y continuar.

Configurar el origen de datos del controlador de base de datos no XA: Procedimiento

1. Seleccione el `controlador JDBC de Oracle` que aparece ahora en la lista de proveedores existentes. Se volverá a abrir la pantalla de configuración;
2. Seleccione el enlace **Orígenes de datos** en **Propiedades adicionales**;
3. Pulse **Nuevo** para añadir un nuevo origen de datos;
4. Establezca los campos como se indica a continuación:

   Nombre de origen de datos: `curamtimerdb`

Nombre JNDI:`jdbc/curamtimerdb`

Pulse **Siguiente**;

5. Establezca el campo Valor en: **URL**

   `jdbc:oracle:thin:@//serverName:port/databaseServiceName`, para conectarse a la base de datos utilizando el nombre de servicio Oracle.

   o

   `jdbc:oracle:thin:@serverName:port:databaseName`, para conectarse con la base de datos usando el nombre SID de Oracle.

   Donde

   serverName es el nombre del servidor que aloja la base de datos.

   port es el número de puerto al que la base de datos escucha.

   databaseName es el SID de la base de datos.

   databaseServiceName es el nombre de servicio de la base de datos.

   Establezca el **Nombre de clase del ayudante de almacenamiento de datos** para que sea el `Ayudante de almacenamiento de datos Oracle 11g`;

   Deje todos los demás campos igual, a menos que sea necesario algún cambio específico y pulse **Siguiente**;

   Nota: Oracle recomienda usar el formato **URL** `jdbc:oracle:thin:/@//serverName:port/databaseServiceName` para conectarse con la base de datos Oracle con el nombre de servicio. Pero este formato de **URL** ('/' extra antes de la '@' en la **URL**) no es soportado por la consola administrativa de WebSphere. Por lo tanto, de usarse el nombre de servicio Oracle **URL** descrito anteriormente (sin '/' extra antes de la '@' en la URL) al configurar el origen de datos Oracle desde la consola de administración, para conectarse con la base de datos de Oracle utilizando el nombre de servicio.

6. Establezca el valor de desglose de **Alias de autenticación gestionado por componentes**en: *<válido para la base de datos>*;

   donde el alias *<válido para la base de datos>* utilizado es el establecido en el apartado “Creación del alias de inicio de sesión del origen de la base de datos” en la página 20;

   Deje todos los demás campos igual, a menos que sea necesario algún cambio específico y pulse **Siguiente**;

7. Pulse **Finalizar** para confirmar los cambios y continuar.

Guardar la configuración maestra

Se puede realizar una operación de *Guardar* pulsando en el enlace **Guardar** en el recuadro de **Mensaje(s)**. Este recuadro sólo se muestra cuando se han realizado cambios en la configuración.

Configurar la seguridad de administración

Acerca de esta tarea

El registro de usuario por omisión que se utiliza es el registro de usuarios basado en archivos de WebSphere Application Server por omisión.

Procedimiento

1. Vaya a **Seguridad** > **Seguridad global**;
2. Establezca como **Definiciones de dominio disponibles** los **Depósitos federados** y pulse en el botón **Configurar**;
3. Establezca como **Nombre de usuario administrativo principal** `websphere`;

4. Seleccone el botón **Identidad de servidor generada automáticamente**;
5. Seleccione **Ignorar caso para la autorización** y pulse **Aceptar**;
6. Entre la contraseña para el usuario administrativo predeterminado, por ejemplo `websphere`, especifique la confirmación y pulse **Aceptar** para confirmar los cambios;
7. Establezca como **Definiciones de dominio disponibles** los **Depósitos federados** y pulse en el botón **Establecer como actual**;
8. Seleccione **Habilitar seguridad administrativa**;
9. Seleccione **Habilitar seguridad de la aplicación**;
10. Seleccione **Utilizar la seguridad Java 2 para restringir el acceso de las aplicaciones a los recursos locales** y **Avisar si se otorgan a las aplicaciones permisos personalizados**;
11. Pulse el botón **Aplicar** para confirmar los cambios;
12. Establezca como **Definiciones de dominio disponibles** los **Depósitos federados**;
13. Pulse el botón **Aplicar** para confirmar los cambios;
14. Vaya a **Seguridad** > **Seguridad global**;
15. Expanda **Seguridad SIP y web** y seleccione **Inicio de sesión único (SSO)**;
16. Seleccione **Requiere SSL**;
17. Pulse **Aceptar** para confirmar el cambio.
18. Vaya a **Seguridad** > **Seguridad global**;
19. Seleccione el enlace **Propiedades personalizadas**;
20. Pulse el botón **Nuevo** y establezca el nombre y el valor del modo siguiente:
    Nombre : `com.ibm.ws.security.web.logoutOnHTTPSessionExpire`
    Valor : `true`
21. Pulse en el botón **Aceptar** para añadir la nueva propiedad.
22. Pulse el botón **Nuevo** y establezca el nombre y el valor del modo siguiente:
    Nombre : `com.ibm.ws.security.addHttpOnlyAttributeToCookies`
    Valor : `true`
23. Pulse **Aceptar** para confirmar el cambio.
24. Guarde los cambios en la configuración maestra.

Reiniciar el servidor de aplicaciones

Este paso es obligatorio. El servidor debe reiniciarse para que los cambios de seguridad entren en vigor y para añadir usuarios adicionales necesarios. El servidor se puede detener utilizando el archivo `stopServer.bat` del directorio `profiles/AppSrv01/bin` de la instalación de WebSphere Application Server. Esto es parecido a iniciar el servidor tal como se describe en “Introducción” en la página 18.

Antes de reiniciar el servidor de aplicaciones (por ejemplo, server1), es necesario hacer disponible los archivos JAR de registro y codificación en WebSphere Application Server. El archivo JAR de registro contiene las clases necesarias para la configuración de seguridad y el archivo JAR de codificación contiene los valores de configuración y datos necesarios para la seguridad de la contraseña.

El archivo `Registry.jar` se encuentra en el directorio `lib` de la instalación de SDEJ. Copie este archivo en el directorio `lib` de la instalación de WebSphere Application Server.

El archivo `CryptoConfig.jar` puede generarse ejecutando el destino ant configtest de la manera siguiente, *build configtest -Dcrypto.ext.dir=filedir* copie CryptoConfig.jar de la ubicación generada. Copie este archivo en el directorio de Java `jre/lib/ext`. Si necesita personalizar la codificación de Curam, consulte *Curam Security Handbook* para obtener más información.

Ahora inicie el servidor de aplicaciones (por ejemplo server1) y abra la consola administrativa para continuar con los pasos de configuración. Puesto que la configuración de seguridad se ha completado y ya se han efectuado los cambios en el script, ahora es posible utilizar los scripts SDEJ para reiniciar el servidor de Application Server. Consulte el apartado "Inicio y detención de servidores WebSphere" en la página 14 para obtener más detalles sobre el reinicio del servidor.

La consola administrativa debe estar ahora abierta para continuar con la configuración. Ahora que la seguridad global está habilitada, será necesario iniciar la sesión en la consola con el nombre de usuario y la contraseña definidos antes.

Configurar usuarios

Acerca de esta tarea

Tal como se detalla en el apartado "Configuración de la seguridad" en la página 10, el registro de usuario de WebSphere Application Server configurado se utiliza para la autenticación de los usuarios de administración y el usuario de la base de datos. Los usuarios de administración de WebSphere y el usuario de la base de datos deben añadirse manualmente al registro de usuarios como se indica a continuación.

Procedimiento

1. Vaya a **Usuarios y grupos** > **Gestionar usuarios**;
2. Pulse el botón **Crear**;
3. Complete los detalles para el usuario administrativo de WebSphere y pulse en el botón **Crear**.
4. Repita los pasos para el usuario de la base de datos.

Resultados

Nota: si se ha habilitado la seguridad administrativa de WebSphere al crear el perfil del usuario administrativo ya se puede definir en el registro.

Configurar el módulo de inicio de sesión JAAS del sistema

La seguridad de aplicaciones utiliza un módulo de inicio de sesión JAAS (servicio de autenticación y autorización Java) para la autenticación. El módulo de inicio de sesión debe configurarse para las configuraciones DEFAULT, WEB_INBOUND y RMI_INBOUND. Repita los siguientes pasos para cada una de estas configuraciones.

Añadir el módulo de inicio de sesión:
Procedimiento

1. Vaya a **Seguridad** > **Seguridad global**;
2. Expanda la entrada **Servicio de autenticación y autorización de Java** en el apartado **Autenticación** y seleccione **Inicios de sesión del sistema**;
3. Seleccione el alias que corresponda de la lista. El módulo de inicio de sesión debe configurarse para los alias DEFAULT, WEB_INBOUND y RMI_INBOUND;

4. Pulse **Nuevo** para configurar un nuevo módulo de inicio de sesión;
5. Establezca el campo **Nombre de clase de módulo** como `curam.util.security.CuramLoginModule`;
6. Marque la opción **Utilizar proxy de módulo de inicio de sesión**;
7. Seleccione OBLIGATORIO en el campo **Estrategia de autenticación**;
8. Entre en **Propiedades personalizadas** parejas de nombre/valor de tabla para las propiedades necesarias tal como que se muestra a continuación, pulsando **Nueva** según sea necesario.

Tabla 1. Propiedades personalizadas de CuramLoginModule

Nombre	Valor del ejemplo	Descripción
exclude_usernames	websphere, db2admin	Obligatorio. Una lista de nombres de usuario que deben excluirse de la autenticación. El delimitador predeterminado es una coma, pero puede ser sustituido por exclude_usernames_delimiter. Esta lista debe incluir el usuario administrativo de WebSphere (tal y como se especifica en "Configurar la seguridad de administración" en la página 25) y el usuario de la base de datos (tal y como se especifica en "Creación del alias de inicio de sesión del origen de la base de datos" en la página 20). Los usuarios que se muestren aquí deben definirse en el registro de usuario de WebSphere Application Server.
exclude_usernames_delimiter	|	*Opcional*. Un delimitador para la lista de nombres de usuario que se proporciona en exclude_usernames. Un delimitador distinto de la coma por omisión puede ser útil cuando los nombres contienen comas incorporadas como con los usuarios LDAP.
login_trace	true	*Opcional*. Esta propiedad debe establecerse en true para depurar el proceso de autenticación. Si se establece en true, la invocación del módulo de inicio de sesión hará que se añada la información de rastreo al archivo de WebSphere Application Server `SystemOut.log`.
module_name	DEFAULT, WEB_INBOUND o RMI_INBOUND	*Opcional*. Esta propiedad debe establecerse en DEFAULT, WEB_INBOUND o RMI_INBOUND, en función de la configuración para la que se haya definido el módulo de inicio de sesión. Se utiliza sólo cuando login_trace se establece en true para el rastreo.
check_identity_only	true	*Opcional*. Si esta propiedad se establece en true, el módulo de inicio de sesión no realiza las verificaciones habituales de autenticación. En su lugar, simplemente se asegurará de que el usuario exista en la tabla de base de datos. En este caso, el registro de usuario de WebSphere Application Server configurado no se pasa por alto y se consulta después del módulo de inicio de sesión. Esta opción está pensada cuando se requiere soporte de LDAP o cuando se va a usar un mecanismo de autenticación alternativo. **Nota:** Si especifica sólo identidad y utiliza LDAP es posible que necesite realizar pasos de configuración adicionales; consulte el apartado "Pasos de configuración especiales al usar sólo identidad y LDAP" en la página 10.
user_registry_enabled	true	*Opcional*. Esta propiedad se utiliza para sustituir el comportamiento de la omisión del registro de usuarios. Si esta propiedad se establece en true, el registro de usuario de WebSphere Application Server se consulta durante el proceso de autenticación. Si esta propiedad se establece en false, el registro de usuario de WebSphere Application Server no se consulta.

Tabla 1. Propiedades personalizadas de CuramLoginModule (continuación)

Nombre	Valor del ejemplo	Descripción
user_registry_enabled_types	EXTERNAL	*Opcional*. Esta propiedad se utiliza para especificar una lista delimitada por comas de tipos de usuario externo que se procesa en el registro de usuario de WebSphere Application Server (por ej. LDAP). Consulte el apartado "Registro de usuarios de WebSphere Application Server" en la página 11 para obtener más información sobre el proceso del registro de usuarios de WebSphere Application Server.
user_registry_disabled_types	EXTGEN,EXTAUTO	*Opcional*. Esta propiedad se utiliza para especificar una lista delimitada por comas de tipos de usuario externo que no se procesa en el registro de usuario de WebSphere Application Server (por ej. LDAP). Consulte el apartado "Registro de usuarios de WebSphere Application Server" en la página 11 para obtener más información sobre el proceso del registro de usuarios de WebSphere Application Server.

9. Pulse en **Aceptar** para confirmar la adición del módulo de inicio de sesión nuevo;

Reordenar el módulo de inicio de sesión:
Procedimiento

1. Vaya a **Seguridad** > **Seguridad global**;
2. Expanda **Servicio de autenticación y autorización de Java** en el apartado **Autenticación** y seleccione **Inicios de sesión del sistema**;
3. Seleccione el alias que corresponda de la lista. El módulo de inicio de sesión debe reordenarse para los alias DEFAULT, WEB_INBOUND y RMI_INBOUND de la manera siguiente:
4. Pulse el botón **Establecer orden**;
5. Seleccione **curam.util.security.CuramLoginModule** y pulse en el botón **Mover hacia arriba**. Repita este procecimiento hasta que la entrada `CuramLoginModule` sea la entrada superior de la lista;
6. Pulse en **Aceptar** para confirmar las modificaciones en el orden.

Inhabilitar la autenticación entre clústeres:
Acerca de esta tarea

Esta propiedad determina el comportamiento de un inicio de sesión LTPA Token2 de inicio de sesión único. La propiedad com.ibm.ws.security.webChallengeIfCustomSubjectNotFound se establece en false para asegurarse de que las sesiones web puedan transferirse sin problemas entre dos servidores de un clúster (por ejemplo, en un caso de migración tras error) sin que se pidan credenciales de seguridad.

Procedimiento

1. Vaya a **Seguridad** > **Seguridad global**;
2. Pulse en **Propiedades personalizadas** y seleccione la propiedad **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** en la lista de propiedades disponibles.
3. En Propiedades generales, cambie el valor de la propiedad **com.ibm.ws.security.webChallengeIfCustomSubjectNotFound** a *false*
4. Pulse **Aceptar** para confirmar la adición;

Guardar los cambios: Guarde los cambios en la configuración maestra tal como se describe en el apartado "Guardar la configuración maestra" en la página 25.

Configuración del servidor

Configurar el puerto de búsqueda JNDI:
Procedimiento

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor relevante de la lista, por ejemplo server1;
3. Expanda **Puertos** en el apartado **Comunicaciones** y pulse en el botón **Detalles**;
4. Seleccione la entrada **BOOTSTRAP_ADDRESS** y defina el **Puerto** de forma que coincida con el valor de la propiedad curam.server.port del archivo `AppServer.properties`;
5. Pulse en **Aceptar** para aplicar los cambios;
6. Guarde los cambios en la configuración maestra utilizando la opción **Guardar** igual que antes.

Configurar el pase ORB por referencia:
Procedimiento

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor relevante de la lista, por ejemplo server1;
3. En la sección **Configuración del contenedor**, expanda **Servicios del contenedor** y pulse el enlace **Servicio ORB service**;
4. Seleccione la opción **Pasar por referencia** desde el apartado **Propiedades generales**.
5. Pulse en **Aceptar** para aplicar los cambios;
6. Guarde los cambios en la configuración maestra utilizando la opción **Guardar** igual que antes.

Configurar la máquina virtual Java:
Procedimiento

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor adecuado en la lista;
3. En el apartado **Infraestructura de servidor** expanda **Java y gestión de procesos**;
4. Seleccione el enlace **Definición de procesos**;
5. En el apartado **Propiedades adicionales** seleccione el enlace **Java Virtual Machine**;
6. Establezca los campos como se indica a continuación:

   Tamaño de almacenamiento dinámico inicial :`1024`

   Tamaño de almacenamiento dinámico máximo:`1024`

   Pulse **Aplicar** para establecer los valores;
7. En el apartado **Propiedades adicionales** seleccione el enlace **Propiedades personalizadas**;
8. Pulse **Nuevo** y establezca las propiedades del modo siguiente:

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

   Valor : `false`

Pulse **Aceptar** para añadir la propiedad nueva;

9. *El paso siguiente sólo es necesario en las plataformas Windows.*

   Pulse **Nuevo** y establezca las propiedades del modo siguiente:

   Nombre: `java.awt.headless`

   Valor: `true`

   Pulse **Aceptar** para añadir la propiedad nueva;
10. Guarde los cambios en la configuración maestra utilizando la opción **Guardar** igual que antes.

Configurar el servicio de temporizador:
Procedimiento

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor adecuado en la lista;
3. En la sección **Valores del contenedor** expanda **Valores del contenedor EJB**;
4. Seleccione el enlace **Valores del servicio de temporizador EJB**;
5. En el panel Tipo de planificador seleccione la opción **Usar instancia de planificador de servicios de temporizador EJB interno**;
6. Establezca los campos como se indica a continuación:

   Nombre JNDI de origen de datos: `jdbc/curamtimerdb`

   Alias de origen de base de datos: *<valid for database>*

   donde el alias utilizado es el establecido en el apartado "Creación del alias de inicio de sesión del origen de la base de datos" en la página 20;
7. Pulse **Aceptar** para confirmar los cambios;
8. Guarde los cambios en la configuración maestra utilizando la opción **Guardar** igual que antes.

Configurar el acceso al puerto:
Procedimiento

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor adecuado en la lista;
3. Seleccione el enlace **Puertos** del apartado **Comunicaciones**;
4. Pulse el botón **detalles**;
5. Pulse **Nuevo** y establezca los campos siguientes para el puerto TCP/IP del cliente:

   Nombre de puerto definido por el usuario: `CuramClientEndPoint`

   Host: `*`

   Puerto: `9044`

   Pulse en **Aceptar** para aplicar los cambios;
6. Pulse **Nuevo** y establezca los campos siguientes para el puerto TCP/IP de WebServices:

   Nombre de puerto definido por el usuario: `CuramWebServicesEndPoint`

   Host: `*`

   Puerto: `9082`

   Pulse en **Aceptar** para aplicar los cambios;
7. Vaya a **Servidores** > **Tipos de servidor** > **Servidores de aplicaciones de WebSphere**;

8. Seleccione el servidor que corresponda de la lista;
9. Expanda la rama **Valores de contenedor web** en la sección **Valores de contenedor**;
10. Seleccione el enlace **Cadenas de transporte de contenedor web**;
11. Pulse **Nuevo** y establezca los campos siguientes para la cadena de transporte del cliente:

    Nombre: `CuramClientChain`

    Plantilla de cadena de transporte: WebContainer-Secure

    Pulse **Siguiente**.

    Usar puerto existente: CuramClientEndPoint

    Pulse **Siguiente** y **Finalizar**
12. Pulse **Nuevo** y establezca los campos siguientes para la cadena de transporte de WebServices:

    Nombre: `CuramWebServicesChain`

    Plantilla de cadena de transporte: WebContainer

    Pulse **Siguiente**.

    Usar puerto existente: CuramWebServicesEndPoint

    Pulse **Siguiente** y **Finalizar**
13. Seleccione la **CuramClientChain** recién creada;
14. Seleccione el enlace **Canal entrante HTTP**;
15. Asegúrese de que el recuadro de selección **Utilizar conexiones persistentes** esté seleccionado;
16. Pulse **Aceptar** para confirmar la adición;
17. Vaya a **Entorno** > **Hosts virtuales**;
18. Pulse **Nuevo** para añadir un nuevo `Host virtual`, estableciendo los campos siguientes;

    Nombre = *client_host*

    Repita este paso sustituyendo *host_cliente* por *host_webservices*;
19. Seleccione el enlace **client_host** de la lista de hosts virtuales;

    Seleccione el enlace **Alias de hosts** del apartado **Propiedades adicionales**;

    Pulse **Nuevo** para añadir un nuevo `Alias`, estableciendo los campos siguientes;

    Nombre de host = *

    Puerto = *9044*

    donde *9044* es el puerto usado en el paso 5. Repita este paso para el otro host virtual y puerto usado (por ejemplo, webservices_host, 9082);
20. Pulse **Aceptar** para confirmar la adición;
21. Guarde los cambios en la configuración maestra tal como se describe en el apartado "Guardar la configuración maestra" en la página 25.

Configurar la integración de seguridad de la sesión: Procedimiento

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor que corresponda de la lista;
3. Pulse **Gestión de sesiones** en la sección **Configuración del contenedor**
4. Desmarque **Integración de seguridad**. *Nota: asegúrese de que la integración de seguridad esté desmarcada.*

5. Pulse en **Aceptar** para aplicar los cambios;
6. Guarde los cambios en la configuración maestra utilizando la opción **Guardar** igual que antes.

   Nota:

   Este valor anterior es necesario para las aplicaciones web de IBM Cúram Social Program Management.

Configuración del bus

Configurar el bus de integración de servicios:
Procedimiento

1. Vaya a **Integración de servicios** > **Buses**;
2. Pulse **Nueva** y en **Paso 1** establezca el campo siguiente:

   Nombre: CuramBus

   Deje todo lo demás con sus valores predeterminados y pulse **Siguiente**;
3. Al entrar en el asistente de **Configurar seguridad de bus**, Paso 1.1, pulse **Siguiente**;

   En el **Paso 1.2** del asistente **Configurar seguridad de bus** utilice el valor predeterminado y pulse **Siguiente**;

   En el **Paso 1.3** del asistente **Configurar seguridad de bus** utilice el valor predeterminado, según corresponda, y pulse **Siguiente**;

   En el **Paso 1.4** del asistente **Configurar la seguridad del bus** revise su configuración y pulse **Siguiente**;
4. En el Paso 2, pulse **Finalizar** para aplicar los cambios.
5. Seleccione el **CuramBus** que se muestra en la lista de buses. Se abrirá la pantalla de configuración;
6. Seleccione **Miembros del bus** en el apartado **Topología**;
7. Pulse en **Añadir** para abrir el asistente para **Añadir un nuevo miembro del bus**;
8. Seleccione el servidor para añadirlo al bus y pulse **Siguiente**;
9. Seleccione **Almacén de datos** y pulse **Siguiente**;
10. Seleccione la opción para **utilizar fuentes de datos existentes** y establezca las opciones tal como se indica a continuación:

    Nombre JNDI de origen de datos = jdbc/curamsibdb

    Nombre de esquema = *username*

    Donde *nombre de usuario* es el nombre de usuario de la base de datos.

    Deseleccione la opción **Crear tablas**;

    Deje todo lo demás con sus valores predeterminados y pulse **Siguiente**;
11. Acepte los parámetros de ajuste predeterminados y pulse **Siguiente**;
12. Pulse **Finalizar** para terminar y salir del Asistente
13. Vaya a **Integración de servicios** > **Buses**;
14. Seleccione el **CuramBus** que se muestra en la lista de buses. Se abrirá la pantalla de configuración;
15. Seleccione **Seguridad** en la sección **Propiedades adicionales**;
16. Seleccione **Usuarios y grupos con el rol de conector de bus** en la sección **Política de autorización** ;
17. Pulse **Nuevo** para abrir el **Asistente de recursos de seguridad de SIB**;

18. Seleccione el botón de selección **Los grupos especiales incorporados** y pulse **Siguiente**;
19. Seleccione las casillas **Servidor** y **Todos los autenticados** y pulse **Siguiente**;
20. Pulse **Finalizar** para terminar y salir del Asistente.
21. Guarde los cambios en la configuración maestra tal como se describe en el apartado "Guardar la configuración maestra" en la página 25.

Configuración JMS

Configurar las fábricas de conexiones JMS:
Procedimiento

1. Vaya a **Recursos** > **JMS** > **Proveedores JMS**;
2. *Nota:* el ámbito adecuado en el que se van a definir los recursos JMS debe seleccionarse en este punto.
3. Seleccione el enlace del **proveedor de mensajería predeterminado**;
4. Seleccione el enlace **Fábricas de conexiones** del apartado **Propiedades adicionales**;
5. Pulse **Nuevo** y establezca los siguientes campos:

   Nombre: CuramQueueConnectionFactory

   Nombre JNDI: jms/CuramQueueConnectionFactory

   Descripción: la fábrica para todas las conexiones con colas de aplicación.

   Nombre de bus: CuramBus

   Alias de autenticación la recuperación de XA: igual que para el origen de datos `jdbc/curamdb` (p.ej. <*SERVERNAME*> /dbadmin)

   Alias de configuración de correlaciones: DefaultPrinicipalMapping

   Alias de autenticación gestionado por el contenedor: el mismo que el alias de autenticación para la recuperación de XA.

   Deje todo lo demás como el valor por omisión y pulse **Aceptar** para aplicar los cambios;
6. Pulse **Nuevo** y establezca los siguientes campos:

   Nombre: CuramTopicConnectionFactory

   Nombre JNDI: jms/CuramTopicConnectionFactory

   Descripción: la fábrica para todas las conexiones con colas de aplicación.

   Nombre de bus: CuramBus

   Alias de autenticación la recuperación de XA: igual que para el origen de datos `jdbc/curamdb` (p.ej. <*SERVERNAME*> /dbadmin)

   Alias de configuración de correlaciones: DefaultPrinicipalMapping

   Alias de autenticación gestionada por el contenedor: igual que para el origen de datos `jdbc/curamdb` (p.ej. <*SERVERNAME*> /dbadmin)

   Deje todo lo demás como el valor por omisión y pulse **Aceptar** para aplicar los cambios;
7. Guarde los cambios en la configuración maestra tal como se describe en el apartado "Guardar la configuración maestra" en la página 25.

Resultados

Nota: Con los pasos de configuración manual anteriores no es posible configurar correctamente la seguridad para las fábricas de conexiones de colas y temas. Para completar esta parte de la configuración debe utilizar la herramienta `wsadmin`. Para hacerlo, salga de la consola administrativa y siga estos pasos:

1. Identifique las entradas de la fábrica de conexiones de colas y temas en el archivo de configuración de WebSphere Application Server `resources.xml`. Este archivo reside en la jerarquía del sistema de archivos de `%WAS_HOME%\profiles\<profile_name>\config` en función de los convenios de denominación y el ámbito donde se hayan definido los recursos JMS. Por ejemplo, utilizando un ámbito de nivel de nodo con un nombre de perfil `AppSrv01`, un nombre de célula `MyNodeCell` y un nombre de nodo `MyNode` podría encontrar este archivo aquí: `C:\WebSphere\profiles\AppSrv01\config\cells\MyNodeCell\nodes\MyNode\resources.xml`. En este archivo debe encontrar las entidades `<factories>` para `CuramQueueConnectionFactory` y `CuramTopicConnectionFactory`, y tomar nota del ID para cada uno que comience con `J2CConnectionFactory_` seguido de un número (por ejemplo, 1264085551611).
2. Invoque el script WebSphere `wsadmin`. En estos ejemplos, el lenguaje es JACL, así que es posible que el argumento *-lang jacl* no se deba especificar junto con las credenciales de inicio de sesión, etc. según la configuración local.
3. En `wsadmin` invoque los mandatos siguientes; una vez más, asumiendo las definiciones del ámbito del nodo, un nombre de celda `MyNodeCell`, y un nombre de nodo `MyNode`, el ID de recurso será diferente en su entorno.
   a. Obtenga el identificador de nodo y célula: `$AdminConfig getid /Node:MyNodo`
   b. Utilizando el identificador de nodo y célula del paso anterior, combínelo con el identificador de fábrica de conexiones obtenido anteriormente para visualizar la fábrica de conexiones: `$AdminTask showSIBJMSConnectionFactory CuramQueueConnectionFactory(cells/MyNodeCell/nodes/MyNode|resources.xml#J2CConnectionFactory_1264085551611)`

      A partir de la salida del comando anterior, deberá comprobar que authDataAlias no está establecido (p. ej. `authDataAlias=`); de lo contrario habrá terminado, tal como se muestra en esta salida de ejemplo de wsadmin:

```
{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. Para establecer authDataAlias, utilice la misma información de fábrica de conexiones de antes, p.ej.: `$AdminTask modifySIBJMSConnectionFactory CuramQueueConnectionFactory(cells/MyNodeCell/nodes/MyNode|resources.xml#J2CConnectionFactory_1264085551611) {-authDataAlias crouch/databaseAlias}`
   d. Guarde los cambios: `$AdminConfig save`

e. Puede invocar el comando `showSIBJMSConnectionFactory` para verificar el cambio.
f. Repita los pasos para `CuramTopicConnectionFactory`.
g. Reinicie el servidor de aplicaciones.

Configurar las colas necesarias:
Acerca de esta tarea

Lleve a cabo los pasos siguientes, sustituyendo <*QueueName*> (sin los corchetes) con cada uno de los siguientes nombres de cola: DPEnactment, DPError, CuramDeadMessageQueue, WorkflowActivity, WorkflowEnactment y WorkflowError.

Procedimiento

1. Vaya a **Integración de servicios** > **Buses** > **CuramBus**;
2. Seleccione el enlace **Destinos** del apartado **Recursos de destino**;
3. Pulse **Nuevo** para abrir el asistente "Crear nuevo destino";
4. Seleccione **Cola** como tipo de destino y pulse **Siguiente**;
5. Establezca los siguientes atributos de cola:
   Identificador : SIB_ <*NombreCola*>
   Deje todo lo demás con sus valores predeterminados y pulse **Siguiente**;
6. Utilice el **miembro de bus seleccionado** y pulse **Siguiente**;
7. Pulse **Finalizar** para confirmar la creación de la cola.
8. Seleccione la cola SIB_MQ_ENDPOINT_ADDRESS recién añadida <*QueueName*> que aparece ahora en la lista de proveedores existente. Se volverá a abrir la pantalla de configuración;
9. Utilice la tabla siguiente para establecer el destino de excepción mediante el botón de selección **Especificar** y el campo asociado;

Tabla 2. Valores de destino de excepción

Nombre de cola	Destino de excepción
SIB_CuramDeadMessageQueue	Sistema
SIB_DPEnactment	SIB_DPError
SIB_DPError	SIB_CuramDeadMessageQueue
SIB_WorkflowActivity	SIB_WorkflowError
SIB_WorkflowEnactment	SIB_WorkflowError
SIB_WorkflowError	SIB_CuramDeadMessageQueue

10. Pulse en **Aceptar** para aplicar los cambios.
11. Vaya a **Recursos** > **JMS** > **Proveedores JMS**;
12. Seleccione el enlace del **proveedor de mensajería predeterminado**;
13. Seleccione el enlace **Colas** del apartado **Propiedades adicionales**;
14. Pulse **Nuevo** y establezca los siguientes campos:
    Nombre: <*QueueName*>
    Nombre JNDI: jms/ <*QueueName*>
    Nombre de bus : CuramBus
    Nombre de cola: SIB_ <*QueueName*>
    Modo de entrega: Persistent

Deje todo lo demás como el valor por omisión y pulse **Aceptar** para aplicar los cambios;

Resultados

Guarde los cambios en la configuración maestra tal como se describe en el apartado "Guardar la configuración maestra" en la página 25.

Configurar los temas necesarios:
Procedimiento

1. Vaya a **Recursos** > **JMS** > **Proveedores JMS**;
2. Seleccione el enlace del **proveedor de mensajería predeterminado**;
3. Seleccione el enlace **Temas** del apartado **Propiedades adicionales**;
4. Pulse **Nuevo** y establezca los siguientes campos:

   Nombre : CuramCacheInvalidationTopic

   Nombre JNDI : jms/CuramCacheInvalidationTopic

   Descripción: Cache Invalidation Topic

   Nombre de bus: CuramBus

   Espacio de tema: Default.Topic.Space

   Modo de entrega JMS: Persistent

   Deje todo lo demás como el valor por omisión y pulse **Aceptar** para aplicar los cambios;
5. Guarde los cambios en la configuración maestra tal como se describe en el apartado "Guardar la configuración maestra" en la página 25.

Configurar las especificaciones de activación de colas necesarias:
Acerca de esta tarea

Como con la configuración de las colas, lleve a cabo los pasos siguientes, sustituyendo <*QueueName*> (sin los corchetes) con cada uno de los siguientes nombres de cola: DPEnactment, DPError, CuramDeadMessageQueue, WorkflowActivity, WorkflowEnactment y WorkflowError.

Procedimiento

1. Vaya a **Recursos** > **JMS** > **Proveedores JMS**;
2. Seleccione el enlace del **proveedor de mensajería predeterminado**;
3. Seleccione el enlace **Especificaciones de activación** del apartado **Propiedades adicionales**;
4. Cree una nueva especificación pulsando **Nueva** y establezca los siguientes campos:

   Nombre: <QueueName>

   Nombre JNDI: eis/ <*QueueName*> AS

   Tipo de destino: Cola

   Nombre JNDI de destino: jms/ <*QueueName*>

   Nombre de bus: CuramBus

   Alias de autenticación: igual que para el origen de datos `jdbc/curamdb` (p.ej. <*SERVERNAME*> /dbadmin)

   Deje todo lo demás como el valor por omisión y pulse **Aceptar** para añadir el puerto.

Resultados

Guarde los cambios en la configuración maestra tal como se describe en el apartado “Guardar la configuración maestra” en la página 25.

Configurar las especificaciones de activación de temas necesarias: Procedimiento

1. Al igual que con las especificaciones de activación de colas de la sección anterior, añada una especificación de activación nueva y establezca los campos siguientes:

   Nombre : CuramCacheInvalidationTopic

   Nombre JNDI: eis/CuramCacheInvalidationTopicAS

   Tipo de destino: tema

   Nombre JNDI de destino: jms/CuramCacheInvalidationTopic

   Nombre de bus : CuramBus

   Alias de autenticación: igual que para el origen de datos `jdbc/curamdb` (p.ej. *<SERVERNAME>* /dbadmin)
2. Deje todo lo demás como el valor por omisión y pulse **Aceptar** para aplicar los cambios;
3. Guarde los cambios en la configuración maestra tal como se describe en el apartado “Guardar la configuración maestra” en la página 25.

Configurar los archivos de registro históricos

Es posible configurar el número máximo de archivos de registro histórico mantenido por un servidor concreto. Para realizar esta acción:

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor que corresponda de la lista de servidores;
3. Seleccione **Registro y rastreo** desde la sección **Resolución de problemas**;
4. Seleccione **Registros JVM** de la lista **Propiedades generales**;
5. Cambie el valor del campo **Número máximo de archivos de registro histórico** por 30 para los archivos `System.out` y `System.err`;
6. Pulse en **Aceptar** para aplicar los cambios;
7. Guarde los cambios en la configuración maestra.

Después de la configuración

Tablas de bases de datos de bus de integración de servicios: Después de la configuración, es necesario crear manualmente tablas de bases de datos necesarias para el bus de integración de servicios. WebSphere Application Server proporciona un programa de utilidad para generar el SQL para la creación de estas tablas, el generador de DDL SIB.

El generador se puede ejecutar mediante el comando siguiente (p.ej., para Windows):

```
%WAS_HOME%\bin\sibDDLGenerator.bat
  -system sistema
  -platform plataforma
  -schema nombreusuario
  -database nombre_basedatos
  -user nombreusuario
  -statementend ;
  -create
```

Donde

- *sistema* es la base de datos que se va a utilizar, por ejemplo `oracle` o `db2`;
- *plataforma* es el sistema operativo, como por ejemplo `windows`, `unix` o `zos`;
- *nombreusuario* es el nombre de usuario necesario para acceder a la base de datos, tal y como se especifica en la propiedad `curam.db.username` de `Bootstrap.properties`;
- *nombre_basedatos* es el nombre de la base de datos a utilizar, tal y como se especifica en la propiedad `curam.db.name` de `Bootstrap.properties`.

Por ejemplo:

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

Este mandato será la salida de algunas sentencias SQL y esta salida deberá ejecutarse a continuación en la base de datos de destino.

Tablas de bases de datos del servicio temporizador: Después de la configuración, es necesario crear manualmente las tablas de base de datos necesarias para el servicio de temporizador. WebSphere Application Server proporciona el DDL para estas tablas en su directorio `WAS_HOME /Scheduler` .

Los archivos DDL que deben ejecutarse son *createTablespaceXXX.ddl* y *createSchemaXXX.ddl* en ese orden, donde *XXX* es el nombre del producto de base de datos de destino.

Cada archivo DDL contiene instrucciones adecuadas para ejecutar para la base de datos de destino.

Finalización

El servidor de aplicaciones está ahora configurado y listo para instalar una aplicación de IBM Cúram Social Program Management en él. Salga de la consola de administración y reinicie el servidor de aplicaciones de WebSphere utilizando los destinos descritos en "Inicio y detención de servidores WebSphere" en la página 14.

Despliegue manual de aplicaciones

Para instalar una aplicación empresarial en WebSphere Application Server, se puede utilizar la consola de administración. Los pasos siguientes describen cómo instalar una aplicación, un componente EJB o un módulo web utilizando la consola administrativa.

Nota: Una vez que se haya iniciado la instalación, debe utilizarse el botón **Cancelar** para salir si la instalación de la aplicación ha finalizado anormalmente. No es suficiente pasar simplemente a otra página de la consola administrativa sin antes pulsar **Cancelar** en una página de instalación de la aplicación.

1. Vaya a **Aplicaciones** > **Nuevas aplicaciones**;
2. Seleccione **Nueva aplicación empresarial**;
3. Pulse el botón de selección correspondiente y especifique el nombre completo de la vía de acceso del archivo de la aplicación de origen o del archivo EAR, opcionalmente mediante el botón **Examinar**, en el panel Vía de acceso a la nueva aplicación y pulse **Siguiente**;

La ubicación predeterminada para la aplicación de los archivos EAR es la siguiente:

```
%SERVER_DIR%/build/ear/WAS/Curam.ear
```

4. Seleccione el botón **Vía de acceso rápido-Solicitud sólo cuando se necesita información adicional** del panel ¿Cómo desea instalar la aplicación? y pulse **Siguiente**;
5. Deje los valores por omisión tal como están para el paso 1, *Seleccionar las opciones de instalación* y pulse **Siguiente**;
6. En el paso 2, **Correlacionar módulos con servidores**, para cada módulo de la lista seleccione un servidor de destino o un clúster de la lista **Clústeres y servidores**. Para ello, marque el recuadro de selección situado junto a los módulos determinados y, a continuación, seleccione el servidor o el clúster y pulse **Aplicar**.
7. En el/los paso(s) siguiente(s), pulse **Siguiente** y luego pulse **Terminar** para finalizar la instalación. Este paso puede durar unos minutos y debe finalizar con el mensaje *La aplicación Curam se ha instalado satisfactoriamente*.
8. Guarde los cambios en la configuración maestra. (Consulte "Guardar la configuración maestra" en la página 25 para obtener información detallada).
9. Vaya a **Aplicaciones** > **Tipos de aplicación** > **Aplicaciones empresariales de WebSphere** y seleccione la aplicación recién instalada.
10. Seleccione la opción **Carga de clases y detección de actualizaciones** desde el apartado **Propiedades detalladas**.
11. Establezca el **Orden del cargador de clase** en **Clases cargadas con cargador de clases local primero (padre última)**.
12. Establezca la **Política del cargador de clases WAR** como **Cargador de una sola clase para la aplicación**.
13. Pulse en **Aceptar**.
14. Vaya a **Usuarios y grupos ->Gestionar usuarios**. Pulse en **Crear...** y especifique un ID de usuario, una contraseña, nombre y apellidos. A continuación, pulse en **Crear**.

    Consulte el apartado "Cambiar el nombre de usuario SYSTEM" en la página 16 para obtener más información sobre las credenciales que espera aquí la aplicación y sobre cómo cambiarlas.
15. Vuelva a la aplicación empresarial (**Aplicaciones** > **Tipos de aplicaciones** > **Aplicaciones empresariales WebSphere**, seleccione la aplicación recién instalada) y seleccione la opción **Rol de seguridad para la correlación de usuarios/grupos** desde el apartado **Propiedades detalladas** y correlacione el rol mdbuser con un nombre de usuario y una contraseña como con estos pasos:

    Nota: El nombre de usuario que se utiliza para correlacionar con el rol mdbuser ya debe estar definido en el registro de usuarios.

    a. Marque **Seleccionar** para el rol mdbuser y pulse **Correlacionar usuarios...**;
    b. Escriba el nombre de usuario apropiado en el campo **Buscar serie** y pulse **Buscar**;
    c. Seleccione el ID de la lista **Disponibles:** y pulse **>>** para añadirlo a la lista **Seleccionados:** y pulse **Aceptar**.
    d. Pulse en **Aceptar**.
16. Tras correlacionar el rol mdbuser ahora puede actualizar el rol RunAs de usuario seleccionando la opción **Roles RunAs de usuario** desde el apartado **Propiedades detalladas**.

17. Escriba un nombre de usuario y una contraseña correctos en los campos **nombre_usuario** y **contraseña**, respectivamente. Marque **Seleccionar** como rol mdbuser y pulse en **Aplicar**.
18. Pulse en **Aceptar**.
19. Guarde los cambios en la configuración maestra.
20. Después del despliegue es necesario iniciar la aplicación antes de que se pueda utilizar. Vaya a **Aplicaciones** > **Tipos de aplicación** > **Aplicaciones empresariales de WebSphere**, marque el recuadro de selección para la aplicación recién instalada y pulse en el botón **Iniciar**. Este paso puede durar unos minutos y debe terminar con el cambio del estado de la aplicación para indicar que se ha iniciado.
21. Finalmente, pruebe el despliegue de la aplicación. Por ejemplo, ponga en un navegador web el URL de la aplicación desplegada, p. ej. `https://localhost:9044/Curam`.

Despliegue de la red WebSphere

El despliegue de la red WebSphere Application Server de IBM ofrece servicios avanzados de despliegue que incluyen la agrupación en clúster, los servicios perimetrales y la alta disponibilidad para las configuraciones distribuidas. La publicación *Cúram Third Party Tools Guía de instalación* contiene más información sobre la instalación del despliegue de red de WebSphere.

Creación de perfiles

Después de instalar el despliegue de la red WebSphere, es necesario en la mayoría de los casos crear al menos dos perfiles. Una actuará como gestor de despliegue para el nodo y el resto como servidores federados.

Esto se realiza mediante el asistente de creación de perfiles, que se inicia a través del archivo `porc<hardware platform>` del directorio `bin/ProfileCreator` de la instalación de WebSphere Application Server.

La primera opción de este asistente es crear uno de estos elementos:

1. Un perfil de gestor de despliegue ; o
2. Un perfil de servidor de aplicaciones.

El segundo es la opción para habilitar la seguridad administrativa. Se recomienda habilitar la seguridad administrativa en la creación del perfil. Estos valores se pueden cambiar posteriormente.

Federación de un nodo

La federación de un perfil de servidor de aplicaciones requiere que se inicie el gestor de despliegue de destino.

El gestor de despliegue puede iniciarse ejecutando el mandato siguiente desde el directorio `profiles/<deployment manager profile name>/bin` de la instalación de despliegue de red WebSphere:

```
startServer dmgr
```

Para añadir el perfil de servidor de aplicaciones en el nodo del Gestor de despliegue se utiliza el mandato siguiente desde el directorio `profiles/<Application Server profile name>/bin` de la instalación de WebSphere Application Server:

```
addNode <deploymgr host> <deploymgr port>
```

Donde *<deploymgr host>* y *<deploymgr port>* son el host y el port de escucha para el conector SOAP del Gestor de despliegue. Los detalles del conector SOAP pueden encontrarse en la consola administrativa del gestor de despliegue aquí:

1. Vaya a **Servidores** > **Tipos de servidor** > **Servidores de aplicación WebSphere**;
2. Seleccione el servidor que corresponda de la lista;
3. Expanda **Puertos** en el apartado **Comunicaciones** y pulse en el botón **Detalles**;
4. Los detalles necesarios se muestran como **Host** y **Puerto** para **SOAP_CONNECTOR_ADDRESS**.

Configuración de un nodo

Antes de desplegar una aplicación en el nodo registrado, el primer servidor debe estar configurado. Esto se realiza a través de la consola de administración del gestor de despliegue, y la configuración se sincroniza con los servidores federados del nodo.

El agente de nodo, que permite la comunicación entre el gestor de despliegue y sus servidores federados, debe iniciarse. Esto debe hacerse con el mandato `startNode.bat` o `startNode.sh` en el directorio `profiles/<federated profile name>/bin` de la instalación de WebSphere Application Server.

Después de que el agente de nodo se inicia, todo el control se entrega al gestor de despliegue para los servidores de este nodo. Para iniciar o detener un servidor en la consola de administración del gestor de despliegue:

1. Vaya a **Servidores** > **Tipos de servidor** > **servidores de aplicaciones de WebSphere**;
2. Marque en la lista el servidor que se va a iniciar/detener y pulse en el botón **Iniciar** o **Detener** según sea necesario.

El siguiente paso del proceso consiste en configurar los servidores federados. Como se ha mencionado antes, toda la configuración se realiza mediante el gestor de despliegue de la consola administrativa. “Configuración manual de WebSphere Application Server” en la página 18 describe la configuración manual de WebSphere Application Server para una instalación básica y debe seguirse con las diferencias que se identifican a continuación. Al guardar la configuración maestra, asegúrese de forzar manualmente la sincronización a través de la consola administrativa:

1. Vaya a **Administración del sistema** > **Guardar cambios en el depósito maestro**;
2. Marque el recuadro de selección **Sincronizar cambios con nodos**;
3. Pulse el botón **Guardar**. La sincronización puede tardar algún tiempo;
4. Compruebe si se ha completado la sincronización en los registros del sistema y/o WebSphere Application Server. Estos mensajes pueden variar de un release a otro de WebSphere Application Server, pero debe buscar algo como esto:

```
ADMS0208I: Se ha completado la sincronización de la configuración para la celda.
```

   Una vez que la sincronización se complete, revise el estado del servidor y varios registros de WebSphere Application Server para garantizar el éxito;

“Configurar la seguridad de administración” en la página 25 detalla la configuración de seguridad necesaria durante la configuración manual. Esta configuración requiere copiar el archivo `Registry.jar` en un directorio dentro de la

instalación de WebSphere Application Server. El archivo `Registry.jar` debe copiarse desde `CuramSDEJ/lib` al directorio `lib` de la instalación del Gestor de despliegue y las instalaciones federadas.

"Configurar la seguridad de administración" en la página 25 esta configuración de seguridad también requiere copiar `CryptoConfig.jar` al directorio `java/jre/lib/ext` de la instalación de WebSphere Application Server. `CryptoConfig.jar` deberá copiarse en la misma estructura de directorios que cualquier otra instalación de WebSphere Application Server del entorno.

Nota: Antes de crear `Curam.ear` para el despliegue vale la pena anotar la dirección *BOOTSTRAP_ADDRESS* del servidor en el que estos se instalarán. *BOOTSTRAP_ADDRESS* se encuentra en la misma lista de puertos que *SOAP_CONNECTOR_ADDRESS* descritas anteriormente.

De forma predeterminada, la dirección *BOOTSTRAP_ADDRESS* esperada por la aplicación es 2809. Para solucionar este problema cambie esta dirección alternativa o la propiedad relevante en su archivo `AppServer.properties`.

La propiedad que debe cambiarse es el valor curam.server.port del archivo `AppServer.properties`. Cambiar esta afecta al valor de puerto en el archivo `web.xml` cuando se crea un archivo EAR. Para obtener más información sobre el archivo `web.xml` consulte la *Cúram Web Client Reference Manual*.

Despliegue en el nodo

Por último, debe seguirse "Despliegue manual de aplicaciones" en la página 39 para desplegar manualmente las aplicaciones en el servidor necesario. Entonces se pueden iniciar o detener las aplicaciones usando la consola administrativa del gestor de despliegue.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los Estados Unidos. Es posible que IBM no ofrezca los productos, servicios o características que se describen en este documento en otros países. Póngase en contacto con el representante local de IBM para obtener información acerca de los productos y servicios que actualmente están disponibles en su zona. Las referencias a programas, productos o servicios de IBM no pretenden establecer ni implicar que sólo puedan utilizarse dichos productos, programas o servicios de IBM. En su lugar, se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM. IBM puede tener patentes o aplicaciones pendientes de patente que conciernan al tema descrito en este documento. La entrega de este documento no le otorga ninguna licencia sobre dichas patentes.. Puede enviar consultas sobre licencias, por escrito, a:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

Para consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

Intellectual Property Licensing

Legal and Intellectual Property Law.

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japón

El siguiente párrafo no se aplica al Reino Unido ni a ningún otro país en las que tales provisiones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, SEA EXPRESA O IMPLÍCITA, INCLUIDAS, AUNQUE SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO CONTRAVENCIÓN, COMERCIABILIDAD O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunos estados no permiten la renuncia de garantías explícitas o implícitas en determinadas transacciones, por lo que es posible que este párrafo no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectuarán cambios en la información aquí contenida; dichos

cambios se incorporarán en las nuevas ediciones de la publicación. BM puede realizar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias en esta información a sitios web que no son de IBM se proporcionan sólo para su comodidad y de ninguna manera constituyen una aprobación de estos sitios web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto y el uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

IBM puede utilizar o distribuir la información que se le suministre del modo que estime oportuno, sin incurrir por ello en ninguna obligación con el remitente. Los titulares de licencias de este programa que deseen tener información sobre el mismo con el fin de: (i) intercambiar información entre programas creados de forma independiente y otros programas (incluido éste) y (ii) utilizar mutuamente la información que se ha intercambiado, deberán ponerse en contacto con:

IBM Corporation

Dept F6, Bldg 1

294 Route 100

Somers NY 10589-3216

U.S.A.

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, incluyendo en algunos casos el pago de una tasa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia que se encuentra disponible para el programa se proporcionan de acuerdo con los términos del Acuerdo del Cliente de IBM, el Acuerdo Internacional de Licencia de Programas o cualquier acuerdo equivalente entre IBM y el Cliente.

Cualquier dato relacionado con el rendimiento que aquí se presente se ha obtenido en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos pueden variar significativamente. Es posible que algunas medidas se hayan tomado en sistemas que se están desarrollando y no se puede garantizar que dichas medidas serán iguales en los sistemas disponibles en general. Además, es posible que algunas mediciones se haya estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información referente a productos que no son de IBM se ha obtenido de los proveedores de esos productos, de sus anuncios publicados o de otras fuentes disponibles.

IBM no ha probado tales productos y no puede confirmar la precisión de su rendimiento, su compatibilidad ni ningún otro aspecto relacionado con productos que no son de IBM. Las preguntas relacionadas con las posibilidades de los productos que no son de IBM deben dirigirse a los proveedores de tales productos.

Todas las sentencias relativas a la dirección o intención futura de IBM están sujetas a modificación o retirada sin previo aviso, y sólo representan objetivos.

Todos los precios de IBM que se muestran son precios actuales de venta al por menor sugeridos por IBM y están sujetos a modificaciones sin previo aviso. Los precios del intermediario podrían variar.

Esta información se utiliza a efectos de planificación. iar antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos pueden incluir nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier similitud con nombres y direcciones utilizados por una empresa real es totalmente fortuita.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente que ilustran técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir los programas de ejemplo de cualquier forma, sin tener que pagar a IBM, con intención de desarrollar, utilizar, comercializar o distribuir programas de aplicación que estén en conformidad con la interfaz de programación de aplicaciones (API) de la plataforma operativa para la que están escritos los programas de ejemplo. Estos ejemplos no se han probado en profundidad bajo todas las condiciones. En consecuencia, IBM no puede garantizar ni afirmar la fiabilidad, utilidad o funcionalidad de estos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin ningún tipo de garantía. IBM no asumirá ninguna responsabilidad por daños ocasionados por el uso de los programas de ejemplo.

Cada copia o parte de estos programas de ejemplo o cualquier trabajo derivado de los mismos, debe incluir un aviso de copyright como el siguiente:

© (nombre de la empresa) (año). Algunas partes de este código se derivan de programas de ejemplo de IBM Corp.

© opyright IBM Corp. _especifique el año o años_. Reservados todos los derechos.

Si visualiza esta información en una copia software, es posible que no aparezcan las fotografías ni las ilustraciones en color.

Consideraciones sobre la política de privacidad

Los productos de IBM Software, incluidas las soluciones de software como servicio (“Ofertas de software”) pueden utilizar cookies u otras tecnologías para recabar información de uso del producto, ayudar a mejorar la experiencia del usuario final, adaptar las interacciones con el usuario final u otros fines. En muchos casos, las Ofertas de software no recopilan información de identificación personal. Algunas de nuestras Ofertas de software pueden ayudar a recabar información de identificación personal. Si esta Oferta de software utiliza cookies para recabar información de identificación personal, a continuación se expone información específica sobre el uso de cookies de esta oferta.

Dependiendo de las configuraciones desplegadas, esta Oferta de software podrá utilizar cookies de sesión u otras tecnologías similares que recaben el nombre, la contraseña u otra información de identificación personal a efectos de gestión de la sesión, autenticación, usabilidad de usuario mejorada, configuración de un inicio

de sesión único u otros fines de seguimiento del uso y/o funcionales. Dichas cookies o tecnologías similares no se pueden inhabilitar.

Si las configuraciones desplegadas para esta Oferta de software le proporcionan a usted como cliente la capacidad de recabar información de identificación personal de usuarios finales por medio de cookies y otras tecnologías, deberá buscar su propio asesoramiento legal relativo a las leyes aplicables a dicha recopilación de datos, incluyendo cualquier requisito de aviso y consentimiento.

Para obtener información adicional relativa al uso de diversas tecnologías, incluidas las cookies, a tales fines, consulte la política de privacidad de IBM en http://www.ibm.com/privacy y la declaración de privacidad en línea de IBM en http://www.ibm.com/privacy/details, las secciones tituladas “Cookies, balizas web y otras tecnologías” y “Declaración de privacidad de los productos software y del software como servicio de IBM” en http://www.ibm.com/software/info/product-privacy.

Marcas registradas

IBM, el logotipo de IBM e ibm.com son marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM u otras empresas. Encontrará una lista actual de marcas registradas de IBM en la web en "Copyright and trademark information" en http://www.ibm.com/legal/us/en/copytrade.shtml.

Apache es una marca registrada de Apache Software Foundation.

Microsoft y Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Oracle, Java y todas las marcas registradas y logotipos basados en Java son marcas registradas de Oracle y/o sus filiales.

Otros nombres pueden ser marcas registradas de sus respectivos propietarios. Otros nombres de empresas, productos o servicios pueden ser marcas registradas o de servicio de terceros.

Impreso en España