

IBM Cúram Social Program Management  
Versión 6.0.5

*Cúram - Guía de despliegue para  
WebSphere Application Server en z/OS*

**IBM**

**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 51

**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.

Materiales bajo licencia - Propiedad de IBM.

© Copyright IBM Corporation 2012, 2013.

© Cúram Software Limited. 2011. Reservados todos los derechos.

# Contenido

**Figuras . . . . . v**

**Tablas . . . . . vii**

## Despliegue de IBM WebSphere

**Application Server en z/OS . . . . . 1**

Introducción . . . . . 1

    Visión general . . . . . 1

    Supuestos . . . . . 1

    Convenciones de documentos . . . . . 2

Herramientas de otros fabricantes . . . . . 2

    Introducción . . . . . 2

    Antes de la instalación . . . . . 2

    DB2 para z/OS . . . . . 3

        Versiones soportadas . . . . . 3

        Requisitos previos . . . . . 3

        Instalación . . . . . 3

        Tareas posteriores a la instalación . . . . . 3

    WebSphere Application Server para z/OS . . . . . 4

        Versiones soportadas . . . . . 4

        Requisitos previos . . . . . 4

        Instalación . . . . . 4

        Tareas posteriores a la instalación . . . . . 5

    Apache Ant . . . . . 5

        Descripción general . . . . . 5

        Versiones soportadas . . . . . 5

        Instalación . . . . . 5

        Tareas posteriores a la instalación . . . . . 6

    JRE y Java EE . . . . . 6

        Descripción general . . . . . 6

        Versiones soportadas . . . . . 6

        Instalación . . . . . 6

        Tareas posteriores a la instalación . . . . . 6

Creación de archivos EAR . . . . . 6

    Introducción . . . . . 6

    Notas específicas de z/OS para generar archivos

    EAR . . . . . 7

        Archivos de propiedades . . . . . 7

    Empaquetado del tiempo de ejecución de Cúram

    para la instalación en z/OS . . . . . 9

Configuración del servidor de aplicaciones . . . . . 10

    Introducción . . . . . 10

    Configuración de WebSphere Application Server . . . . . 10

        Ubicaciones alternativas del archivo JAR . . . . . 12

    Configuración de seguridad . . . . . 13

        Configuración de SAF (RACF) . . . . . 13

        Pasos de configuración especiales al usar sólo

        identidad y LDAP . . . . . 13

        Registro de usuarios de WebSphere

        Application Server . . . . . 15

        Registro del proceso de autenticación . . . . . 16

        Establecimiento de un delimitador de nombre

        de usuario de exclusión alternativo . . . . . 16

        Comportamiento de almacenamiento

        intermedio de WebSphere Application Server . . . . . 16

        Propiedades personalizadas de seguridad . . . . . 16

        Medidas de endurecimiento de la seguridad . . . . . 17

        Cifrado de Cúram . . . . . 17

    Modalidad de 64 bits . . . . . 17

    Configuración de huso horario . . . . . 18

    Inicio y detención de servidores WebSphere . . . . . 18

        Iniciar un servidor WebSphere . . . . . 18

        Detener un servidor WebSphere . . . . . 18

        Reiniciar un servidor WebSphere . . . . . 19

Despliegue . . . . . 19

    Introducción . . . . . 19

    Archivos de propiedades . . . . . 19

        Bootstrap.properties . . . . . 19

        AppServer.properties . . . . . 20

        Comprobación de la configuración . . . . . 20

    Despliegue . . . . . 21

        Instalar una aplicación . . . . . 21

        Cambiar el nombre de usuario SYSTEM . . . . . 21

        Desinstalar una aplicación . . . . . 22

    Precompilación de las JSP . . . . . 22

    Creación de una base de datos . . . . . 23

    Prueba del despliegue . . . . . 23

        Utilización de IBM WebSphere Application

        Server con USGCB . . . . . 23

Configuración manual de WebSphere Application

Server . . . . . 24

    Introducción . . . . . 24

    Configuración manual de WebSphere Application

    Server . . . . . 24

        La consola administrativa . . . . . 24

        Soporte para scripts . . . . . 25

        Creación del alias de inicio de sesión del

        origen de la base de datos . . . . . 26

        Configurar DB2 para los orígenes de datos

        z/OS . . . . . 26

        Guardar la configuración maestra . . . . . 30

        Configurar la seguridad de administración . . . . . 30

        Reiniciar el servidor de aplicaciones . . . . . 31

        Probar la conexión de DB2 para z/OS . . . . . 32

        Configurar usuarios . . . . . 32

        Configurar el módulo de inicio de sesión

        JAAS del sistema . . . . . 32

        Configuración del servidor . . . . . 35

        Configuración del bus . . . . . 39

        Configuración JMS . . . . . 40

        Después de la configuración . . . . . 44

        Finalización . . . . . 45

Despliegue manual de aplicaciones . . . . . 45

Despliegue de la red WebSphere . . . . . 47

    Sugerencias para trabajar con el despliegue de

    la red WebSphere . . . . . 47

    Configuración de un nodo . . . . . 48

    Despliegue en el nodo . . . . . 49

**Avisos . . . . . 51**  
Consideraciones sobre la política de privacidad . . . 53

Marcas registradas . . . . . 54

---

## Figuras

|    |   |    |    |   |    |
|----|---|----|----|---|----|
| 1. | Archivo de propiedades AppServer de ejemplo                     | 11 | 6. | Ejemplo de uso  | 21 |
| 2. | Ejemplo de uso  | 18 | 7. | Ejemplo de uso  | 22 |
| 3. | Ejemplo de uso  | 18 | 8. | Ejemplo de uso  | 22 |
| 4. | Archivo de propiedades Bootstrap relacionadas con el despliegue | 20 | 9. | Mandatos de shell de ejemplo para crear una base de datos | 23 |
| 5. | Archivo de propiedades AppServer relacionadas con el despliegue | 20 |    |   |    |



---

## Tablas

|    |   |    |
|----|---|----|
| 1. | Propiedades de la base de datos específicas de z/OS para DB2. . . . .                         | 7  |
| 2. | Propiedades que dependen del sistema de archivos z/OS . . . . .                               | 8  |
| 3. | Propiedades de puerto relacionadas con WebSphere Application Server para z/OS. . . . .        | 8  |
| 4. | Propiedades relacionadas con la estructura de WebSphere Application Server para z/OS. . . . . | 9  |
| 5. | Variables de entorno de UNIX System Services z/OS . . . . .                                   | 9  |
| 6. | Propiedades personalizadas de CuramLoginModule . . . . .                                      | 33 |
| 7. | Valores de destino de excepción. . . . .  | 42 |





---

# Despliegue de IBM WebSphere Application Server en z/OS

Se necesitan una serie de herramientas de terceros para desplegar IBM Cúram Social Program Management en IBM WebSphere Application Server para IBM z/OS. Para desplegar la aplicación se necesitan los archivos ear de aplicación y servidor de Webclient.

---

## Introducción

### Visión general

Esta guía describe el proceso de configuración y despliegue de IBM® Cúram Social Program Management con IBM WebSphere Application Server para IBM z/OS. Para obtener detalles exactos sobre las versiones soportadas, consulte el documento *Requisitos previos soportados de Cúram*.

Las tareas de configuración se puede resumir como sigue:

1. Instalar y configurar herramientas de terceros necesarias;
2. Configurar WebSphere Application Server para z/OS para los archivos .ear (Enterprise ARchive) de la aplicación IBM Cúram Social Program Management;
3. Crear y empaquetar los archivos .ear de la aplicación.  
Los archivos .ear se crean por separado (en una plataforma Microsoft Windows o UNIX);
4. Desplegar la aplicación IBM Cúram Social Program Management y el cliente web; los pasos implicados son los siguientes:
  - Establecimiento de los archivos de propiedades;
  - Instalacion de los archivos .ear de la aplicación;
  - Creación de una base de datos;
  - Pre-compilación de JSP (opcional);
  - Prueba de despliegue.

WebSphere Application Server para z/OS puede personalizarse y configurarse en una serie de maneras para mejorar el rendimiento, los recursos, la seguridad y por otros motivos. Este documento ilustra un enfoque simple y de un solo servidor para la configuración de WebSphere Application Server para z/OS que pueden no ser adecuados para la instalación.

### Supuestos

Cualquier equipo o individuo que utilice este documento debe tener conocimientos razonables y la experiencia sobre una amplia gama de productos, tecnologías, etc. de z/OS. Consulte la publicación *Directorio de programas para WebSphere Application Server para z/OS 7.0 (GI11-4295)* y la documentación relacionada para obtener más información.

La instalación y la personalización de WebSphere Application Server para z/OS y, y su software relacionado y basado en z/OS no se aborda; sin embargo los pasos específicos necesarios para IBM Cúram Social Program Management son tratados en este documento.

Puede que se requiera una mayor personalización específica del cliente, por ejemplo:

- Dependiendo de sus requisitos de seguridad local (p. ej. IBM RACF) es posible que deba realizar requisitos adicionales de configuración y personalización.

## Convenciones de documentos

En este documento se utilizan varios convenios:

- Los valores entre corchetes, por ejemplo, `<WebSphere Configuration Directory>`; consulte las sustituciones para las que debe proporcionar valores.
- Navegación en la consola administrativa de WebSphere Application Server para z/OS:
  - “Navegar” hace referencia a las selecciones realizadas mediante el control de árbol del panel izquierdo de la ventana del navegador y que aparecen así: **Servidores > Servidores de aplicación.**
  - “Seleccionar” hace referencia a los hipervínculos que aparecen en la ventana del navegador y que se muestran en este documento en cursiva; por ejemplo, *local\_host*.
  - “Pulsar” hace referencia a botones como **Aceptar** y **Siguiente**.
  - “Marcar” o “Seleccionar” hace referencia a los recuadros de selección o a las opciones que debe seleccionar; por ejemplo, marcar la opción **Forzar Java 2 Security**.

---

## Herramientas de otros fabricantes

### Introducción

Para poder utilizar la aplicación de gestión de IBM Cúram Social Program es necesario instalar y configurar el software de terceros. En el documento *Cúram Supported Prerequisites* se pueden encontrar detalles exactos para estos productos.

Queda fuera del ámbito de un documento como este proporcionar datos e instrucciones detallados sobre la instalación y la configuración de todos los productos de software de **z/OS** necesarios para dar soporte a WebSphere Application Server para z/OS y DB2 para z/OS. Este capítulo sólo intenta dar detalles breves de la configuración mínima necesaria para cada producto.

Las secciones siguientes describen los requisitos previos, las notas de instalación y/o las actividades de configuración posteriores a la instalación para cada uno de los siguientes elementos:

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

Una vez que se han instalado y configurado las herramientas de otros proveedores, el sistema quedará listo para la configuración de WebSphere Application Server para z/OS.

### Antes de la instalación

Además de la información de los manuales *Directorio de programas para WebSphere Application Server para z/OS V7.0 (GI11-4295)* y *IBM WebSphere Application Server*

para z/OS, Versión V7.0: *Instalación del entorno de aplicaciones Centro de información de WebSphere Application Server, Versión V7.0.* , para z/OS se recomienda lo siguiente:

- Almacenamiento principal: adecuado para ejecutar sus aplicaciones, incluir el número de usuarios, los requisitos de rendimiento, etc.
- Espacio del sistema de archivos: deje espacio adicional en su sistema de archivos de UNIX System Services para el entorno de Cúram y para el despliegue en la configuración de WebSphere Application Server para z/OS.

## DB2 para z/OS

### Versiones soportadas

Las versiones exactas de DB2 que deben instalarse están listadas en el documento *Requisitos previos soportados de Cúram*.

### Requisitos previos

Consulte el *Directorio de programa para IBM DB2 8 Universal Database para z/OS versión 8 (GI10-8566) y a versión 9 (GI10-8737)*.

### Instalación

Antes de empezar con la configuración e instalación de Cúram se da por supuesto que DB2 para z/OS ha sido instalado satisfactoriamente utilizando SMP/E, y que la instalación se ha configurado utilizando los paneles de personalización ISPF según los requisitos de su instalación.

Necesitará la siguiente información para desplegar la aplicación de archivos .ear:

1. Nombre de ubicación = <Nombre de ubicación de DB2> - Especifica el nombre de la ubicación de DB2 para z/OS. El nombre de ubicación debe mostrarse en el registro del sistema z/OS durante el inicio de DB2 para z/OS (DDF):  
DSNL004I - DDF START COMPLETE  
LOCATION <Nombre de ubicación de DB2>
2. ID de usuario = <nombre de usuario de base de datos> - Representa un ID de usuario de z/OS que tiene todo el acceso de seguridad necesario habilitado para conectarse con y gestionar la base de datos DB2 para z/OS;
3. Contraseña = <contraseña de la base de datos> - Es la contraseña para <nombre de usuario de la base de datos>.

### Tareas posteriores a la instalación

#### Acerca de esta tarea

Los pasos siguientes pueden ejecutarse utilizando interfaces z/OS DB2 típicas; por ejemplo, SPUFI, DB2 Connect o DB2 por lotes. Proporcione valores adecuados del sitio para sustituir los valores entre corchetes (<storage\_group>):

#### Procedimiento

1. Cree el grupo de almacenamiento de bases de datos necesario.  
CREATE STOGROUP <storage\_group> VOLUMES (<volumes>  
VCAT <catalog\_name>;
2. Cree la base de datos de la aplicación Cúram: la base de datos puede ser configurada para la modalidad EBCDIC,ASCIIoUNICODE; esto puede realizarse al crear la base de datos utilizando la palabra clave CCSID. Para la bases de datos ASCII oUNICODE consulte el apartado "Propiedades de programa de arranque" en la página 7 para obtener más información sobre el establecimiento de la propiedad necesaria curam.db.zos.encoding.

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

3. Asegúrese de que el parámetro DSNZPARM RRULOCK, de la macro DSN6SPRM, esté establecido en YES.
4. Debe crearse una variable de entorno denominada DB2JCC\_LICENSE\_CISUZ\_JAR en su entorno de shell UNIX System Services z/OS que apunte al archivo jar de licencia de DB2 z/OS instalado utilizado para la conectividad con DB2 para los servidores z/OS en z/OS. Esta se suele denominar db2jcc\_license\_cisuz.jar y se proporciona como parte de la instalación de DB2 para z/OS.

## Resultados

### Nota:

Puede que los valores del módulo de parámetros DSNZPARM necesiten un ajuste para ser compatibles con Cúram. Un parámetro de especial interés es el umbral de vencimiento del tiempo de espera de una transacción desocupada (IDTHTOIN). Puede que deba incrementarse para determinadas actividades CER relacionadas con la inicialización tras una construcción de base de datos como, por ejemplo, el destino Ant prepare application data, porque puede ejecutar más tiempo de lo normal en aplicaciones con DB2 para z/OS. El tiempo que puedan requerir dichas actividades, y si se vence o no el tiempo de espera, dependerá de diversos factores, pero un síntoma indicativo de que este cambio puede ser necesario es el que se manifiesta en el shell del cliente cuando se recibe un error similar a este:

```
[java] infrastructure:RUN_ID_RUNTIME: Se ha producido una excepción en tiempo de ejecución:
[jcc][t4][10335][10366][3.63.131] Operación no válida: se ha cerrado la conexión.
ERRORCODE=-4470, SQLSTATE=08003.
```

Asimismo, puede que DB2 produzca en el SYSLOG de z/OS un mensaje de agotamiento del tiempo de espera DSNL027I con un código de razón de 00D3003B en la misma ventana temporal. La correspondiente documentación de DB2 para z/OS proporciona información sobre cómo cambiar el valor del tiempo de espera de los hilos desocupados.

## WebSphere Application Server para z/OS

### Versiones soportadas

Las versiones exactas de WebSphere Application Server para z/OS que deben instalarse están listadas en el documento *Requisitos previos soportados de Cúram*.

### Requisitos previos

Consulte el *Directorio de programas para WebSphere Application Server para z/OS V7.0 (GI11-4295)* de WebSphere Application Server para ver los requisitos específicos de z/OS.

### Instalación

Antes de empezar con la configuración y el despliegue de Cúram se da por supuesto que WebSphere Application Server para z/OS ha sido instalado satisfactoriamente utilizando las herramientas de instalación adecuadas a su sitio y a los requisitos de WebSphere Application Server para z/OS.

La instalación de WebSphere Application Server para z/OS se cubre en diversas publicaciones de IBM y en el Documentación de producto de WebSphere

Application Server, Versión V7.0. Sin embargo, la seguridad global requiere más información, así que la ampliamos a continuación.

**Seguridad global: configuración de los valores de seguridad:** La activación de la seguridad global de WebSphere Application Server para z/OS ha sido descrita como activar un gran interruptor, y esto va a afectar al comportamiento del sistema WebSphere Application Server para z/OS significativamente. Por este motivo se recomienda encarecidamente:

- Familiarizarse con la documentación de WebSphere Application Server para z/OS en materia de seguridad. Específicamente, debe consultar:
  - Temas de Seguridad del *Centro de información de WebSphere Application Server para z/OS*;
  - IBM WebSphere Application Server for z/OS, Version V7.0: Protección de aplicaciones y de su entorno

Tenga en cuenta que si tiene otras aplicaciones que se ejecutan en WebSphere Application Server para z/OS, se verán afectadas cuando se active la seguridad global y es posible que ya no funcionen.

### Tareas posteriores a la instalación

Debe realizarse el paso siguiente:

- Debe crearse una variable de entorno denominada WAS\_HOME en su entorno de shell UNIX System Services z/OS. Debe establecerse en el directorio AppServer del servidor de Application Server para la instalación de z/OS (/WebSphere/AppServer).

## Apache Ant

### Descripción general

Apache Ant es una herramienta basada en Java. Para las personas familiarizadas con las herramientas que se utilizan en otros entornos puede considerarse como similar a la herramienta de la marca.

### Versiones soportadas

Las versiones exactas de Ant que deben instalarse están listadas en el documento *Requisitos previos soportados de Cúram*.

### Instalación

El archivo ZIP puede obtenerse a partir de Apache Ant y extraerse en una carpeta en la máquina como se indica a continuación:

- Coloque el archivo ZIP de Ant en el sistema de archivos de z/OS UNIX System Services (p. ej. /usr/local) y procese el archivo; por ejemplo:

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

Donde "<version>" representa la versión correspondiente identificada en el documento *Requisitos previos soportados de Cúram v6.0*.

- Asegúrese de que el script Ant en apache-ant-<version>/bin sea el siguiente:

- En el formato EBCDIC ; por ejemplo:

```
iconv -t IBM-1047 -f IS08859-1 apache-ant-<version>/bin/ant \
> /tmp/ant
mv /tmp/ant apache-ant-<version>/bin
```

- Ejecutable; por ejemplo:

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

## Tareas posteriores a la instalación

### Acerca de esta tarea

Los pasos siguientes deben realizarse:

#### Procedimiento

1. Debe crearse una variable de entorno denominada ANT\_HOME en su entorno de shell UNIX System Services z/OS que apunte al directorio de instalación elegido para Ant;
2. Añada \$ANT\_HOME/bin en la vía de acceso de ejecución a través de la variable de entorno UNIX System Services z/OS;
3. Cree una variable de entorno del sistema, ANT\_OPTS, en su entorno de shell UNIX System Services de z/OS, que debe establecerse al menos en -Xmx512m.

#### Resultados

Pruebe Ant ejecutando:

```
ant -version
```

Debería ver la versión y la fecha de compilación de Ant.

## JRE y Java EE

### Descripción general

Tanto el JRE como Java EE son necesarios.

### Versiones soportadas

Las versiones exactas que deben instalarse están listadas en el documento *Requisitos previos soportados de Cúram*.

### Instalación

No se proporcionan instrucciones de instalación específicas para JRE y Java EE en z/OS, ya que WebSphere Application Server para z/OS, Versión 7.0 proporciona un JRE y Java EE integrados, que se deben usar. Consulte la información correspondiente suministrada por IBM para su entorno concreto.

### Tareas posteriores a la instalación

- Debe crearse una variable de entorno denominada JAVA\_HOME en su entorno de shell UNIX System Services z/OS que apunte al JRE instalado. \$JAVA\_HOME debe establecerse en \$WAS\_HOME/java. \$JAVA\_HOME/bin debe colocarse en la vía de acceso a través de la variable de entorno \$PATH.
- Debe crearse una variable de entorno denominada J2EE\_JAR en su entorno de shell UNIX System Services z/OS que apunte al archivo jar de Java EE instalado. Este debe apuntar a \$WAS\_HOME/lib/j2ee.jar.

---

## Creación de archivos EAR

### Introducción

El paso principal antes del despliegue de una gestión de IBM Cúram Social Program consiste en empaquetar la aplicación en archivos EAR (Enterprise ARchive). Sin embargo, la creación de los archivos .ear de la aplicación no se

puede realizar para **z/OS**, sino que debe realizarse en Windows o cualquier otro entorno que se haya identificado como de posible creación en la publicación *Cúram Soportado Prerrequisitos*.

El resto de este capítulo describe los requisitos específicos de **z/OS** para crear archivos `.ear` compatibles con **z/OS**. Para obtener más detalles sobre la generación de archivos `.ear` de IBM Cúram Social Program Management, consulte el capítulo 2 de la publicación *Guía de despliegue de Cúram de WebSphere Application Server*. También puede encontrar información útil en los manuales siguientes:

- *Cúram Application Workshop Guide*: este manual contiene instrucciones de creación básicas para los archivos `.ear` de la aplicación;
- *Cúram Server Guía del desarrollador*: este manual contiene instrucciones detalladas para la generación de un servidor (capítulo 3);
- *Cúram Web Client Manual de referencia*: este manual contiene instrucciones detalladas para el desarrollo de clientes web, incluida la instalación y la configuración (capítulo 4);

## Notas específicas de z/OS para generar archivos EAR

Estas secciones resaltan información específica para generar archivos `.ear` compatibles con **z/OS**.

### Archivos de propiedades

Al crear una aplicación de IBM Cúram Social Program Management, deben configurarse correctamente los archivos `bootstrap.properties` y `AppServer.properties` para la plataforma **z/OS** de destino.

**Propiedades de programa de arranque:** El archivo `Bootstrap.properties` contiene las propiedades de configuración específicas de la máquina para obtener inicialmente una conexión con la base de datos. Preste atención específica a los elementos siguientes:

1. Propiedades de la base de datos:

*Tabla 1. Propiedades de la base de datos específicas de z/OS para DB2*

| Propiedad                                   | Notas   |
|---|---|
| <code>curam.db.type</code>                  | El valor debe establecerse en "zos".  |
| <code>curam.db.zos.enableforeignkeys</code> | Establézcalo de forma adecuada para el entorno ("true" o "false").  |
| <code>curam.db.zos.encoding</code>          | Especifica si la base de datos que se utiliza en <b>z/OS</b> requiere un proceso para EBCDIC, ASCII, o UNICODE. Esto debe establecerse en "EBCDIC", "ASCII" o "UNICODE" en función de la codificación correspondiente a la base de datos en uso. "EBCDIC" es el valor predeterminado. |
| <code>curam.db.zos.dbname</code>            | El valor debe ser el nombre de la base de datos DB2 para <b>z/OS</b> .  |
| <code>curam.db.zos.32ktablespace</code>     | El valor debe ser el nombre del espacio de tabla de 32 K DB2 para <b>z/OS</b> .   |
| <code>curam.db.username</code>              | El valor depende de la configuración del sistema <b>z/OS</b> tal como se describe en el apartado "DB2 para <b>z/OS</b> " en la página 3.  |

Tabla 1. Propiedades de la base de datos específicas de z/OS para DB2 (continuación)

| Propiedad           | Notas   |
|---------------------|---|
| curam.db.password   | El valor depende de la configuración del sistema z/OS tal como se describe en el apartado "DB2 para z/OS" en la página 3. Dado que esta es una contraseña cifrada, se debe generar ejecutando el destino de cifrado Ant en cualquier plataforma soportada; por ejemplo <code>cd \$CURAMSDEJ/bin; ant cifrar -Dpassword&lt;La contraseña para curam.db.username&gt;</code> |
| curam.db.name       | El valor es el nombre de ubicación de DB2 para z/OS como se describe en el apartado "DB2 para z/OS" en la página 3.   |
| curam.db.servername | El valor depende del sistema principal (o la dirección IP) de la DB2 para el sistema z/OS.  |
| curam.db.serverport | El valor depende de la configuración del sistema DB2 para z/OS.   |

2. Propiedades dependientes del sistema de archivos:

Tabla 2. Propiedades que dependen del sistema de archivos z/OS

| Propiedad                           | Notas  |
|-------------------------------------|--|
| curam.environment.bindings.location | El valor debe reflejar un directorio válido en el sistema de archivos de UNIX System Services z/OS de destino. |

**Propiedades de AppServer:** Preste atención específica a los elementos siguientes:

1. Las propiedades de WebSphere Application Server para z/OS relacionadas con el puerto se muestran en el apartado Tabla 3.

Tabla 3. Propiedades de puerto relacionadas con WebSphere Application Server para z/OS

| Propiedad                  | Notas  |
|----------------------------|--|
| curam.server.port          | El valor debe coincidir con el puerto de arranque de WebSphere Application Server para z/OS (consulte "Configurar el acceso al puerto" en la página 37). |
| curam.client.httpport      | El valor debe coincidir con el valor del puerto CuramClientEndPoint (consulte el apartado "Configurar el acceso al puerto" en la página 37).             |
| curam.webservices.httpport | El valor debe coincidir con el valor del puerto CuramWebServicesEndPoint (consulte el apartado "Configurar el acceso al puerto" en la página 37).        |

2. Las propiedades relacionadas con la estructura de WebSphere Application Server para z/OS se muestran en Tabla 4 en la página 9.



Tabla 4. Propiedades relacionadas con la estructura de WebSphere Application Server para z/OS

| Propiedad         | Notas   |
|-------------------|---|
| curam.server.host | El valor depende del sistema principal (o la dirección IP) de la DB2 para el sistema z/OS.                                    |
| curam.server.name | El valor debe coincidir con el nombre del destino de WebSphere Application Server para z/OS.                                  |
| cell.name         | El valor debe coincidir con el nombre de la celda WebSphere Application Server para z/OS de destino.                          |
| node.name         | El valor debe coincidir con el nombre del nodo de WebSphere Application Server para z/OS.                                     |
| profile.name      | Para WebSphere Application Server para z/OS el único nombre de perfil soportado es "default", que es el valor predeterminado. |

## Empaquetado del tiempo de ejecución de Cúram para la instalación en z/OS

Después de haber creado los archivos .ear debe empaquetar estos y el entorno de tiempo de ejecución para la instalación en z/OS.

Por ejemplo, en **Windows** (con su configuración de entorno según la publicación *Guía de despliegue de Cúram de WebSphere Application Server*) especifique estos mandatos:

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

Luego debe poner en **FTP** o copiar (**copy**) el archivo release.zip en la ubicación del sistema de archivos z/OS.

Para descomprimir el archivo release.zip en z/OS, debe establecer dos variables de entorno en su entorno de shell de UNIX System Services de z/OS para esta tarea y las tareas posteriores:

Tabla 5. Variables de entorno de UNIX System Services z/OS

| Variable de entorno | Valor   |
|---------------------|---|
| SERVER_DIR          | representa la ubicación en la que se va a descomprimir el archivo release.zip; por ejemplo: /curam/release. |
| CURAMSDEJ           | representa el directorio para ejecutar scripts de creación: \$CuramSDEJ.                                    |

Con release.zip en el sistema z/OS, en su entorno de shell entre los mandatos siguientes para descomprimirlo:

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

---

# Configuración del servidor de aplicaciones

## Introducción

En este capítulo se supone que WebSphere Application Server para z/OS ya se ha instalado en z/OS. Consulte “Herramientas de otros fabricantes” en la página 2 para obtener información específica de Cúram sobre la instalación de WebSphere Application Server para z/OS.

La configuración de WebSphere es similar en todas las plataformas, y hay una serie de destinos Ant disponibles para ayudar a configurar y gestionar la instalación. Para quienes estén interesados, “Configuración manual de WebSphere Application Server” en la página 24 detalla los pasos manuales realizados por los scripts de configuración.

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

**Nota:** En WebSphere Application Server para z/OS el perfil sólo está disponible en el perfil *por omisión*; no es posible ninguna otra opción.

El destino **configure** utiliza el perfil *predeterminado* creado por WebSphere Application Server para z/OS. Es muy recomendable tener una copia de WebSphere Application Server para el sistema de archivos de configuración z/OS en el caso de que necesite volver a ejecutar el destino **configure** por cualquier razón.

## Configuración de WebSphere Application Server

La configuración de WebSphere Application Server para z/OS implica la creación de un origen de datos, una serie de servidores y configurar el JMS y los valores de seguridad. Todas estas tareas pueden realizarse mediante la ejecución del destino **configure** proporcionado.

El perfil creado por el destino **configurar** de Ant tomará los siguientes valores predeterminados. Al llamar al destino se puede sustituir la propiedad `cell.name`; sin embargo, la propiedad `profile.name` no puede tener un valor que no sea "default", ya que es el único valor soportado por WebSphere Application Server para z/OS.

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

El mandato **build.sh configurar** 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`<sup>1</sup> directorio. Consulte “Archivos de propiedades” en la página 7 y la publicación *Cúram Server Guía del desarrollador* para obtener más información sobre la configuración de un archivo `Bootstrap.properties`. “Configuración de WebSphere Application Server”, muestra contenido de ejemplo del archivo `AppServer.properties`.

---

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

De forma predeterminada, el destino **configure** establece un origen de datos de controlador de tipo 4 universal (XA). Sin embargo, puede configurar un origen de datos de controlador de tipo 2 Universal de DB2 (RRS) estableciendo la propiedad `curam.db.type2.required` en `AppServer.properties`. Cuando utilice esta propiedad debe tener la variable de entorno `DB2DIR` establecida en la vía de acceso de instalación de DB2 para z/OS.

Existen varias maneras posibles de configurar DB2 para z/OS y WebSphere Application Server para z/OS para dar soporte a un controlador de tipo 2. Debe consultar la Documentación de WebSphere Application Server, Versión 7.0 y el artículo "Soporte de controlador JDBC universal de DB2", así como la información relacionada.

Es posible configurar un controlador Universal de tipo 2 pasando una propiedad `curam.db.zos.jcc.propfile` opcional, especificando el nombre completo de una DB2 para el archivo de propiedades `jcc z/OS` que se establezca en la propiedad de siervo `db2.jcc.propertiesFile`, que puede contener varios valores, como el ID de subsistema.

```
## PROPIEDADES DE SERVIDOR DE APLICACIONES

# 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 de la celda WebSphere.
cell.name=mycell

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

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

# El alias que se debe usar para la autorización de la base de datos
curam.db.auth.alias=dbadmin

# 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 al cliente
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 1. Archivo de propiedades AppServer de ejemplo*

De forma predeterminada el destino **configure** establece 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`.

Para WebSphere Application Server para z/OS, también debe incluir una propiedad `cell.name` que sea igual al nombre largo de la celda.

**Nota:**

1. El valor del almacenamiento dinámico de Java, tal como se describe en el ejemplo “Configuración de WebSphere Application Server” en la página 10 y se establece con los scripts de configuración es para 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. Pueden producirse problemas de memoria con WebSphere Application Server para los controladores de la base de datos envueltos de z/OS durante la recuperación de CLOB y BLOB de gran tamaño (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.

**Ubicaciones alternativas del archivo JAR**

Con WebSphere Application Server for z/OS V8, los sistemas de instalación de solo lectura pueden causar problemas con la colocación de los archivos JAR de registro y codificación de Cúram (descritos aquí “Reiniciar el servidor de aplicaciones” en la página 31). De forma predeterminada, cada vez que el destino **configure** de Ant se ejecuta, estos archivos JAR se copian en el sistema de archivos de configuración de WebSphere (\$JAVA\_HOME/lib/ext y \$WAS\_HOME/lib). Si se monta el sistema de archivo de instalación subyacente de solo lectura, estas copias fallarán y el sistema de archivos no podrá volver a montar como de lectura/Escritura para la invocación **configure**. Pero, es posible configurar un enlace simbólico, con el sistema de archivos montados como de lectura/Escritura (una actividad de una vez), especificando una ubicación alternativa en la que se copien estos archivos.

El procedimiento de una vez es el siguiente:

1. Monte el sistema de archivos de instalación de WebSphere (por ejemplo, /usr/lpp/zWebSphere/V8R0) de solo lectura.
2. Cree un enlace simbólico en el directorio de WebSphere lib para Cúram Registry.jar, que contenga CuramLoginModule. Por ejemplo:

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

3. Cree un enlace simbólico en el directorio Java lib/ext para el jar codificado de Cúram: CryptoConfig.jar. Por ejemplo:

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

4. Vuelva a montar el sistema de archivos de instalación de WebSphere como de solo lectura.

Los pasos anteriores permitirán que permanezca el sistema de archivos de WebSphere como de solo lectura cuando se ejecuta el destino **configure**, el cual copia los archivos en la ubicación alternativa que apunta al sistema de archivos de instalación. Cuando se ejecuta el destino **configure** de Ant, se especifican las siguientes propiedades, las cuales se muestran en las ubicaciones del ejemplo anteriores:

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

## Configuración de seguridad

La configuración de seguridad por omisión de IBM Cúram Social Program Management dentro de WebSphere Application Server para z/OS implica el registro de usuario basado en archivos por omisión 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 una serie de configuraciones de seguridad alternativas que pueden utilizarse con WebSphere Application Server para z/OS. 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 de sesión para la autenticación de identidad sólo debe establecerse la propiedad `curam.security.check.identity.only` en `true`. Esto es para asegurarse de que se utilice el mecanismo de autenticación alternativo configurado.

Consulte la sección Sólo autenticación de identidad de la publicación *Cúram Security Handbook* para obtener más detalles.

### Configuración de SAF (RACF)

Al configurar WebSphere Application Server para el sistema z/OS para que utilice SAF (RACF), tras haber configurado WebSphere Application Server para z/OS adecuadamente con la herramienta de gestión de perfiles o los paneles de personalización ISPF z/OS, debe establecer la propiedad `curam.security.zos.saf` en `true` antes de ejecutar el destino `configure`.

Al ejecutar el destino `configure`, el valor predeterminado para la propiedad `curam.security.user.registry.enabled` es `true`. No se recomienda sustituir `curam.security.user.registry.enabled` estableciéndola en `false`. La propiedad `curam.security.check.identity.only` se puede establecer para cada uno de los requisitos (consulte más adelante).

### Pasos de configuración especiales al usar sólo identidad y LDAP

#### Acerca de esta tarea

Cuando utilice sólo identidad en combinación con WebSphere Application Server para z/OS y LDAP puede que tenga que realizar pasos adicionales de configuración manual; es decir, independientemente de si la configuración se realiza a través de la consola administrativa de WebSphere para z/OS Application Server o el destino `configure`. Con esta combinación, puede encontrar que WebSphere Application Server para z/OS no se puede iniciar correctamente y esto es debido a la necesidad de añadir un nombre de usuario generado por WebSphere Application Server para z/OS a la propiedad de la lista de exclusión del módulo de inicio de sesión (`exclude_usernames`) que se describe en el apartado "Añadir el módulo de inicio de sesión" en la página 33. En este caso, en el que no se puede iniciar WebSphere Application Server para z/OS, habrá un mensaje de error SECJ0270E en el archivo `SystemOut.log` antes de la anomalía.

Estos son los pasos necesarios para resolver este error:

## Procedimiento

1. Identifique el nombre de usuario que está provocando que no se inicie WebSphere Application Server para z/OS. Configure el rastreo de módulo de inicio de sesión como se describe en el apartado “Registro del proceso de autenticación” en la página 16 (en relación con la meta configure ) o “Añadir el módulo de inicio de sesión” en la página 33 (en relación con la configuración a través de la consola administrativa) y reinicie WebSphere Application Server para z/OS. 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 nombre de usuario fallido con un registro como el siguiente:

```
SystemOut      0 Username: server:MyNodeCell_MyNode_CuramServer
```

Donde "MyNode" es el nombre de nodo, "MyNodeCell" es el nombre de celda y "CuramServer" es el nombre de servidor de WebSphere Application Server para z/OS. 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 para z/OS. Puesto que WebSphere Application Server para z/OS no consigue iniciarse, puede realizar este cambio a través de la consola administrativa y debe editar el archivo de configuración de WebSphere Application Server z/OS directamente. En el sistema de archivos de configuración de WebSphere Application Server para z/OS edite config\cells\MyNodeCell\security.xml, que tendrá tres apariciones de la propiedad exclude\_usernames (uno 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 id variará según la configuración del sistema y el separador por comas en el atributo de valor de ejemplo representa el valor curam.security.usernames.delimiter predeterminado, que puede ser diferente en su caso.

3. Reinicie WebSphere Application Server para z/OS.

## Registro de usuarios de WebSphere Application Server

De forma predeterminada, el servidor para el registro de usuario de z/OS Application Server configurado 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 servidor de Application Server para el registro de usuarios z/OS será consultado durante el proceso de autenticación, independientemente de si la autenticación de identidad sólo está habilitada o inhabilitada. Si esta propiedad se establece en `false`, no se consultará el registro de usuarios de WebSphere Application Server para z/OS. Por ejemplo, si `curam.security.check.identity.only` está establecido en `true` y `curam.security.user.registry.enabled` se establece en `false`, ni las verificaciones de autenticación de Cúram ni el registro de usuarios WebSphere Application Server para z/OS se utilizarán 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 para z/OS 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 externo que se autenticarán, o que no se autenticarán, mediante el registro de usuarios de WebSphere Application Server para z/OS:

- Los tipos de usuario especificados en la lista de `curam.security.user.registry.enabled.types` serán procesados en el registro de usuarios de WebSphere Application Server para z/OS (p. ej. LDAP) y la implementación de `ExternalAccessSecurity`.
- Los tipos de usuario especificado en la lista de `curam.security.user.registry.disabled.types` no se procesarán en el registro de usuarios de WebSphere Application Server para z/OS y el proceso de su aplicación `ExternalAccessSecurity` será la autorización para realizar la autenticación.

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

- De forma predeterminada, el registro de usuarios de WebSphere Application Server para z/OS no está seleccionado 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 registro de usuarios de WebSphere Application Server para z/OS o externo (por ej. LDAP), 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 autenticado mediante el registro de usuarios de WebSphere Application Server para z/OS o 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 autenticado por el registro de usuarios de WebSphere Application Server para z/OS o 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 32 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 hace que se añada la información de rastreo al archivo SystemOut.log de WebSphere Application Server para z/OS 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 para z/OS almacena en antememoria la información de usuario y las credenciales en una memoria caché de seguridad, y el módulo de inicio de sesión de la aplicación no se invocará mientras haya una entrada de usuario 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 establece 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 LTPA Token2 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 para z/OS, com.ibm.ws.security.webChallengeIfCustomSubjectNotFound, en false para asegurarse de que las sesiones web puedan transferirse sin interrupciones entre dos servidores de un clúster (por ejemplo, en caso de una migración tras error) sin que se pidan credenciales de seguridad. Este valor permite validar correctamente la señal de seguridad utilizada por WebSphere Application Server para z/OS sin intervención del usuario.

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 32 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 endurecimiento 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 30.

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#step19)
- [http://www.ibm.com/developerworks/websphere/techjournal/1004\\_botzum/1004\\_botzum.html?ca=drs#step29](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 importa obtener un nivel de seguridad menor, puede elegir, bajo su responsabilidad, seguir los pasos para 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*.

## Modalidad de 64 bits

Si se utiliza el destino **configure** se puede especificar la propiedad `curam.zos.64bitmode` en el archivo `AppServer.properties` con un valor de `true` para hacer que el servidor esté configurado para soportar la modalidad de 64 bits.

**Nota:** Al utilizar el soporte de la modalidad de 64 bits también puede ser necesario revisar y ajustar los tamaños de almacenamiento dinámico JVM basándose en el tamaño, el rendimiento, los objetivos de rendimiento de la aplicación, y otros factores.

## Configuración de huso horario

Si se utilizan varias máquinas de servidor, todas 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 proporcionan numerosos destinos Ant para ayudar en el inicio y la detención de los servidores WebSphere Application Server para z/OS. Estos destinos deben ejecutarse desde el directorio <SERVER\_DIR> y, en cuanto al destino **configure**, se requiere que se configure correctamente el archivo `AppServer.properties` ("Configuración de WebSphere Application Server" en la página 10). También requieren un número de opciones extra que especificar, que se detallan a continuación.

### Iniciar un servidor WebSphere

El destino Ant para iniciar un servidor de WebSphere Application Server para z/OS es **startserver** y requiere las siguientes opciones:

- `-Dserver.name`

El nombre del servidor que se debe 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 se producirán tiempos de espera de transacción excedidos durante el primer inicio de sesión y 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 volver a ejecutar el destino **prepare.application.data**.

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

Figura 2. Ejemplo de uso

### Detener un servidor WebSphere

El destino Ant para detener un servidor de WebSphere Application Server para z/OS es **stopserver** y requiere las siguientes opciones:

- `-Dserver.name`

El nombre del servidor que se va a detener.

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

Figura 3. Ejemplo de uso

## Reiniciar un servidor WebSphere

El destino Ant para reiniciar un WebSphere Application Server para z/OS es **restartserver** y las opciones son las mismas que para el destino **startserver**. Consulte “Iniciar un servidor WebSphere” en la página 18 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 archivos `.ear` y configurar WebSphere Application Server para z/OS, es desplegar los archivos `.ear` en el servidor de aplicaciones.

Antes del despliegue es importante tener en cuenta que en WebSphere Application Server para z/OS los scripts de configuración que se proporcionan con IBM Cúram Social Program Management soportan una configuración simple en una instalación de servidor de base de WebSphere Application Server para z/OS.

El despliegue implica:

- Establecimiento de los archivos de propiedades;
- Instalar los archivos `.ear`;
- Creación de una base de datos;
- De forma opcional, pero muy recomendable, pre-compilar los JSP;
- Probar la aplicación.

### Archivos de propiedades

Para instalar los archivos `.ear` de la aplicación utilizando Ant debe tener los archivos de propiedad adecuados en el directorio `$SERVER_DIR/project/property`. Estos archivos son:

- `bootstrap.properties`: para crear una base de datos;
- `AppServer.properties`: para instalar archivos `.ear`.

Esta sección describe lo que necesitan contener estos archivos. Para obtener más información, consulte el *Cúram Server Guía del desarrollador*.

### Bootstrap.properties

Las propiedades de despliegue específicas o correspondientes para WebSphere Application Server para z/OS se muestran en el apartado “Bootstrap.properties”.

```

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

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

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

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

```

Figura 4. Archivo de propiedades Bootstrap relacionadas con el despliegue

Algunas de estas propiedades se describen en el apartado “Propiedades de programa de arranque” en la página 7 y son las mismas que las que necesita para generar IBM Cúram Social Program Management en Windows para desplegarlo en z/OS, pero tenga en cuenta lo siguiente:

- El <valor de \$SERVER\_DIR> es el valor de su variable de entorno \$SERVER\_DIR.

### AppServer.properties

Las propiedades de despliegue específicas o correspondientes para WebSphere Application Server para z/OS se muestran en el apartado “AppServer.properties”.

```

# Propiedad que indica WebSphere
as.vendor=IBM

# El nombre de la celda WebSphere.
cell.name=mycell

# El nombre del nodo WebSphere.
node.name=mynode

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

```

Figura 5. Archivo de propiedades AppServer relacionadas con el despliegue

Algunas de estas propiedades se describen en el apartado “Propiedades de AppServer” en la página 8 y son las mismas que lo necesario para generar archivos .ear de la aplicación de IBM Cúram Social Program Management para desplegarlos en z/OS.

### Comprobación de la configuración

Puede comprobar los archivos de propiedades y de configuración ejecutando el destino **configtest** de Ant.

Ejecute el destino **configtest** del shell como se indica a continuación:

```

cd $CURAMSDEJ/bin
ant configtest

```

Revise el resultado para ver si hay errores o avisos y resolverlos.

## Despliegue

No hay destinos Ant para instalar y desinstalar aplicaciones en un servidor de WebSphere Application Server para z/OS. Al igual que con los destinos **startserver** y **stopserver**, los destinos **installapp** y **uninstallapp** requieren que el archivo `AppServer.properties` se haya configurado correctamente (consulte el apartado "Configuración de WebSphere Application Server" en la página 10). 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 archivo `.ear`) es **installapp** y requiere las siguientes opciones:

- `-Dserver.name`  
El nombre del servidor que se va a instalar.
- `-Dear.file`  
Nombre completo del archivo `.ear` que se debe instalar.
- `-Dapplication.name`  
El nombre de la aplicación.

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

Figura 6. Ejemplo de uso

**Nota:** El archivo `.ear` (EAR) que contiene el módulo de servidor debe ser desplegado antes de instalar cualquier otro archivo EAR (sólo de 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"
```

En función del shell del usuario, es posible que haya que eludir las citas anteriores; por ejemplo, `-Dwsadmin.extra.args="\-appendtrace true\"`. No debería utilizar esta propiedad para definir argumentos ya pasados a través de los scripts 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 para z/OS. Vaya a **Aplicaciones > Tipos de aplicación > Aplicaciones empresariales de WebSphere** y seleccione la aplicación. 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 30.

Tenga en cuenta que, si se cambia el nombre de usuario, 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 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.sh uninstallApp -Dserver.name=CuramServer  
-Dapplication.name=Curam
```

Figura 7. Ejemplo de uso

### Precompilación de las JSP

Hay un destino adicional disponible durante el despliegue, **precompilejsp**, que permite precompilar los JSP de un cliente .ear compilado *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 estas:

- `-Dear.file`  
Nombre completo del archivo .ear que se debe precompilar.

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

Figura 8. Ejemplo de uso

**Nota:** Es una actividad de larga duración y dependiendo de las posibilidades de su sistema, etc. podría tardar varias horas. Asegúrese de que la tarea no esté restringido significativamente con respecto al tiempo de CPU disponible y de que haya suficiente espacio libre disponible en el sistema de archivos \$CURAMSDEJ.

Además al ejecutar el destino **precompilejsp** de WebSphere Application Server para z/OS, puede producirse una excepción de memoria (o se puede omitir y no precompilar algún JSP silencioso). Para solucionar esto el script `JspBatchCompiler.sh` en el directorio `$WAS_HOME/bin` debe ser modificado para aumentar el tamaño máximo de memoria. Cambie el consumo de memoria de `-Xmx256m` por al menos `-Xmx1024m`.

## Creación de una base de datos

Para utilizar la aplicación de gestión de IBM Cúram Social Program debe crear e inicializar una base de datos. En esta sección se presupone que está utilizando el destino **database** de Ant para crear una base de datos. No obstante, es posible utilizar las herramientas de cliente de DB2 para hacerlo. Consulte la *Guía de instalación de Cúram* para obtener más detalles sobre este método.

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

Figura 9. Mandatos de shell de ejemplo para crear una base de datos

## Prueba del despliegue

Cuando los archivos `.ear` de la aplicación IBM Cúram Social Program Management están instalados<sup>2</sup> en una instalación configurada de WebSphere Application Server z/OS el paso siguiente es iniciar y probar la aplicación.

Asegúrese de que se inicie el servidor que corresponda<sup>3</sup> y abra la página siguiente en un navegador web:

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

donde,

`<some.machine.com>` identifica el nombre de sistema principal o la dirección IP donde se ejecuta WebSphere Application Server para el sistema z/OS, `<port>` identifica el puerto del servidor en el que se despliega la aplicación cliente (como en el apartado “Configurar el acceso al puerto” en la página 37) y `<context-root>` identifica la raíz de contexto del módulo WAR.

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 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

---

2. La instalación de una aplicación de servicios web también pueden ser necesaria.

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

*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

Aquí se tratan los pasos necesarios de configuración y despliegue en una instalación base de WebSphere Application Server para z/OS. Tendrá que modificar estos pasos adecuadamente para desplegar una instalación de despliegue de red de WebSphere Application Server para z/OS. Consulte el apartado “Despliegue de la red WebSphere” en la página 47 para obtener más información en esta área.

### Configuración manual de WebSphere Application Server

La instalación de IBM WebSphere Application Server para z/OS puede configurarse manualmente si es necesario, pero no es recomendable hacerlo cuando se utiliza una instalación básica del servidor de aplicaciones. Esta sección detalla los pasos manuales necesarios para configurar WebSphere Application Server para z/OS solo con fines informativos.

Vale la pena observar que los valores especificados en el apartado **Recursos** de la consola administrativa se pueden configurar a 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 visualizar los distintos recursos en el ámbito actual. El ámbito, y a su vez la ubicación de cualquier conjunto de recursos, debe basarse en el uso previsto. Es decir, si trabaja en un clúster puede que no sea necesario establecer los mismos valores en cada uno de los servidores. Por lo tanto, el ámbito se puede establecer como celda o nodo.

#### La consola administrativa

La mayor parte de la configuración de WebSphere Application Server para z/OS se realiza utilizando la consola administrativa de WebSphere. Para ejecutar la consola administrativa, debe iniciarse el servidor del perfil predeterminado, ya que la consola administrativa se instala como una aplicación web en dicho servidor (consulte el apartado “Inicio y detención de servidores WebSphere” en la página 18 para obtener información adicional relativa al inicio de servidores).

Para abrir la consola de administración, se debe apuntar a un navegador web a:  
`http://<Your WebSphere host>:<protocol_http_port>/ibm/console`

Donde:

`<Your WebSphere host>` identifica el nombre de sistema principal o la dirección IP donde el sistema WebSphere Application Server para z/OS se está ejecutando y



<protocol\_http\_port> identifica el puerto asignado en la instalación y la personalización de WebSphere Application Server para z/OS.

## Soporte para scripts

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

**sas.client.props:** Abra el archivo `sas.client.props`, que se encuentra en el directorio de instalación `profiles/default/properties` de WebSphere Application Server para z/OS. 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 ejecutan. 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 de la consola administrativa.

**soap.client.props:** Abra el archivo `soap.client.props`, que también se encuentra en el directorio `profiles/default/properties` de instalación de WebSphere Application Server para z/OS. 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 siguientes credenciales para que coincidan con las credenciales que ha configurado para WebSphere en “Configuración de WebSphere Application Server” en la página 10. 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 agotamientos del tiempo de espera cuando se instalan los archivos `.ear` de la aplicación, asegúrese de configurar adecuadamente lo siguiente; p.ej.:

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

Según el rendimiento de su entorno, puede que necesite un valor diferente.

**server.policy:** Abra el archivo `server.policy.props`, que se encuentra en el directorio de instalación `profiles/default/properties` de WebSphere Application Server para z/OS. 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/default/installedApps/
<cell.name>/<SERVER_MODEL_NAME>.ear/
guice-2.0.jar" { permission java.lang.RuntimePermission
"modifyThread"; permission java.lang.RuntimePermission
"modifyThreadGroup"; };
```

donde *<cell.name>* es el nombre de la celda de WebSphere Application Server para z/OS de destino

y *<SERVER\_MODEL\_NAME>* es el nombre del archivo .ear (EAR) de la aplicación.

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

### Acerca de esta tarea

DB2 para z/OS es la base de datos soportada en z/OS. La consola administrativa de WebSphere Application Server para z/OS se utiliza para configurar un alias de inicio de sesión de los orígenes de datos DB2 para z/OS como se indica a continuación:

### Procedimiento

1. Vaya a **Seguridad > Seguridad global**;
2. Expanda la opción **Servicio de autenticación y autorización Java** en el recuadro **Autenticación** y seleccione la opción **Datos de autenticación de J2C**;
3. Pulse el botón **Nuevo** para abrir la pantalla 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 en el botón **Aceptar** para confirmar los cambios.

## Configurar DB2 para los orígenes de datos z/OS

Para z/OS tiene la opción de configurarlo con el controlador universal JDBC de DB2 del tipo 4 (XA) o el tipo 2 (RRS).

### Configuración para un controlador universal JDBC del tipo 4 (XA):

#### Configuración de la variable de entorno DB2 para z/OS

1. Vaya a **Entorno > Variables de WebSphere**;
2. *Nota:* el ámbito adecuado en el que se van a definir los orígenes de datos debe seleccionarse en este punto.
3. Seleccione el enlace **DB2UNIVERSAL\_JDBC\_DRIVER\_PATH** en la lista de variables de entorno. Esto abrirá la pantalla de configuración;
4. Establezca el campo **Valor** para que apunte al directorio que contiene los controladores de tipo 4. Este es normalmente el directorio de instalación **drivers** de Cúram SDEJ, por ejemplo: */CuramSDEJ/drivers*
5. Pulse en el botón **Aceptar** para confirmar los cambios.

### Configurar el proveedor del controlador de base de datos

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 el botón **Nuevo** para añadir un nuevo controlador. Esto abrirá una pantalla de configuración;
4. Seleccione el desplegable **DB2** de la lista de **tipos de datos** proporcionada;
5. Seleccione el desplegable **Proveedor de controlador JDBC universal de DB2** de la lista de **tipos de proveedores** suministrada;
6. Seleccione el desplegable **Origen de datos XA** de la lista de **tipos de implementaciones** suministrada;
7. Pulse el botón **Siguiente** para continuar;
8. Revise las propiedades en la pantalla de configuración que se abre. Cambie la línea de ruta de clases `${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar` para que apunte a la licencia de DB2 para z/OS proporcionada por IBM para la conectividad de DB2 para z/OS y pulse **Aplicar**;
9. Pulse en el botón **Siguiente** y en **Finalizar** para confirmar los cambios.

### Configurar el origen de datos del controlador de la base de datos

Los pasos siguientes deben repetirse para cada uno de los orígenes de datos de aplicación, sustituyendo `curamdb`, `curamsibdb` y `curamtimerdb` por `<DataSourceName>` (sin los corchetes):

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 para el proveedor;
2. Seleccione el enlace **Orígenes de datos** en **Propiedades adicionales**;
3. Pulse el botón **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>`  
Pulse **Siguiente**;
5. Establezca los campos como se indica a continuación:  
**Tipo de controlador :** 4;  
**Nombre de base de datos:** el nombre de la base de datos DB2 para z/OS;  
**Nombre del servidor :** el nombre del servidor de bases de datos de DB2 para z/OS;  
**Número de puerto:** el puerto del servidor de bases de datos DB2 para z/OS;  
Deje todos los demás campos sin tocar, a menos que se requiera un cambio específico, y pulse **Siguiente**;
6. Establezca los campos como se indica a continuación:  
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: `DefaultPrincipalmapping`  
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 26;

Deje todos los demás campos sin tocar, a menos que se requiera un cambio específico, y pulse **Siguiente**;

7. Pulse el botón **Finalizar** para confirmar los cambios y continuar;
8. Seleccione el origen de datos *nombreOrigenDatos* recién creado en la lista visualizada;
9. Seleccione el enlace **Propiedades personalizadas** en **Propiedades adicionales**;
10. Seleccione la entrada `fullyMaterializeLobData`;
11. Defina el valor a `false`;
12. Pulse en el botón **Aceptar** para confirmar el cambio.

### Configuración para un controlador universal JDBC del tipo 2 (RRS):

#### Establecer variables de entorno DB2

1. Vaya a **Entorno > Variables de WebSphere**;
2. *Nota:* el ámbito adecuado en el que se van a definir los orígenes de datos debe seleccionarse en este punto.
3. Seleccione el enlace `DB2UNIVERSAL_JDBC_DRIVER_PATH` de la lista de variables de entorno. Esto abrirá la pantalla de configuración de esta variable;
4. Establezca el campo **Valor** para que apunte al directorio que contiene el controlador de tipo 2. Esta suele ser la vía de acceso de instalación de DB2 que contiene el archivo `db2jcc.jar`.
5. Pulse en el botón **Aceptar** para confirmar los cambios.
6. Seleccione el enlace `DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH` en la lista de variables de entorno. Esto abrirá la pantalla de configuración de esta variable;
7. Establezca el campo **Valor** para que apunte al directorio que contiene los enlaces de la biblioteca compartida de DB2 para z/OS para el controlador del tipo 2. Esta es la vía de acceso de la instalación de DB2 z/OS que contiene las bibliotecas del controlador de tipo 2 (como `libdb2jcc2zos.so`, que variará según la DB2 para la versión de z/OS y la implementación de 31/64 bits);
8. Pulse en el botón **Aceptar** para confirmar los cambios.

#### Establecer el proveedor de controlador de base de datos

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 el botón **Nuevo** para añadir un nuevo controlador. Se abrirá una pantalla de configuración;
4. Seleccione el desplegable **DB2** de la lista de **tipos de datos** proporcionada;
5. Seleccione el desplegable **Proveedor de controlador JDBC universal de DB2** de la lista de **tipos de proveedores** suministrada;
6. Seleccione el desplegable **Origen de datos de agrupación de conexiones** de la lista de **tipos de implementaciones** suministrada;
7. Pulse el botón **Siguiente** para continuar;
8. Revise las propiedades en la pantalla de configuración que se abre para garantizar que los valores de la vía de acceso a la biblioteca de clases y nativa sean correctos, basándose en los valores previamente establecidos para las

variables de entorno DB2UNIVERSAL\_JDBC\_DRIVER\_PATH y DB2UNIVERSAL\_JDBC\_DRIVER\_NATIVEPATH. No debe ser necesario realizar cambios;

9. Pulse en el botón **Siguiente** y en **Finalizar** para confirmar los cambios.

### Configurar el origen de datos del controlador de la base de datos

Los pasos siguientes deben repetirse para cada uno de los orígenes de datos de aplicación, sustituyendo curamdb,curamsibdb y curamtimerdb por *<DataSourceName>* (sin los corchetes) en los pasos siguientes:

1. Seleccione el Proveedor de controlador universal JDBC de DB2 que ahora aparece en la lista **Proveedores de JDBC**. Esto abrirá la pantalla de configuración del proveedor;
2. Seleccione el enlace **Orígenes de datos** en **Propiedades adicionales**;
3. Pulse el botón **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/<NombreOrigenDeDatos>*
5. Pulse **Siguiente** para continuar;
6. Establezca los campos como se indica a continuación:  
**Nombre de base de datos**: el nombre de la base de datos DB2 para z/OS;  
**Tipo de controlador** : 2;  
Deje todos los demás campos igual, a menos que sea necesario algún cambio específico y pulse **Siguiente**;
7. Establezca los campos como se indica a continuación:  
Establezca el valor de desglose de **Alias de autenticación gestionado por componentes**: *<válido para la base de datos>*;  
Establezca el valor de la lista desplegable **Alias de configuración de correlaciones** en: DefaultPrincipialMapping  
Establezca el valor de desglose de **Alias de autenticación gestionado por contenedores**: *<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 26;  
Deje todos los demás campos igual, a menos que sea necesario algún cambio específico y pulse **Siguiente**;
8. Pulse el botón **Finalizar** para confirmar los cambios y continuar;
9. Seleccione el origen de datos recién creado *NombreOrigenDeDatos* en la lista que se muestra;
10. Seleccione el enlace **Propiedades personalizadas** en **Propiedades adicionales**;
11. Seleccione la entrada `fullyMaterializeLobData`;
12. Defina el valor a `false`;
13. Pulse en el botón **Aceptar** para confirmar el cambio.

### Establecer la propiedad `db2.jcc.propertiesFile` JVM (opcional)

Si desea utilizar un archivo de configuración externo identificado por la propiedad `db2.jcc.propertiesFile` para el controlador JDBC universal de tipo 2:

1. Vaya a **Servidores** > **Tipos de servidor** > **Servidores de aplicación WebSphere**;

2. Seleccione el servidor correspondiente de la lista;
3. En el panel Infraestructura de servidor expanda **Java y gestión de procesos**;
4. Seleccione el enlace **Definición de procesos**
5. En el panel processType lleve a cabo los pasos siguientes para cada elemento de la lista (adjunto, control y siervo):
  - a. Seleccione el enlace **processType**;
  - b. En el panel Propiedades adicionales seleccione el enlace **Java Virtual Machine**.
  - c. En el panel Propiedades adicionales seleccione el enlace **Propiedades personalizadas**.
  - d. Pulse el botón **Nuevo** y establezca la propiedad del modo siguiente:  
**Nombre:** db2.jcc.propertiesFile  
**Valor:** nombre completo del archivo de propiedades  
 Pulse en el botón **Aceptar** para añadir la propiedad.  
 Consulte la información en el apartado “Configuración de WebSphere Application Server” en la página 10 sobre cómo configurar el archivo de propiedades.

### 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 usuarios por omisión que se utiliza es el registro de usuario basado en archivos por omisión de WebSphere Application Server para z/OS.

#### 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. Seleccione el botón **Identidad de servidor generada automáticamente**;
5. Seleccione **Ignorar mayúsculas para autorización** y pulse en el botón **Aceptar**;
6. Escriba la contraseña para el usuario administrativo predeterminado, por ejemplo, websphere, especifique la confirmación y pulse en el botón **Aceptar** para confirmar los cambios;
7. Seleccione **Habilitar seguridad administrativa**;
8. Seleccione **Habilitar seguridad de la aplicación**;
9. 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**;
10. Establezca como **Definiciones de dominio disponibles** los **Depósitos federados**;
11. Pulse el botón **Aplicar** para confirmar los cambios;
12. Vaya a **Seguridad > Seguridad global**;
13. Expanda **Seguridad SIP y web** y seleccione **Inicio de sesión único (SSO)**;
14. Seleccione **Requiere SSL**;

15. Pulse **Aceptar** para confirmar el cambio.
16. Vaya a **Seguridad > Seguridad global**;
17. Seleccione el enlace **Propiedades personalizadas**;
18. Pulse el botón **Nuevo** y establezca el nombre y el valor del modo siguiente:  
Nombre : `com.ibm.ws.security.web.logoutOnHTTPSessionExpire`  
Valor : `true`
19. Pulse en el botón **Aceptar** para añadir la nueva propiedad.
20. Pulse el botón **Nuevo** y establezca el nombre y el valor del modo siguiente:  
Nombre : `com.ibm.ws.security.addHttpOnlyAttributeToCookies`  
Valor : `true`
21. Pulse **Aceptar** para confirmar el cambio.
22. Guarde los cambios realizados en la configuración maestra.

### Reiniciar el servidor de aplicaciones

Este paso es obligatorio. Los espacios de direcciones de WebSphere Application Server para z/OS deben reiniciarse para que los cambios de seguridad entren en vigor y para añadir los usuarios adicionales necesarios. Los espacios de direcciones se pueden detener usando el script `stopServer.sh` adecuado en el directorio `profiles/default/bin` de la instalación de WebSphere Application Server para z/OS o usando el comando de operador de **z/OS STOP** adecuado para la instalación.

Antes de reiniciar el servidor de aplicaciones, es necesario hacer disponible los archivos JAR de registro y codificación de WebSphere Application Server para z/OS. El archivo JAR de registro contiene las clases necesarias para la configuración de seguridad y el archivo JAR de codificación contiene los valores de codificación necesarios y los datos para la protección de contraseñas.

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

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 `Java jre/lib/ext`. Si requiere personalizaciones en la configuración de codificación de Curam, consulte *Curam Security Handbook* para obtener más información.

En los sitios en los que el sistema de archivos de la instalación de WebSphere sea de solo lectura, consulte el procedimiento: "Ubicaciones alternativas del archivo JAR" en la página 12.

Ahora inicie el servidor de aplicaciones utilizando el script `startServer.sh` en el directorio `profiles/default/bin` de instalación de WebSphere Application Server para z/OS o el mandato **START** del operador **z/OS** adecuado para su instalación 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 aplicaciones. , consulte el apartado "Inicio y detención de servidores WebSphere" en la página 18 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 *websphere* y la contraseña *websphere* establecidos anteriormente.

## **Probar la conexión de DB2 para z/OS**

### **Acerca de esta tarea**

Pruebe probar sus conexiones de DB2 para z/OS una vez se haya reiniciado el servidor de aplicaciones.

### **Procedimiento**

1. Vaya a **Recursos > JDBC > Orígenes de datos**;
2. Marque el recuadro **curamdb DataSource** y/o **curamsibdb DataSource**;
3. Pulse el botón **Probar conexión**;
4. Debe visualizarse el mensaje siguiente si la operación es satisfactoria:

La conexión de prueba para el origen de datos <nombre de origen de datos> en el servidor <nombre de servidor> en el nodo <nombre de nodo> ha sido satisfactoria.

De lo contrario, compruebe los registros de WebSphere Application Server z/OS para obtener detalles sobre la anomalía, corregirla y volver a intentarlo.

## **Configurar usuarios**

### **Acerca de esta tarea**

Como se detalla en el apartado “Configuración de seguridad” en la página 13, el registro de usuarios de WebSphere Application Server para z/OS configurado se utiliza para la autenticación de los usuarios de administración y el usuario de la base de datos. Los usuarios administradores de WebSphere Application Server para z/OS deben añadirse manualmente en el registro de usuarios como se indica a continuación.

### **Procedimiento**

1. Vaya a **Usuarios y grupos > Gestionar usuarios**;
2. Seleccione el botón **Crear**;
3. Complete los detalles para el usuario administrador de WebSphere Application Server para z/OS 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 Application Server para z/OS al crear el perfil, es posible que el usuario administrativo ya esté definido 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:**

1. Vaya a **Seguridad > Seguridad global**;
2. Expanda la entrada **Autenticación y autorización de servicios Java** bajo la cabecera **Autenticación** y seleccione **Inicios de sesión del sistema**;
3. Seleccione el alias correspondiente de la lista. El módulo de inicio de sesión debe configurarse para los alias **DEFAULT**, **WEB\_INBOUND** y **RMI\_INBOUND** de la manera siguiente:
4. Pulse el botón **Nuevo** para configurar un nuevo módulo de inicio;
5. Establezca el campo **Nombre de clase de módulo** en `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. Pulse en el botón **Aceptar** para confirmar la adición del nuevo módulo de inicio de sesión;
9. Seleccione el recién añadido `curam.util.security.CuramLoginModule` de la lista;
10. Seleccione el enlace **Propiedades personalizadas** bajo la cabecera **Propiedades adicionales**;
11. Pulse el botón **Nuevo** para añadir las propiedades necesarias que se enumeran a continuación.

*Tabla 6. Propiedades personalizadas de CuramLoginModule*

| Nombre                      | Valor de ejemplo                   | Descripción  |
|-----------------------------|------------------------------------|--|
| exclude_usernames           | websphere, db2admin                | Obligatorio. Una lista de nombres de usuario que deben excluirse de la autenticación. Esta lista debe incluir el usuario administrativo de WebSphere Application Server (tal y como se especifica en "Configurar la seguridad de administración" en la página 30) 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 26). El delimitador predeterminado es una coma, pero puede ser sustituido por <code>exclude_usernames_delimiter</code> . Los usuarios listados aquí deben estar definidos en el registro de usuarios de WebSphere Application Server para z/OS. |
| exclude_usernames_delimiter |                                    | <i>Opcional.</i> Un delimitador para la lista de nombres de usuario que se proporciona en <code>exclude_usernames</code> . 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                               | <i>Opcional.</i> Esta propiedad debe establecerse en <code>true</code> para depurar el proceso de autenticación. Si se establece en <code>true</code> , la invocación del módulo de inicio de sesión añadirá información de rastreo al archivo <code>SystemOut.log</code> de WebSphere Application Server para z/OS.   |
| module_name                 | DEFAULT, WEB_INBOUND o RMI_INBOUND | <i>Opcional.</i> Esta propiedad debe establecerse en <code>DEFAULT</code> , <code>WEB_INBOUND</code> o <code>RMI_INBOUND</code> , en función de la configuración para la que se haya definido el módulo de inicio de sesión. Se utiliza sólo cuando <code>login_trace</code> está establecido en <code>true</code> para fines de rastreo.  |

Tabla 6. Propiedades personalizadas de CuramLoginModule (continuación)

| Nombre                       | Valor de ejemplo | Descripción   |
|------------------------------|------------------|---|
| check_identity_only          | true             | <i>Opcional.</i> Si esta propiedad se establece en true en el módulo de inicio de sesión no realice 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 usuarios de WebSphere Application Server para z/OS configurado no se omitirá y se consultará después del inicio de sesión del módulo. Esta opción está pensada cuando se requiere soporte de LDAP o cuando se va a usar un mecanismo de autenticación alternativo.  |
| user_registry_enabled        | true             | <i>Opcional.</i> Esta propiedad se utiliza para sustituir el comportamiento de la omisión del registro de usuarios. Si esta propiedad se establece en true, no se consultará el registro de usuarios de WebSphere Application Server para z/OS durante el proceso de autenticación. Si esta propiedad se establece en false, no se consultará el registro de usuarios de WebSphere Application Server para z/OS.<br><b>Nota:</b> Si especifica sólo identidad y utiliza LDAP puede ser necesario realizar pasos de configuración adicionales; consulte el apartado "Pasos de configuración especiales al usar sólo identidad y LDAP" en la página 13. |
| user_registry_enabled_types  | EXTERNAL         | <i>Opcional.</i> Esta propiedad se utiliza para especificar una lista delimitada por comas de tipos de usuarios externos que se procesa en el el registro de usuarios de WebSphere Application Server para z/OS (por ej. LDAP). Consulte el apartado "Registro de usuarios de WebSphere Application Server" en la página 15 para obtener más información sobre el proceso del registro de usuarios de WebSphere Application Server para z/OS.   |
| user_registry_disabled_types | EXTGEN,EXTAUTO   | <i>Opcional.</i> Esta propiedad se utiliza para especificar una lista delimitada por comas de tipos de usuarios externos que no se procesará en el el registro de usuarios de WebSphere Application Server para z/OS (por ej. LDAP). Consulte el apartado "Registro de usuarios de WebSphere Application Server" en la página 15 para obtener más información sobre el proceso del registro de usuarios de WebSphere Application Server para z/OS.  |

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

**Reordenar el módulo de inicio de sesión:**

1. Vaya a **Seguridad > Seguridad global**;
2. Expanda **Autenticación y autorización de servicios Java** bajo la cabecera **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;

4. Seleccione el enlace **Módulos de inicio de sesión JAAS** bajo la cabecera **Propiedades adicionales**;
5. Pulse el botón **Establecer orden**;
6. Seleccione **curam.util.security.CuramLoginModule** y pulse en el botón **Mover hacia arriba**. Repita esto hasta que la entrada CuramLoginModule sea la superior en la lista;
7. Pulse en el botón **Aceptar** para confirmar las modificaciones del orden.

**Inhabilitar la autenticación entre clústeres:** 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 se puedan transferir perfectamente entre dos servidores en un clúster (por ejemplo, en una migración tras error escenario) sin que se pidan credenciales de seguridad.

1. Vaya a **Seguridad > Seguridad global**;
2. Pulse en **Propiedades personalizadas** bajo la cabecera **Autenticación** 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 en el botón **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 30.

## Configuración del servidor

### Configurar el soporte de 64 bits:

#### Procedimiento

1. Vaya a **Servidores > Tipos de servidor > servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor que corresponda de la lista;
3. Marque el recuadro **Ejecutar en modalidad JVM de 64 bits**;
4. Pulse **Aplicar** o **Aceptar** para aplicar los cambios;
5. Guarde los cambios en la configuración maestra utilizando la opción **Guardar** igual que antes.

#### Resultados

**Nota:** También puede ser necesario revisar y ajustar los tamaños de almacenamiento dinámico JVM basándose en el tamaño, el rendimiento, los objetivos de rendimiento de la aplicación, y otros factores.

### Configurar el puerto de búsqueda JNDI:

#### Procedimiento

1. Vaya a **Servidores > Tipos de servidor > servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor que corresponda de la lista;
3. Expanda **Puertos** en el recuadro **Comunicaciones** y pulse 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 los valores del cargador de clases:**

##### **Procedimiento**

1. Vaya a **Servidores > Tipos de servidor > servidores de aplicaciones de WebSphere**;
2. Seleccione el servidor adecuado en la lista;
3. Establezca la **Política del cargador de clases** como MULTIPLE;
4. Pulse en **Aceptar** para aplicar los cambios;
5. 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 que corresponda de la lista;
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 panel Infraestructura de servidor expanda **Java y gestión de procesos**;
4. Seleccione el enlace **Definición de procesos**;
5. En el panel processType lleve a cabo los pasos siguientes para cada elemento de la lista (adjunto, control y siervo):
  - a. Seleccione el enlace **processType**;
  - b. En el panel Propiedades adicionales seleccione el enlace **Java Virtual Machine**.
  - c. 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;
  - d. En el panel Propiedades adicionales seleccione el enlace **Propiedades personalizadas**.
  - e. Pulse el botón **Nuevo** y establezca las propiedades del modo siguiente:  
**Nombre**: com.ibm.websphere.security.util.authCacheCustomKeySupport  
**Valor**: false  
Pulse en el botón **Aceptar** para añadir la propiedad;

6. 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 EJB internos**;
6. Establezca los campos como se indica a continuación:  
**Nombre JNDI del origen de datos** :jdbc/curamtimerdb  
**Alias del origen de datos** : <válido para la base de datos>  
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 26;
7. Pulse en el botón **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** en el recuadro **Comunicaciones**.
4. Seleccione el recuadro **detalles**;
5. Pulse el botón **Nuevo** y establezca los siguientes campos para el puerto TCP/IP del cliente:  
**Nombre de puerto definido por el usuario**: CuramClientEndPoint  
**Host**: \*  
**Puerto**: <puerto de cliente>  
Establezca el la <puerto de cliente> para que coincida con el valor curam.client.httpport del archivo AppServer.properties  
Pulse en el botón **Aceptar** para aplicar los cambios;
6. Pulse el botón **Nuevo** y establezca los siguientes campos para el puerto TCP/IP de WebServices:  
**Nombre de puerto definido por el usuario**: CuramWebServicesEndPoint  
**Host**: \*  
**Puerto**: <puerto de servicios web>  
Establezca el la <puerto de servicios web> para que coincida con el valor curam.webservices.httpport del archivo AppServer.properties  
Pulse en el botón **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 el botón **Nuevo** y establezca los siguientes campos para la cadena de transporte del cliente:
  - Nombre:** CuramClientChain
  - Plantilla de cadena de transporte:** WebContainer-Secure
 Pulse **Siguiente**.
  - Utilizar puerto existente:** CuramClientEndPoint
 Pulse **Siguiente** y **Finalizar**
12. Pulse el botón **Nuevo** y establezca los siguientes campos para la cadena de transporte de servicios web:
  - Nombre:** CuramWebServicesChain
  - Plantilla de cadena de transporte:** WebContainer
 Pulse **Siguiente**.
  - Utilizar puerto existente:** CuramWebServicesEndPoint
 Pulse **Siguiente** y **Finalizar**
13. Seleccione la **CuramClientChain** recién creada;
14. Seleccione el enlace **Canal entrante HTTP**;
15. Asegúrese de que esté seleccionado el recuadro de selección **Utilizar conexiones persistentes**;
16. Pulse en el botón **Aceptar** para confirmar la adición;
17. Vaya a **Entorno > Hosts virtuales**;
18. Pulse el botón **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 host** en el recuadro; **Propiedades adicionales**.
  - Pulse el botón **Nuevo** para añadir un nuevo Alias, estableciendo los campos siguientes:
    - Nombre de host** = \*
    - Puerto** = *<puerto del cliente>*
 Establezca el la *<puerto de cliente>* para que coincida con el valor curam.client.httpport del archivo AppServer.properties. Repita este paso para el otro sistema principal virtual y el puerto utilizados (por ejemplo, webservices\_host);
20. Pulse en el botón **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 30.

### 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 el botón **Nuevo** y establezca el siguiente campo:  
**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 la lista **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 en el botón **Siguiente**;
9. Seleccione **Almacén de datos** y pulse en el botón **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 30.

## 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** en el recuadro; **Propiedades adicionales**.
5. Pulse el botón **Nuevo** y establezca los siguientes campos:
  - Nombre:** CuramQueueConnectionFactory
  - Nombre JNDI:** jms/CuramQueueConnectionFactory
  - Descripción:** la fábrica de todas las conexiones con las colas de la 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:** DefaultPrincipialMapping
  - Alias de autenticación gestionado por el contenedor:** el mismo que el alias de autenticación para la recuperación de XA.

Deje todo lo demás como valor predeterminado y pulse en el botón **Aceptar** para aplicar los cambios;
6. Pulse el botón **Nuevo** y establezca los siguientes campos:
  - Nombre:** CuramTopicConnectionFactory
  - Nombre JNDI:** jms/CuramTopicConnectionFactory
  - Descripción:** la fábrica de todas las conexiones con las colas de la 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:** DefaultPrincipialMapping
  - 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 valor predeterminado y pulse en el botón **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 30.

#### Resultados

**Nota:** Con los pasos de configuración manual anteriores no es posible configurar correctamente la seguridad para la cola de Curam y las fábricas de conexiones de 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. Identificar la cola y la fábrica de conexiones de temas de entradas en la configuración del archivo `resources.xml` de WebSphere Application Server para z/OS. 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 `wsadmin` de WebSphere Application Server para z/OS. 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 comandos siguientes, una vez más, asumiendo definiciones de ámbito de 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: `$AdminConfig getid /Node:MyNode`
  - b. Utilizando el identificador de nodo y célula del paso anterior, combínelo con el identificador de fábrica de conexiones obtenido anteriormente para visualizar la fábrica de conexiones: `$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 anteriores para CuramTopicConnectionFactory.
- g. Salga de la sesión de wsadmin mediante el comando quit, asegurándose de haber guardado los cambios.

**Configurar las colas necesarias:  
Acerca de esta tarea**

A través de la consola administrativa, 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** en el recuadro **Recursos de destino**.
3. Pulse el botón **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\_ <QueueName>  
Deje todo lo demás como valor predeterminado y pulse en el botón **Siguiente**;
6. Utilice **Miembro de bus seleccionado** y pulse **Siguiente**:
7. Pulse **Finalizar** para confirmar la creación de la cola:
8. Seleccione la cola SIB\_ <QueueName> recién añadida que ahora aparece en la lista de proveedores existentes. Esto abrirá la pantalla de configuración de nuevo;
9. Utilice la tabla siguiente para establecer el destino de excepción mediante el botón **Especificar** y el texto asociado.

Tabla 7. 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 el botón **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** en el recuadro; **Propiedades adicionales**.
14. Pulse el botón **Nuevo** y establezca los siguientes campos:  
**Nombre**: <QueueName>  
**Nombre JNDI**: jms/ <QueueName>  
**Nombre de bus** : CuramBus

**Nombre de cola:** SIB\_ <QueueName>

**Modalidad de entrega:** persistente

Deje todo lo demás como valor predeterminado y pulse en el botón **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 30.

### 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** en el recuadro; **Propiedades adicionales**.
4. Pulse el botón **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

**Modalidad de entrega JMS:** No persistente

Deje todo lo demás como valor predeterminado y pulse en el botón **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 30.

### 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** en el recuadro; **Propiedades adicionales**.
4. Crear una nueva especificación pulsando el botón **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 valor predeterminado y pulse en el botón **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 30.

### 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 valor predeterminado y pulse en el botón **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 30.

## 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 para z/OS proporciona un programa de utilidad para generar el SQL para crear estas tablas, el generador DDL SIB.

El generador se puede ejecutar mediante el mandato siguiente:

```
$WAS_HOME/bin/sibDDLGenerator.sh
-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, db2;
- *plataforma* es el sistema operativo, por ejemplo: 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.zos.dbname de Bootstrap.properties.

Por ejemplo:

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

Este comando generará sentencias SQL para definir las tablas del bus de integración de servicios y dichas sentencias de SQL deberán ejecutarse en la base de datos de destino.

**Nota:** Existen valores predeterminados de DB2 específicos de z/OS para STOGROUP y BUFFERPOOL; consulte el Documentación de producto de WebSphere Application Server, para obtener más información.

**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 para z/OS proporciona el DDL de estas tablas en su directorio \$WAS\_HOME/Scheduler.

Los archivos DDL que deben ejecutarse son createTablespaceDB2ZOS.ddl y createSchemaDB2ZOS.ddl, en ese orden.

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

### Finalización

El servidor de Application Server para z/OS ahora está configurado y listo para la instalación de los archivos .ear de la aplicación IBM Cúram Social Program Management. Salga de la consola de administración y reinicie WebSphere Application Server para z/OS utilizando la descripción de los destinos del apartado “Inicio y detención de servidores WebSphere” en la página 18.

## Despliegue manual de aplicaciones

### Acerca de esta tarea

Para instalar una aplicación empresarial en WebSphere Application Server para z/OS, 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.

### Procedimiento

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

Las ubicaciones predeterminadas para la aplicación de los archivos .ear son:  
\$SERVER\_DIR/ear/WAS/

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, en el panel Resumen, 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 realizados en la configuración maestra. (Consulte "Guardar la configuración maestra" en la página 30 para obtener más detalles).
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 **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 **Crear**.  
Consulte "Cambiar el nombre de usuario SYSTEM" en la página 21 para obtener información sobre las credenciales que espera aquí la aplicación y 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 un nombre de usuario adecuado 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 **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 el nombre de usuario y la contraseña adecuados en los campos **nombre\_usuario** y **contraseña** respectivamente. Marque **Seleccionar** como rol **mdbuser** y pulse en **Aplicar**.
18. Pulse **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, apunto a un navegador web en el URL de la aplicación desplegada, por ejemplo:  
`https://<Your WebSphere host>:<CuramClientEndPoint>/Curam`  
 Donde:  
*<Your WebSphere host>* identifica el nombre de sistema principal o la dirección IP donde WebSphere Application Server para el sistema z/OS se está ejecutando y *<CuramClientEndPoint>* identifica el puerto asignado (como en el apartado "Configurar el acceso al puerto" en la página 37).

## Despliegue de la red WebSphere

IBM WebSphere Application Server Network Deployment ofrece servicios de despliegue avanzados, incluyendo agrupaciones en clúster, servicios edge y alta disponibilidad para configuraciones distribuidas.

### Sugerencias para trabajar con el despliegue de la red WebSphere

**Personalización para el despliegue de la red WebSphere:** La personalización de WebSphere Network Deployment (utilizando la herramienta de gestión de perfiles z/OS o ISPF) está fuera del ámbito de este documento, pero junto con la información que encontrará en el *Directorio de programas para WebSphere Application Server para z/OS V7.0 (GI11-4295)* y *IBM WebSphere Application Server para z/OS, Versión 7.0: Instalación del entorno de servicio de aplicaciones Documentación de producto de WebSphere Application Server, Versión V7.0*. IBM ofrece una serie de Redbooks útiles para hacer esto. Se pueden encontrar en el sitio web de IBM Redbook: <http://www.redbooks.ibm.com/>.

**Sincronizar cambios:** Si está operando en un entorno de despliegue de red, es muy recomendable asegurarse de que WebSphere Application Server para z/OS sincronice su configuración después de *cada* cambio en la consola de administración o de destino Ant.

Al guardar la configuración maestra asegúrese de forzar la sincronización manualmente a través de la consola de administración:

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. Marque los registros del sistema y/o WebSphere Application Server para z/OS para completar la sincronización. Estos mensajes pueden variar según el release de WebSphere Application Server para z/OS, pero deberá buscar algo parecido

a 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 los registros de Server Application Server para z/OS para garantizar el éxito;

## Configuración de un nodo

Antes de desplegar una aplicación el servidor debe estar configurado. Esto se realiza a través de la consola de administración del gestor de despliegue, y entonces 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 puede hacerse a través mandato **START** del operador **z/OS** adecuado para su instalación o el mandato `startNode.sh` en `profiles/<federated profile name>/bin` del directorio de instalación de WebSphere Application Server para z/OS.

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 24 describe la configuración manual para una instalación básica de WebSphere Application Server para z/OS y debe seguirse con las diferencias que se identifican a continuación. Al guardar la configuración maestra, asegúrese de sincronizar los cambios como se describe en el apartado “Sincronizar cambios” en la página 47.

“Configurar el módulo de inicio de sesión JAAS del sistema” en la página 32 detalla de la configuración de seguridad necesaria durante la configuración manual. Esta configuración requiere que se copie `Registry.jar` en un directorio de instalación de WebSphere Application Server para z/OS. Debe copiarse `Registry.jar` de `CuramSDEJ/lib` al directorio `lib` de la instalación del Gestor de despliegue y las instalaciones federadas que haya.

“Configurar el módulo de inicio de sesión JAAS del sistema” en la página 32 esta configuración de seguridad también requiere copiar `CryptoConfig.jar` al directorio `java64/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 la aplicación `.ear` para el despliegue vale la pena observar el `BOOTSTRAP_ADDRESS` del servidor en el que se instalará. `BOOTSTRAP_ADDRESS` se encuentra en la misma lista de puertos que `SOAP_CONNECTOR_ADDRESS` descrita anteriormente.

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



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

### **Despliegue en el nodo**

Por último, debe seguirse “Despliegue manual de aplicaciones” en la página 45 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, COMERCIALIZACIÓN 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. Ver 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.

© copyright 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](http://www.ibm.com) son marcas registradas de International Business Machines Corp. 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 la sección "Copyright and trademark information" del sitio <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 EE.UU. y/o en otros países.

UNIX es una marca registrada de The Open Group en EE.UU. y en otros países.

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

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





Impreso en España