Red Hat JBoss Enterprise Application Platform 7.1

7.1.0 Notas de lanzamiento

Para usar con Red Hat JBoss Enterprise Application Platform 7.1

Last Updated: 2018-01-11

Red Hat JBoss Enterprise Application Platform 7.1 7.1.0 Notas de lanzamiento

Para usar con Red Hat JBoss Enterprise Application Platform 7.1

Legal Notice

Resumen

Estas notas de lanzamiento cuentan con información importante relacionada con Red Hat JBoss Enterprise Application Platform 7.1.

Table of Contents

CAPÍTULO 1. ACERCA DE RED HAT JBOSS ENTERPRISE APPLICATION PLATFORM 7.1

Red Hat JBoss Enterprise Application Platform 7.1 (JBoss EAP) es una plataforma de middleware desarrollada con estándares abiertos y conforme a la especificación de Java Enterprise Edition 7.

JBoss EAP incluye una nueva estructura modular, la cual permite la habilitación de servicios solo cuando se requieran, mejorando así, la velocidad de arranque.

La consola administrativa y la interfaz de línea de comandos administrativa (CLI) hacen innecesaria la modificación de archivos de configuración XML y agregan la habilidad para utilizar scripts y automatizar tareas.

JBoss EAP proporciona dos modos operativos para instancias JBoss EAP: el servidor autónomo o el dominio administrado. El servidor autónomo representa la ejecución de JBoss EAP como una instancia de servidor sencilla. El modo operativo de dominio administrado permite la administración de múltiples instancias JBoss EAP desde un punto de control único.

Además, JBoss EAP 7 incluye APIs y marcos de trabajo de desarrollo para desarrollar rápidamente aplicaciones Java EE seguras y escalables.

CAPÍTULO 2. CONFIGURACIONES ADMITIDAS

Las siguientes configuraciones son recientemente compatibles con JBoss EAP 7.1.

- Sistemas operativos
  - Windows Server 2016 en arquitectura x86_64
    - Esto incluye el uso de JBoss EAP en Microsoft Azure en una máquina virtual Windows Server 2016.
- Bases de datos
  Las siguientes bases de datos fueron certificadas y ahora se admiten por completo:
  - SQL Server 2016
  - Sybase 16.0
  - MariaDB Galera Cluster 10.1
- Proveedores de JMS externos
  - Red Hat JBoss AMQ 7.0
  - IBM WebSphere MQ 8
- Servicios LDAP
  - Red Hat Directory Server 10.1
  - Microsoft Active Directory 2016
- Conectores nativos
  - Microsoft IIS 10
- Red Hat JBoss Developer Studio
  - JBoss EAP 7.1 está certificado para su uso con Red Hat JBoss Developer Studio 11.

Consulte la página Configuraciones admitidas de Red Hat JBoss Enterprise Application Platform (EAP) 7 para obtener información completa de la configuración admitida para JBoss EAP 7.1.

CAPÍTULO 3. NUEVAS FUNCIONES Y MEJORAS

3.1. SEGURIDAD Y ELYTRON

Elytron y el subsistema Elytron

El subsistema **`elytron`**, el cual se basa en el proyecto WildFly Elytron, es nuevo en JBoss EAP 7.1. Elytron es un marco de seguridad usado para unificar la seguridad en todo el servidor de aplicaciones. El subsistema **`elytron`** ofrece un único punto de configuración para asegurar las aplicaciones y las interfaces de administración. Ofrece un conjunto de API y SPI para crear implementaciones personalizadas de funcionalidad e integración. Para aprender más acerca de los diferentes componentes de Elytron, consulte la sección Conceptos y componentes básicos de la guía *Arquitectura de seguridad*.

El subsistema **`security`** de legado y la autenticación de administración principal de legado aún están presentes en JBoss EAP 7.1 y se utilizan de manera predeterminada. Puede encontrar información sobre cómo configurar el subsistema **`elytron`** en la sección Subsistema Elytron de *Cómo configurar la seguridad del servidor*.

Entre las funciones importantes del subsistema **`elytron`**, se incluye:

- Mecanismos de autenticación más sólidos para la autenticación de HTTP y SASL.
- Una arquitectura mejorada que permite que las identidades de seguridad se propaguen por dominios de seguridad y se transformen de manera transparente para que estén listas para la autorización. La transformación se lleva a cabo mediante decodificadores de roles configurables, asignadores de roles y asignadores de permisos.
- Un punto centralizado para la configuración de SSL/TLS, incluidos los suites de cifras y protocolos.
- Las optimizaciones de SSL/TLS como la construcción de identidad segura eager y la autorización de vinculación estrecha para establecer una conexión SSL/TLS. Esto permite que las verificaciones de permisos se produzcan antes de que se reciba la primera solicitud. La construcción de identidad segura de Eager elimina la necesidad de que la identidad segura se construya a pedido.
- Un almacén de credenciales seguro que reemplaza la implementación del vault de contraseñas de legado. El almacén de credenciales seguro puede almacenar varios tipos de credenciales cifradas, además de cadenas cifradas. Puede consultar más información sobre almacenes de credenciales en la sección Almacén de credenciales de *Cómo configurar la seguridad del servidor*. Con excepción del subsistema **`elytron`**, los vaults de contraseñas de legado nuevos y existentes aún se pueden usar con otros subsistemas.

Almacenes de credenciales

Puede configurar almacenes de credenciales en el subsistema **`elytron`** para JBoss EAP 7.1. Un almacén de credenciales permite un almacenamiento y uso de credenciales seguro, y tiene muchos beneficios en comparación con el uso de un vault de contraseñas de legado. Las credenciales almacenadas en un almacén pueden ser nombradas de manera segura por otros subsistemas de JBoss EAP. Esto evita que las credenciales, como las contraseñas, se almacenen en un texto plano. Para obtener más información, consulte Almacén de credenciales en *Cómo configurar la seguridad del servidor*.

Asignación de identidad para usuarios de administración autenticados

Al usar el subsistema **`elytron`** para asegurar las interfaces de administración, puede brindar un dominio de seguridad a las interfaces de administración para la asignación de identidad de usuarios

autenticados. Esto permite que los usuarios autenticados aparezcan con la identidad adecuada cuando inician sesión en las interfaces de administración. Para obtener más información, consulte Asignación de identidad para usuarios de administración autenticados en *Cómo configurar la seguridad del servidor*.

Creación de certificado autofirmado automático para aplicaciones

JBoss EAP 7.1 proporciona generación automática de un certificado autofirmado con propósitos de desarrollo para ámbitos de seguridad de legado. Para obtener más información, consulte Creación de certificado autofirmado automático para aplicaciones en *Cómo configurar la seguridad del servidor*.

Almacenamiento en caché para ámbitos de seguridad

Elytron proporciona un **`caching-realm`**, que le permite almacenar en caché los resultados de una búsqueda de credenciales desde un ámbito de seguridad. Por ejemplo, podría usarlo para configurar una memoria caché para credenciales que provienen de LDAP o una base de datos para aumentar el rendimiento de usuarios consultados frecuentemente. Para obtener más información, consulte Configurar almacenamiento en caché para ámbitos de seguridad en *Cómo configurar la administración de identidades*.

Inicio de sesión único gestionado por contenedor

Puede configurar JBoss EAP 7.1 para usar un inicio de sesión único gestionado por contenedor para aplicaciones mediante el método de autenticación **`FORM`** de Elytron. Esto permite a los usuarios autenticar una única vez y acceder a otros recursos seguros mediante el método de autenticación **`FORM`** sin tener que reautenticar. Para obtener más información, consulte Configurar aplicaciones para que usen el inicio de sesión único gestionado por contenedor en *Cómo configurar la administración de identidades*.

Propagación de identidades de seguridad para llamadas remotas

JBoss EAP 7.1 introduce la capacidad de configurar fácilmente el servidor y sus aplicaciones para propagar una identidad de seguridad de un cliente al servidor para llamadas remotas. También puede configurar componentes del servidor para ejecutar dentro de la identidad de seguridad de un usuario dado.

Para obtener más información, consulte Propagación de identidades de seguridad para llamadas remotas en *Cómo configurar la seguridad del servidor* para JBoss EAP.

Herramienta WildFly Elytron

JBoss EAP 7.1 incluye la herramienta WildFly Elytron, que le permite crear y modificar almacenes de credenciales sin tener que ejecutar el servidor JBoss EAP. También se puede usar para convertir vaults de contraseñas en almacenes de credenciales mediante la opción **`vault`**.

See Cree y modifique los almacenes de credenciales sin conexión con la herramienta WildFly Elytron en *Cómo configurar la seguridad del servidor* para obtener información sobre cómo usar la herramienta WildFly Elytron.

Script para habilitar Elytron en subsistemas aplicables e interfaces de administración

Se proporciona un script para habilitar el marco de trabajo de Elytron en subsistemas aplicables e interfaces de administración. Este script, **`enable-elytron.cli`** está disponible en el directorio ***`EAP_HOME`*`/docs/examples/`**. El uso de este script es opcional; Elytron también se puede habilitar en subsistemas individuales, según sea necesario. Para obtener más información, consulte Cómo Red Hat JBoss Enterprise Application Platform 7.1 maneja la seguridad preestablecida en la guía *Arquitectura de seguridad*.

Configuración del subsistema Elytron mediante la consola de administración

Para configurar el subsistema **`elytron`**, en la consola de administración, navegue a **Configuration** (Configuración) → **Subsystems** (Subsistemas) → **Security - Elytron** (Seguridad - Elytron). Para obtener más información, consulte Elytron Subsystem (Subsistema Elytron) en *Cómo configurar la seguridad del servidor*.

Integración de Elytron con los subsistemas JBoss EAP

En JBoss EAP 7.1, puede usar Elytron para garantizar diferentes aspectos de los siguientes subsistemas JBoss EAP:

`batch-jberet`

Puede configurar el subsistema **`batch-jberet`** para ejecutar trabajos por lotes mediante un dominio de seguridad de Elytron. Para obtener más información, consulte Configurar la seguridad para los trabajos por lotes en la *Guía de configuración*.

`datasources`

Puede usar un almacén de credenciales o un dominio de seguridad de Elytron para proporcionar información de autenticación en una definición de fuente de datos. Para obtener más información, consulte Seguridad de fuente de datos en la *Guía de configuración*.

`ejb3`

Puede crear asignaciones para dominios de seguridad de Elytron en el subsistema **`ejb3`** para que las implementaciones hagan referencia a ellas. Para obtener más información, consulte Integración de Elytron con el subsistema EJB en *Desarrollo de aplicaciones EJB*.

`iiop-openjdk`

Puede configurar el subsistema **`iiop-openjdk`** para usar SSL/TLS a fin de proteger la comunicación entre clientes y servidores. Para obtener más información, consulte Configurar IIOP para usar SSL/TLS con el subsistema Elytron en la *Guía de configuración*.

`jca`

Puede usar el atributo **`elytron-enabled`** para habilitar la seguridad de Elytron para un gerente de trabajo. Para obtener más información, consulte Configuración del subsistema JCA en la *Guía de configuración*.

`jgroups`

Puede configurar los protocolos **`SYM_ENCRYPT`** y **`ASYM_ENCRYPT`** para hacer referencia a los almacenes de claves o de credenciales definidos en el subsistema **`elytron`**. El protocolo **`AUTH`** también se puede configurar para hacer referencia a los almacenes de claves y de credenciales gestionados por elytron. Para obtener más información, consulte Protección de clúster en la *Guía de configuración*.

`mail`

Puede usar un almacén de credenciales para proporcionar contraseñas para el subsistema **`mail`**. Para obtener más información, consulte Uso de un almacén de credenciales para contraseñas en la *Guía de configuración*.

`messaging-activemq`

Puede usar la seguridad de Elytron para proteger el subsistema **`messaging-activemq`**. Para obtener más información, consulte la sección Uso del subsistema Elytron de la *Configuración de mensajería*.

`modcluster`

Puede usar un cliente Elytron **`ssl-context`** para comunicarse con un balanceador de carga mediante SSL/TLS. Para obtener más información, consulte Integración de Elytron con el subsistema ModCluster en *Cómo configurar la seguridad del servidor*.

`remoting`

Puede configurar conexiones entrantes y salientes en el subsistema **`remoting`** para hacer referencia a contextos de autenticación, fábricas de autenticación de SASL y contextos de SSL definidos en el subsistema **`elytron`**. Para obtener más información, consulte Integración de Elytron con el subsistema remoto en *Cómo configurar la seguridad del servidor*.

`resource-adapters`

Puede proteger las conexiones al adaptador de recursos mediante Elytron. Puede habilitar el flujo entrante de seguridad para establecer las credenciales de seguridad al enviar trabajo para ser ejecutado por el gerente de trabajo. Para obtener más información, consulte Configurar adaptadores de recursos para usar el subsistema Elytron en la *Guía de configuración*.

`undertow`

Puede usar el subsistema elytron para configurar la autenticación de SSL/TLS y de la aplicación. Para obtener más información, consulte Uso de SSL/TLS en *Cómo configurar la seguridad del servidor* y Configurar aplicaciones web para usar Elytron o la seguridad de legado para la autenticación en *Cómo configurar la administración de identidades*.

3.2. ADMINISTRACIÓN DE SERVIDORES

Inicio de servidores en estado de suspensión

Durante el proceso de inicio, los servidores de JBoss EAP 7.1 permanecen en estado de suspensión hasta que todos los servicios se hayan iniciado. En este estado, el servidor no acepta ninguna solicitud. Una vez iniciados todos los servicios requeridos, el servidor se colocará en un estado de ejecución normal para comenzar a aceptar solicitudes.

También es posible iniciar servidores en estado de suspensión y mantenerlos suspendidos hasta que se invoque la operación **`resume`**. Para iniciar el servidor en estado de suspensión, establezca el argumento **`start-mode`** en **`suspend`** para la operación adecuada.

- Para un servidor autónomo, pase el argumento **`--start-mode=suspend`** al script **`standalone.sh`**:

  Ejemplo: Iniciar un servidor autónomo en estado de suspensión

  ```
  $ EAP_HOME/bin/standalone.sh --start-mode=suspend
  ```

- En un dominio administrado, pase el argumento **`start-mode=suspend`** a la operación CLI de administración **`start`**:

  Ejemplo: Iniciar un servidor de dominio administrado en estado de suspensión

  ```
  /host=HOST_NAME/server-config=SERVER_NAME:start(start-mode=suspend)
  ```

Monitoreo de los eventos de ciclo de vida del servidor mediante el subsistema de administración de núcleos

En JBoss EAP 7.1, puede registrar un agente de escucha en el subsistema **`core-management`** de JBoss EAP para monitorear eventos de ciclo de vida del servidor. Para obtener más información, consulte Eventos de ciclo de vida del servidor del monitor mediante el subsistema de administración de núcleos en la *Guía de configuración*.

Monitoreo de los eventos de ciclo de vida del servidor mediante notificaciones de JMX

En JBoss EAP 7.1, puede registrar un agente de escucha de notificaciones de JMX para que monitoree los eventos de ciclo de vida del servidor. Para obtener más información, consulte Monitoreo de los eventos de ciclo de vida del servidor mediante notificaciones de JMX en la *Guía de configuración*.

Control y visualización de cambios de configuración de la CLI de administración

En un dominio administrado, los cambios de configuración se controlan a nivel del host para modificaciones relacionadas con el host y el servidor. Permitir cambios de configuración para un controlador de host lo activa para todos sus servidores administrados. La configuración del control de

cambios de configuración se movió al subsistema **`core-management`**. Para obtener más información, consulte Ver cambios de configuración en la *Guía de configuración*.

Monitoreo de estadísticas del trabajador

Puede ver las estadísticas del tiempo de ejecución del trabajador mediante la CLI de administración. Esto expone las estadísticas del trabajador, como el conteo de conexiones, el conteo de hilos y el tamaño de la cola.

El siguiente comando muestra estadísticas de tiempo de ejecución para el trabajador predeterminado:

```
/subsystem=io/worker=default:read-resource(include-
runtime=true,recursive=true)
```

Para obtener más información, consulte Configuración de trabajadores en la *Guía de ajuste de rendimiento*.

Monitoreo mejorado de recursos para controladores de host esclavos

En JBoss EAP 7.1, los controladores de host configurados como esclavos pueden ignorar los recursos no requeridos en la configuración de todo el dominio. Los recursos pueden ser irrelevantes si no están asociados con los servidores gestionados por los controladores de host esclavos.

Para ignorar la configuración no utilizada, establezca el atributo **`ignore-unused-configuration`** en **`true`** en la configuración de conexión del controlador de host de JBoss EAP 7.0 para el controlador de dominio remoto. De manera predeterminada, no se define el atributo **`ignore-unused-configuration`**.

Para obtener más información y una configuración de ejemplo, consulte Configurar un controlador de dominio de JBoss EAP 7.1 para administrar instancias de JBoss EAP 7.0 en la *Guía de configuración*.

También puede usar la etiqueta de línea de comando **`--backup`** junto con **`ignore-unused-configuration`** establecido en **`true`**, que permite que un controlador de host esclavo comience a usar una copia de seguridad de la configuración de dominio si el controlador de dominio no está disponible. El controlador de host esclavo no solicita que lo realice el **`domain.xml`** completo.

Los controladores de host comenzaron a usar una configuración almacenada en caché para reconectarse automáticamente al controlador de dominio

En JBoss EAP 7.1, un controlador de host que se inició mediante una configuración almacenada en caché porque no se podía establecer comunicación con el controlador de dominio, se reconectará automáticamente una vez que el controlador de dominio se vuelva disponible.

Establecer la configuración regional del servidor

Puede usar la propiedad **`org.jboss.logging.locale`** para sobrescribir la configuración regional de los mensajes registrados mediante JBoss Logging, incluidos los mensajes de JBoss EAP y sus dependencias.

Para obtener más información, consulte Establecer la configuración regional del servidor mediante la propiedad org.jboss.logging.locale en la *Guía de configuración*.

Nuevo atributo: parse-group-name-from-dn

En JBoss EAP 7.1, el atributo **`parse-group-name-from-dn`** ahora está disponible en **`/core-service=management/security-realm=realm/authorization=ldap/group-search=principal-to-group`**. Se brinda el atributo en lugar de la propiedad del sistema **`org.jboss.as.domain.management.security.parseGroupNameFromLdapDN`**.

Para obtener más información, consulte Habilitación del dominio de seguridad de LDAP para analizar roles de una DN en la *Guía de migración*.

Administración de JBoss EAP mediante la red de operaciones JBoss

Puede monitorear los servidores de JBoss EAP 7.1 y administrar su configuración mediante la red de operaciones Red Hat JBoss.

IMPORTANTE

La red de operaciones JBoss no incluye soporte para configurar el nuevo subsistema **`elytron`** de JBoss EAP 7.1. El soporte de monitoreo está limitado a las funciones del plugin JBoss EAP de la Red de operaciones de JBoss, disponibles para JBoss EAP 6.4, además de los subsistemas **`undertow`**, **`iiop-openjdk`**, **`io`** y **`messaging-activemq`** de JBoss EAP.

3.3. CLI ADMINISTRATIVA

Desplegar y guardar anexos

En JBoss EAP 7.1, puede usar el comando **`attachment`** para visualizar o guardar el contenido de un flujo anexo. Esto funciona para recursos de administración que pueden exponer contenido como flujo.

Use el siguiente comando de CLI de administración para ver el contenido de un anexo:

```
attachment display --operation=/subsystem=logging/log-
file=server.log:read-attribute(name=stream)
```

Use el siguiente comando de CLI de administración para guardar el contenido de un anexo en un archivo:

```
attachment save --operation=/subsystem=logging/log-file=server.log:read-
attribute(name=stream) --file=test.log
```

NOTA

Si no se ingresa un nombre de archivo, entonces se usa ***`EAP_HOME`*`/bin/`*`STREAM_UUID`*** como ruta del archivo.

Consulte Mostrar el contenido de un adjunto y Guardar el contenido de un anexo en la *Guía de CLI de administración*.

Anexo de archivos a operaciones de administración

En JBoss EAP 7.1, puede usar la CLI de administración para anexar un archivo a una operación de administración. Puede usar la operación **`add-content`** para añadir contenido a una implementación ampliada existente o la operación **`remove-content`** para eliminar el contenido. Por ejemplo:

```
/deployment=test.war:add-content(content=[{input-stream-
index=/path/to/a.txt,target-path=a.txt}])
```

Puede usar la operación **`browse-content`** para explorar el contenido de una implementación.

Establecer un tiempo de expiración para comandos

JBoss EAP 7.1 le permite establecer el tiempo máximo, en segundos, para esperar que se complete un comando de CLI. Un valor de **0** significa que no hay un tiempo de expiración. De manera predeterminada, no hay tiempo de expiración. Por ejemplo:

```
command-timeout set 30
```

Incluya la solicitud y el comando en el resultado en modo no interactivo

En JBoss EAP 7.1, el argumento **--echo-command** muestra la solicitud y el comando con el resultado para comandos ejecutados en modo no interactivo. Esto puede ser útil al resolver fallas haciendo coincidir el resultado del comando que se ejecutó.

```
$ EAP_HOME/bin/jboss-cli.sh --connect --file=/path/to/cli_commands.txt --
echo-command
```

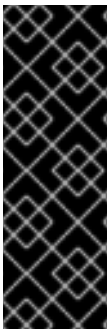
El comando y su resultado se visualizan a medida que se ejecuta.

```
[standalone@localhost:9990 /] :read-attribute(name=running-mode)
{
    "outcome" => "success",
    "result" => "NORMAL"
}
[standalone@localhost:9990 /] ls /deployment
helloworld.war
```

Especificar dependencias exportadas para un módulo personalizado

JBoss EAP 7.1 ofrece un argumento **--export-dependencies** para especificar las dependencias exportadas para un módulo. Por ejemplo:

```
module add --name=com.mysql --resources=/path/to/mysql-connector-java-
5.1.36-bin.jar --export-dependencies=javax.api,javax.transaction.api
```



IMPORTANTE

El uso del comando **module** de la CLI de administración para añadir y eliminar módulos se ofrece como muestra de tecnología únicamente. Este comando no es adecuado para su uso en un dominio administrado o al conectarse a la CLI de administración de manera remota. Los módulos se deben añadir y eliminar en forma manual en un entorno de producción. Para obtener más información, consulte las secciones Crear un módulo personalizado en forma manual y Eliminar un módulo personalizado en forma manual de la *Guía de configuración* de JBoss EAP.

Establecer un directorio de módulo alternativo durante la creación del módulo

Si ha definido un directorio de módulos JBoss EAP externo para usar en lugar del directorio ***EAP_HOME*/modules/** predeterminado, puede usar el argumento **--module-root-dir** para especificar el directorio a usar durante la creación del módulo.

```
module add --module-root-dir=/path/to/my-external-modules/ --
name=com.mysql --resources=/path/to/mysql-connector-java-5.1.36-bin.jar --
dependencies=javax.api,javax.transaction.api
```

IMPORTANTE

El uso del comando **`module`** de la CLI de administración para añadir y eliminar módulos se ofrece como muestra de tecnología únicamente. Este comando no es adecuado para su uso en un dominio administrado o al conectarse a la CLI de administración de manera remota. Los módulos se deben añadir y eliminar en forma manual en un entorno de producción. Para obtener más información, consulte las secciones Crear un módulo personalizado en forma manual y Eliminar un módulo personalizado en forma manual de la *Guía de configuración* de JBoss EAP.

Inicio de una sesión de CLI de administración mediante la JDK de IBM

Los scripts **`jboss-cli`** establecen la propiedad **`com.ibm.jsse2.overrideDefaultTLS`** en **`true`**. Esta configuración es importante si usa IBM JDK, para evitar problemas de autenticación al usar SSL configurado por Elytron. Asegúrese de establecer esta propiedad si usa IBM JDK y usa otro método para iniciar una sesión de CLI, por ejemplo, de manera programática, mediante las clases disponibles en ***`EAP_HOME`*`/bin/client/jboss-cli-client.jar`**.

3.4. CONSOLA ADMINISTRATIVA

Actualizaciones de implementación de aplicaciones

JBoss EAP 7.1 incluye una interfaz de usuario actualizada para administrar las implementaciones de aplicaciones. En la pestaña **Deployments** (Implementaciones) de la consola de administración ahora se incluyen las siguientes funciones de implementaciones:

- Una opción desplegable **Explode** (Expandir), que le permite descomprimir una implementación deshabilitada.
- Una opción desplegable **Browse Content** (Explorar contenido), que le permite explorar los archivos en la implementación. No se admite la navegación.
- Detalles acerca de si la aplicación es un archivo o una implementación ampliada.

Soporte de monitoreo de transacciones

JBoss EAP 7.1 ofrece métricas del subsistema **`transactions`** mejoradas, así como métricas de recursos de transacciones JDBC y JMS en la consola de administración.

Visualización y administración de transacciones preparadas de mensajería

Puede usar la consola de administración para ver, asignar o revertir transacciones preparadas para el subsistema **`messaging-activemq`**. Para obtener más información, consulte Administrar transacciones preparadas mediante la consola de administración en *Configuración de mensajería*.

Sugerencias de campo de texto

A medida que escribe en algunos campos de texto en la consola de administración, los valores de otra parte de la configuración pueden aparecer como sugerencias.

Adición de un puente de JMS

Para añadir un puente de JMS, en la consola de administración, navegue a **Configuration** (Configuración) → **Subsystems** (Subsistemas) → **Messaging - ActiveMQ** (Mensajería - ActiveMQ) → **JMS Bridge** (Puente de JMS) → **View** (Vista) → **Add** (Añadir). Proporcione la información requerida y haga clic en **Save** (Guardar).

Control y visualización de cambios de configuración

Para permitir el control de los cambios de configuración de la consola de administración, navegue a la pestaña **Runtime** (Tiempo de ejecución), seleccione el host de servidor autónomo o dominio administrado, y seleccione **Configuration Changes** (Cambios de configuración) del menú desplegable.

Haga clic en el botón **Enable** (Habilitar) y proporcione un valor histórico máximo.

A continuación, la tabla que se encuentra en esta página enumera cada cambio de configuración realizado, con la fecha, el origen, el resultado y los detalles de la operación.

Configuración de filtros

Para configurar los filtros de Undertow mediante la consola de administración, navegue a **Configuration** (Configuración) → **Subsystems** (Subsistemas) → **Web/HTTP - Undertow** → **Filters** (Filtros) → **View** (Vista).

Administración de trabajos por lotes

En JBoss EAP 7.1, puede administrar trabajos por lotes de la consola de administración. Navegue a la pestaña **Runtime** (Tiempo de ejecución), seleccione el servidor y seleccione **Subsystems** (Subsistemas) → **Batch** (Lote) → **View** (Vista). Abra la pestaña **Jobs** (Trabajos) e inicie, detenga o reinicie los trabajos según sea necesario.

Prueba de las conexiones de fuentes de datos

Al usar el asistente **Create Datasource** (Crear fuente de datos) en la consola de administración, tiene la oportunidad de probar la conexión antes de crear la fuente de datos. En la pantalla **Test Connection** (Probar conexión) del asistente, haga clic en el botón **Test Connection** (Probar conexión).

Uso de plantillas de fuente de datos

Al crear una fuente de datos mediante la consola de administración, el asistente **Create Datasource** (Crear fuente de datos) proporciona plantillas con valores predeterminados para las bases de datos admitidas. Esto ahora es compatible con JBoss EAP 7.1.

Soporte de subsistema

En JBoss EAP 7.1, ahora se admite la configuración de los siguientes subsistemas mediante la consola de administración:

- BeanValidation
- IO
- Jaxrs
- Jdr
- Jsf
- Jsr77
- Nombrado
- Pojo
- Remoto
- RequestController
- Sar
- Seguridad - Elytron
- Singleton
- Weld

3.5. SERVIDOR WEB

Soporte de HTTP/2

JBoss EAP 7.1 admite HTTP/2 seguro en todos los sistemas operativos compatibles, con la excepción de HP-UX. Existen dos formas admitidas de habilitar HTTP/2 en JBoss EAP 7.1:

- Uso del soporte interno de JBoss EAP 7.1 para ALPN, que utiliza la API de reflexión. Esto funciona de manera preestablecida, pero está limitado solamente a OpenJDK y Oracle JDK.
- Uso del soporte ALPN de la nueva JBoss Core Services OpenSSL, que trabaja en todos los sistemas operativos compatibles, con la excepción de HP-UX.
  - Puede descargar JBoss Core Services OpenSSL de la página de descarga de JBoss Core Services OpenSSL.

3.6. REGISTRO

Informes mejorados para errores de arranque causados por archivos de configuración del servidor no válidos

Antes de JBoss EAP 7.1, los errores de arranque que se producían al analizar archivos de configuración del servidor no válidos proporcionaban poca retroalimentación y eran difíciles de depurar. JBoss EAP 7.1 usa análisis de XSD para producir más mensajes de error informativos al encontrar errores de análisis de XML. Ahora muestra dónde ocurrió el error, proporciona retroalimentación sobre el error de validación y, de ser posible, obtiene y muestra documentación de soporte de la XSD para describir el problema. La validación mejorada de la configuración de XML no incluye descriptores de implementaciones.

El registro del servidor incluye información sobre parches

La información relacionada con parches ahora se registra en el archivo **`server.log`** durante el inicio. Esta información es útil al depurar problemas.

3.7. IMPLEMENTACIONES

Gestión de implementaciones ampliadas

En JBoss EAP 7.1, puede crear implementaciones administradas ampliadas y manipular su contenido mediante operaciones de administración de implementaciones.

Para obtener más información, consulte Administración de implementaciones ampliadas en la *Guía de configuración*.

Soporte para explorar el repositorio de contenido

En JBoss EAP 7.1, puede ver el contenido de las implementaciones administradas mediante las operaciones de administración de implementaciones. Para obtener más información, consulte Visualización del contenido de las implementaciones en la *Guía de configuración*.

Dejar de implementar todas las implementaciones

En JBoss EAP 7.1, ahora puede dejar de implementar todas las implementaciones de la CLI de administración mediante el uso de un comodín (**`*`**). Por ejemplo:

```
undeploy *
```

Reimplementación de todas las implementaciones deshabilitadas

En JBoss EAP 7.1, ahora puede implementar todas las implementaciones deshabilitadas de la CLI de administración mediante el uso de un comodín (**`*`**). Por ejemplo:

```
deploy --name=*
```

3.8. CARGA DE CLASES

Uso de rutas absolutas para recursos en archivos module.xml

En JBoss EAP 7.1, ahora se admite el uso de rutas absolutas en el elemento de ruta **`resource-root`** del archivo **`module.xml`** para módulos. Esto le permite acceder a sus librerías de recursos sin tener que moverlos al directorio ***`EAP_HOME`*`/modules/`**.

3.9. NOMBRADO

Cambio de vinculaciones de JNDI de manera dinámica

En JBoss EAP 7.1, puede usar la operación **`rebind`** para actualizar las vinculaciones JNDI de manera dinámica sin necesitar recargar o reiniciar los servicios. No obstante, esto no funciona para vinculaciones de contexto externas, ya que requieren el reinicio de los servicios.

Para obtener más información, consulte la sección Cambiar en forma dinámica las vinculaciones de JNDI de la *Guía de configuración*.

3.10. TRANSACCIONES

Cierre correcto de transacciones

Una vez suspendido, el servidor no aceptará nuevas solicitudes, pero a las transacciones y solicitudes en vuelo se les permite continuar hasta que se completen o haya transcurrido el tiempo de expiración. Esto también se aplica para solicitudes de servicio web relacionadas con una transacción XTS. Consulte Suspender y apagar JBoss EAP correctamente en la *Guía de configuración* para más información.

Monitoreo de transacciones mejorado

JBoss EAP 7.1 ofrece estadísticas mejoradas para recursos de transacción en los subsistemas **`datasources`**, **`transactions`** y **`messaging-activemq`**.

Consulte Estadísticas de fuentes de datos y Ver estadísticas de transacciones en la *Guía de configuración*, y Monitoreo de estadísticas de mensajería en *Configuración de mensajería* para información sobre la visualización de las estadísticas disponibles.

Olvide la llamada al borrar la transacción

Al usar la operación **`delete`** en un registro de transacción, la llamada **`forget`** se activa para que los registros del proveedor de recursos XA se limpien correctamente. Para obtener más información y saber cómo configurar el comportamiento de la llamada **`forget`**, consulte Eliminar una transacción en la *Guía de configuración*.

3.11. JCA

Soporte del administrador de trabajo distribuido

JBoss EAP 7.1 admite el uso de administradores distribuidos para reprogramar la ejecución del trabajo en otra instancia del administrador de trabajo. Para obtener más información, consulte la sección Administradores de trabajo distribuidos de la *Guía de configuración*.

3.12. FUENTES DE DATOS

Vaciado de conexiones de fuentes de datos

Puede vaciar las conexiones de fuentes de datos mediante la CLI de administración o la consola de administración. Para obtener más información, consulte la sección Vaciar las conexiones de la fuente de datos de la *Guía de configuración*.

El registro de rastros de alistamiento está deshabilitado

En JBoss EAP 7.1, de manera predeterminada, el atributo **`enlistment-trace`** se establece como **`false`** para las fuentes de datos. Puede habilitar el registro de rastros de alistamiento estableciendo el atributo **`enlistment-trace`** como **`true`**.

AVISO

Permitir el rastreo de enlistamiento facilita la detección de errores durante el enlistamiento de la transacción, pero viene con un impacto de rendimiento.

3.13. ADAPTADORES DE RECURSOS

Configuración del adaptador de recursos genérico JMS

JBoss EAP 7.1 le permite configurar un adaptador de recursos genérico JMS para su uso con proveedores de JMS.

Vaciar conexiones del adaptador de recursos

Puede vaciar las conexiones del adaptador de recursos mediante la CLI de administración. Para obtener más información, consulte la sección Vaciar las conexiones del adaptador de recursos de la *Guía de configuración*.

El registro de rastros de alistamiento está deshabilitado

En JBoss EAP 7.1, de manera predeterminada, el atributo **`enlistment-trace`** se establece como **`false`** para los adaptadores de recursos. Puede habilitar el registro de rastros de alistamiento estableciendo el atributo **`enlistment-trace`** como **`true`**.

AVISO

Permitir el rastreo de enlistamiento facilita la detección de errores durante el enlistamiento de la transacción, pero viene con un impacto de rendimiento.

3.14. EJB

Soporte de Singleton MDB agrupada

JBoss EAP 7.1 ahora admite el uso de Singleton MDB agrupados. Cuando se identifica un MDB como un Singleton agrupado e implementado en un clúster, solo estará activo únicamente en un nodo a la vez. Cuando el nodo de servidor falla o es apagado, el Singleton MDB agrupado se activa en un nodo diferente y comienza a consumir mensajes en dicho nodo.

Para obtener más información, consulteSingleton MDB agrupados en *Desarrollo de aplicaciones EJB*.

Rebalanceo de todas las conexiones entrantes de MDB

En JBoss EAP 7.0, puede usar la propiedad de configuración de activación **`rebalanceConnections`** para que las MDB permitan el rebalanceo de todas las conexiones MDB entrantes cuando cambian los cambios de topología de clúster Artemis.

En JBoss EAP 7.1, ahora puede establecer este comportamiento mediante el atributo **`rebalance-connections`** en las configuraciones **`pooled-connection-factory`** en el subsistema **`messaging-activemq`**.

Compatibilidad del cliente EJB de legado

JBoss EAP 7.1 se envía con dos clientes EJB:

Cliente EJB

El nuevo cliente EJB es mayormente, pero no completamente, compatible con versiones anteriores del cliente EJB de JBoss EAP 7.0. Este cliente EJB admite el cambio dinámico de identidad y las capacidades remotas fueron mejoradas para admitir múltiples identidades en una única conexión, en lugar de requerir una nueva conexión por identidad.

Cliente EJB de legado

El cliente EJB de legado proporciona compatibilidad binaria completa con versiones anteriores. Este cliente EJB de legado se puede ejecutar con las aplicaciones del cliente que se recopilaron en un principio mediante el cliente EJB de JBoss EAP 7.0. Todas las API presentes en el cliente EJB para JBoss EAP 7.0 están presentes en el cliente EJB de legado para JBoss EAP 7.1.
Para obtener más información, consulte Compatibilidad del cliente EJB de legado en *Desarrollo de aplicaciones EJB*.

Simplificación del código del cliente EJB

En JBoss EAP 7.1, puede simplificar el código del cliente EJB al invocar los componentes en clústeres del lado del servidor EJB.

Para obtener más información, consulte Simplificación del código del cliente EJB en *Desarrollo de aplicaciones EJB*.

Configuración de la dirección del cliente EJB

En JBoss EAP 7.1, puede vincular el socket del cliente EJB a una dirección y un puerto particulares. A continuación, el EJB objetivo puede leer la dirección y el puerto de origen del cliente remoto que lo invocó.

Para obtener más información, consulte Configurar la dirección del cliente EJB en *Desarrollo de aplicaciones EJB*.

ArtifactID única para las dependencias de jboss-ejb-client

Incluida la dependencia **`jboss-ejb-client`**, con su versión gestionada mediante **`wildfly-ejb-client-bom`**, incluye todas las dependencias requeridas para el cliente EJB.

En los lanzamientos previos de JBoss EAP, las dependencias debían incluirse manualmente en **`pom.xml`**. En JBoss EAP 7.1, esto no es necesario.

Para obtener más información, consulte Dependencias del proyecto para clientes EJB remotos en *Desarrollo de aplicaciones EJB*.

Soporte de expresión regular en vinculaciones de interceptor

En JBoss EAP 7.1, puede establecer el atributo **`allow-ejb-name-regex`** del subsistema **`ejb3`** en **`true`** para permitir expresiones regulares en vinculaciones de interceptor. Esto permite que los interceptores se asignen a todos los beans que coinciden con la expresión regular especificada.

Para obtener más información, consulte Configurar un interceptor de contenedores en *Desarrollo de aplicaciones EJB*.

3.15. JSF

Soporte Multi-JSF

JBoss EAP 7.1 proporciona soporte completo para Multi-JSF. Esta función permite a un usuario reemplazar la implementación de JSF provista con JBoss EAP por una implementación JSF suministrada por el usuario. Esta función también permite a un usuario instalar implementaciones de JSF múltiple y cambiar fácilmente la implementación predeterminada.

Tenga en cuenta que el siguiente problema puede producirse al brindar e instalar sus propias implementaciones de JSF:

Mojarra/MyFaces 2.1.x/2.0.x

JBoss EAP 7 es una implementación certificada de Java EE 7. No obstante, si instala una implementación JSF alternativa de versión 2.1 o posterior, JBoss EAP 7 ya no cumple con Java EE 7. Estas versiones anteriores cumplen con la especificación de JSF 2.0 definida en JSR-314, por lo que faltarán las funciones de la especificación JSF 2.2 definidas en JSR-344.

Para obtener más información, consulte Implementación Multi-JSF de JavaServer Faces en la *Guía de configuración*.

3.16. HIBERNATE

Actualizado a Hibernate ORM 5.1

JBoss EAP 7.1 ahora incluye Hibernate ORM 5.1. La versión 5.1 de Hibernate ORM incluye muchas mejoras de rendimiento y correcciones de errores. También presenta las siguientes nuevas funciones y mejoras:

Funciones Hibernate ORM 5.1

- En Hibernate Query Language (HQL), puede definir un vínculo a una entidad, no solo una asociación asignada. Por ejemplo:

```
select ...
from FinancialRecord f
    left join User u
        on r.lastUpdateBy = u.username
```

- Además de ofrecer la capacidad de cargar una única identidad por identificador, la API ahora también respalda la carga de múltiples entidades del mismo tipo por identificador mediante la interfaz **`Session`** de la API nativa Hibernate. Por ejemplo:

```
// Cargue los usuarios 1, 2 y 3 de una única vez
List<User> users = session.byMultipleIds(User.class).multiLoad( 1,
2, 3 );
```

- Esta versión ofrece mejoras en la integración de CDI, incluidas las soluciones al problema que se produce cuando Hibernate intenta acceder a la CDI **`BeanManager`** prematuramente. Para obtener más información, consulte HHH-8706 y HHH-10477.

- Al definir una consulta de auditoría Envers, ahora puede hacer referencias en asociaciones de uno a uno y muchos a uno.

Actualizado a Hibernate Validator 5.3.x

JBoss EAP 7.1 ahora incluye Hibernate Validator 5.3.x. Entre lo más destacado, se incluye lo siguiente:

- Correcciones de errores
- La capacidad de agregar cargas útiles dinámicas a violaciones de restricción
- Una nueva API programática para definición y declaración de restricciones
- Nuevas traducciones de los mensajes de restricciones incorporados

Para obtener más información, consulte la sección Nuevas funciones de de Hibernate Validator 5.3.x en la *Guía de desarrollo*.

Acceso a propiedades de asociaciones en consultas de Envers

En JBoss EAP 7.1, puede acceder a propiedades de entidades asociadas en consultas de Envers. Para obtener más información, consulte Cruzar asociaciones de entidades mediante propiedades de entidades a las que se hace referencia en *Desarrollo de aplicaciones Hibernate*.

Definir grupos de obtención de atributos de carga perezosa

En JBoss EAP 7.1, si usa carga perezosa mejorada de bytecode, puede definir los grupos de atributos que se deben obtener cuando se accede a uno del grupo. Para obtener más información, consulte Carga perezosa de atributos en *Desarrollo de aplicaciones Hibernate*.

3.17. ALTA DISPONIBILIDAD

Nuevo perfil del equilibrador de carga

JBoss EAP 7.1 incluye un nuevo perfil de balanceador de carga preconfigurado para permitir que un servidor se ejecute como balanceador de carga. El archivo de configuración del servidor autónomo para este perfil es **`standalone-load-balancer.xml`**, ubicado en el directorio ***`EAP_HOME`*`/standalone/configuration/`**. El perfil del dominio administrado es **`load-balancer`** y está definido en el archivo ***`EAP_HOME`*`/domain/configuration/domain.xml`**. Para obtener información sobre el uso de este perfil, consulte Configurar Undertow como balanceador de carga mediante mod_cluster en la *Guía de configuración*.

3.18. RESTEASY

Visualizar los detalles de recursos de extremos de REST

En JBoss EAP 7.1, puede usar la operación **`read-resource`** de la CLI de administración en el subsistema **`jaxrs`** para que las implementaciones consulten información acerca de los extremos de RESTEasy. Para obtener más información, consulte Visualización de extremos de RESTEasy en *Desarrollo de aplicaciones de servicios web*.

Soporte de módulo Jackson para Java 8

JBoss EAP 7.1 ofrece soporte para los módulos Jackson necesarios para funciones Java 8. Para obtener más información, consulte Soporte de módulo Jackson para Java 8 en *Desarrollo de aplicaciones de servicios web*.

Soporte de filtro JSON

En JBoss EAP 7.1, puede anotar clases con **`@JsonFilter`** para realizar filtrado dinámico. Para obtener más información, consulte Soporte de JsonFilter en RESTEasy Jackson2 en *Desarrollo de aplicaciones de servicios web*.

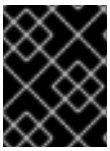
Registro de Proveedores e Interceptores de RESTEasy

RESTEasy registra los proveedores e interceptores a nivel de registro **DEBUG**. Para obtener más información, consulte Registro de proveedores e interceptores RESTEasy en *Desarrollo de aplicaciones de servicios web*.

3.19. MENSAJERÍA

Mensajería de almacén de persistencia JDBC

En JBoss EAP 7.1, puede usar JDBC para persistir mensajes y vincular datos a una base de datos, en lugar del registro predeterminado basado en archivos.



IMPORTANTE

JBoss EAP 7.1 actualmente admite solo Oracle Database 12c y excluye las topologías de alta disponibilidad (HA).

Para obtener más información, consulte la sección Persistencia del registro de mensajería mediante una base de datos JDBC de *Configuración de mensajería*.

Establecer el tamaño del conjunto de hilos del cliente mediante propiedades del sistema

Las siguientes propiedades se pueden usar para establecer el tamaño del conjunto de hilos global de un cliente y el conjunto global de hilos programados.

- `activemq.artemis.client.global.thread.pool.max.size`
- `activemq.artemis.client.global.scheduled.thread.pool.core.size`

Para obtener más información, consulte la sección Administración de hilos del cliente de *Configuración de mensajería*.

Acceda a un agente AMQ mediante el adaptador de recursos ActiveMQ Artemis integrado

Puede usar el adaptador de recursos ActiveMQ Artemis integrado en el subsistema **`messaging-activemq`** de JBoss EAP para acceder a un agente Red Hat JBoss AMQ 7 externo.

Para obtener más información, consulte la sección Uso del adaptador de recursos Artemis integrado para conexiones remotas en *Configuración de mensajería*.

3.20. CONFIGURACIÓN DEL CLIENTE

Archivo de configuración del nuevo cliente

JBoss EAP 7.1 introduce un archivo de configuración **`wildfly-config.xml`** que le permite especificar diferentes configuraciones de clientes, como EJB, la autenticación de Elytron, y acceso remoto en un único archivo de configuración.

Consulte Configuración de cliente mediante el archivo wildfly-config.xml en la *Guía de desarrollo* para obtener información sobre los clientes y tipos de configuración que se pueden realizar utilizando el archivo **`wildfly-config.xml`**.

3.21. HERRAMIENTA DE MIGRACIÓN DEL SERVIDOR JBOSS

Herramienta de migración del servidor JBoss disponible

La herramienta de migración del servidor JBoss ahora está disponible con la distribución JBoss EAP 7.1. Esta lo asiste en migrar su configuración de servidor de JBoss EAP 6.4 o 7.0 a JBoss EAP 7.1. Puede convertir el servidor autónomo y las configuraciones de dominio administrado.

Para obtener más información sobre el uso de la herramienta de migración del servidor JBoss, consulte Usar la herramienta de migración del servidor JBoss para migrar configuraciones del servidor en la *Guía de migración* de JBoss EAP.

3.22. DOCUMENTACIÓN

Guía de ajuste de rendimiento disponible

La *Guía de ajuste de rendimiento* ahora está disponible para JBoss EAP 7.1. En esta guía se proporcionan recomendaciones de optimización para casos de uso comunes de JBoss EAP, así como instrucciones para monitorear el rendimiento y diagnosticar problemas de rendimiento.

3.23. INSTALADOR GRÁFICO

El instalador gráfico ofrece la opción de instalación personalizada de JSF

Puede instalar una implementación de JSF personalizada cuando utiliza el instalador gráfico para instalar JBoss EAP 7.1. En la página **Configure Runtime Environment** (Configurar el entorno de tiempo de ejecución) del asistente del instalador, seleccione **Perform advanced configuration** (Realizar configuración avanzada) → **Install JSF implementation** (Instalar implementación de JSF) y haga clic en **Next** (Siguiente). Proporcione la información requerida en la página **JSF Setup** (Configuración de JSF) y complete el resto de la instalación.

NOTA

El instalador de JBoss EAP 7.1 admite la instalación de MyFaces v2.1.x/v2.2.x y Mojarra v2.1.x/v2.2.x. No se admite la propia implementación de MyFaces.

3.24. INICIOS RÁPIDOS

Nuevo inicio rápido disponible: ha-singleton-deployment

El inicio rápido **`ha-singleton-deployment`** se envía con JBoss EAP 7.1. Este es un ejemplo práctico completo de un servicio empaquetado en una aplicación como un Singleton en todo el clúster mediante implementaciones de Singleton.

Nuevo inicio rápido disponible: messaging-clustering-singleton

El inicio rápido **`messaging-clustering-singleton`** se envía con JBoss EAP 7.1. Este inicio rápido demuestra el agrupamiento mediante ActiveMQ Artemis con la configuración de Singleton MDB.

Actualizaciones de inicios rápidos para la seguridad de Elytron

Los siguientes inicios rápidos son nuevos para JBoss EAP 7.1 y demuestran cómo se puede utilizar Elytron para proteger las aplicaciones.

- ejb-security-context-propagation
- ejb-security-jaas
- ejb-security-programmatic-auth
- helloworld-mutual-ssl
- helloworld-mutual-ssl-secured

- helloworld-ssl

Los siguientes inicios rápidos existentes se actualizaron para usar la seguridad de Elytron:

- ejb-asynchronous
- ejb-multi-server
- ejb-remote
- ejb-security
- helloworld-jms
- servlet-security
- shopping-cart

CAPÍTULO 4. MUESTRA DE TECNOLOGÍA

AVISO

Las siguientes configuraciones y funciones se proporcionan como muestras de tecnología únicamente. No se admite su uso en un entorno de producción y pueden estar sujetas a cambios significativos en el futuro. Consulte esta nota en el Portal del cliente de Red Hat en el ámbito de soporte para funciones de muestras de tecnología.

EJB y JNDI por HTTP/HTTPS con balanceador de carga HTTP

La realización de invocaciones de EJB y JNDI mediante el protocolo HTTP, para que las solicitudes se asignen directamente a las solicitudes de HTTP es una función de muestra de tecnología en JBoss EAP 7.1. Puede invocar EJB a través de un balanceador de HTTP. Esto se puede realizar mediante las API del cliente EJB/nomenclatura. Para obtener más información, consulte Invocación de EJB por HTTP en la sección *Desarrollo de aplicaciones EJB*.

Aplicaciones web empresariales modernas con JavaScript del lado del servidor en JVM

JBoss EAP 7.1 le permite escribir JavaScript del lado del servidor, mediante funcionalidades JDK 8 Nashorn, para desarrollar rápidamente los extremos de REST que pueden sacar CDI beans, realizar búsquedas JNDI e invocar JPA Entity Beans. El subsistema **`undertow`** ofrece esta funcionalidad como muestra de tecnología únicamente.

Eventos enviados por el servidor (SSE) en Java

Se proporciona una implementación del modelo de eventos enviados por el servidor en Java como muestra de tecnología para usuarios que trabajen con clientes móviles y eficaces. Esto incluye únicamente la implementación del servidor.

Configuración del subsistema administrador de seguridad mediante la consola de administración

En JBoss EAP 7.1, la capacidad de configurar el subsistema **`security-manager`** de la consola de administración se ofrece únicamente como muestra de tecnología.

Descargar el repositorio Maven mediante la aplicación Offliner

JBoss EAP 7.1 proporciona la capacidad de usar la aplicación Offliner para descargar el repositorio Maven como muestra de tecnología únicamente. Para obtener más información, consulte Descargar el repositorio JBoss EAP Maven mediante la aplicación Offliner en la *Guía de desarrollo*.

Funciones Elytron

Las siguientes funciones Elytron se proporcionan como muestra de tecnología únicamente:

- Uso de **`filesystem-realm`**, que es una definición de dominio de seguridad simple respaldada por el sistema de archivos.
- Uso de **`custom-realm`** modificable, que es un dominio de seguridad predeterminado que implementa **`org.wildfly.security.auth.server.ModifiableSecurityRealm`**.
- Operaciones de manipulación de identidad en un **`ldap-realm`** o **`jdbc-realm`**.

Operador de expresión regular de coincidencia de CLI administrativa

El operador de expresión regular de coincidencia (**~=**) para el flujo de control de CLI administrativa **`if-else`** se proporciona como muestra de tecnología únicamente. Para obtener más información, consulte Utilice si existe otro flujo de control en la *guía de CLI administrativa*.

CAPÍTULO 5. FUNCIONALIDAD SIN SOPORTE Y OBSOLETA

5.1. FUNCIONES NO COMPATIBLES

Se ha retirado el soporte para algunas tecnologías, debido al alto costo de mantenimiento, al bajo interés de la comunidad y a que existen mejores soluciones alternativas. Las siguientes funciones no son compatibles con JBoss EAP 7.1.

NOTA

Las funciones no compatibles enumeradas en la sección Funciones no compatibles de las *Notas de la versión 7.0.0* también se aplican a la versión 7.1 de JBoss EAP, a menos que estén mencionados en la sección Nuevas funciones y mejoras de este documento.

Mensajería (ActiveMQ Artemis)

Las siguientes funciones de mensajería no son compatibles con JBoss EAP 7.1:

- Protocolos AMQP, STOMP, REST, MQTT y OpenWire
- Opciones de transporte de Netty por HTTP y Netty Servlet para conectores/aceptadores
- Ya no se puede configurar el tipo de conectores/aceptadores OIO (Old Java IO)
- Vert.x, AeroGear, Spring e integración Jolokia
- Creación de cola dinámica
- Clúster en cadena
- Agrupación de mensajes en clúster
- Uso de ActiveMQ Artemis Management con JMX
- Apagado seguro/reducción de escalabilidad de nodos en un clúster Artemis
- Topología HA colocalizada configurada mediante replication-colocated/shared-store-colocated

NOTA

No obstante, la topología HA colocalizada está admitida, como se describe en la sección Servidores de seguridad colocalizados de *Configuración de mensajería*.

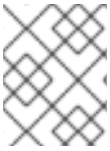
- Uso de mensajería con tipo de registro ASIGNADO
- Evitar el aislamiento de la red
- Configuración de múltiples conexiones de clústeres

Las API de Infinispan

Infinispan se entrega como módulo privado para brindar las funcionalidades de almacenamiento en caché de JBoss EAP. Infinispan no recibe soporte por el uso directo de las aplicaciones.

Jackson API

Las librerías Jackson 1 no reciben soporte para desarrollo o uso en producción en JBoss EAP.



NOTA

Las librerías Jackson 2 reciben soporte. Para obtener más información, consulte ¿JBoss EAP admite el uso de librerías Jackson? en el Portal de clientes de Red Hat.

OAuth con RESTEasy

OAuth no se admite con RESTEasy.

ElytronAuthenticator

No se admite el uso de la clase **`ElytronAuthenticator`** para propagar identidades de seguridad. Para obtener más información, consulte Uso de ElytronAuthenticator para propagar identidades en *Cómo configurar la administración de identidades*.

5.2. FUNCIONES DEPRECIADAS

Algunas funciones han sido depreciadas con el lanzamiento de JBoss EAP 7.1. Es decir, que no se le harán mejoras y pueden ser retiradas en el futuro, por lo general, en el siguiente lanzamiento.

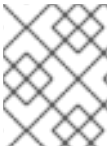
Red Hat seguirá proporcionando soporte completo y correcciones de errores según los términos y condiciones de soporte estándar. Para obtener más información sobre la política de soporte Red Hat, consulte el artículo Red Hat JBoss Middleware Product Update and Support Policy en el Portal del clientes de Red Hat.

Para obtener información sobre las funciones que han sido depreciadas, consulte JBoss Enterprise Application Platform Component Details en el Portal del cliente de Red Hat.

Imagen de contenedores JBoss EAP

La imagen de base de JBoss EAP para contenedores, **`registry.access.redhat.com/jboss-eap-7-tech-preview/eap70`**, distribuida a través del Registro de Red Hat Docker no se actualizará para JBoss EAP 7.1 y esta imagen se eliminará de la 7.1 de JBoss EAP.

Atributos



NOTA

En la mayoría de los casos, los atributos depreciados no se muestran en la consola de administración.

- Se deprecian los siguientes atributos para los agentes de escucha HTTP en el subsistema **`undertow`**:
  - enable-spdy
  - activado
  - enabled-cipher-suites
  - enabled-protocols
  - security-realm
  - ssl-session-cache-size
  - ssl-session-timeout

    - verify-client

- Se deprecian los siguientes atributos para cachés en el subsistema **`infinispan`**:
    - queue-flush-interval
    - queue-size
- Se deprecian los siguientes atributos en el subsistema **`iiop-openjdk`**:
    - add-component-via-interceptor
    - queue-flush-interval
- Se deprecian los siguientes atributos del recurso **`remote-outbound-connection`** en el subsistema **`remoting`**:
    - protocolo
    - security-realm
    - username

Recursos

- Se deprecian los siguientes recursos de administración básicos debido a que la seguridad de administración ahora la provee Elytron.
    - audit
    - ldap-connection
    - security-realm
- Se deprecian las siguientes conexiones salientes remotas en el subsistema **`remoting`**:
    - local-outbound-connection
    - outbound-connection
- Se deprecian los siguientes tipos de almacén persistentes en el subsistema **`infinispan`**:
    - binary-jdbc
    - mixed-jdbc

Operaciones

- Se deprecia la siguiente operación de administración para el subsistema **`jaxrs`**:
    - show-resources

CAPÍTULO 6. PROBLEMAS RESUELTOS

Consulte Problemas resueltos para JBoss EAP 7.1.0 para ver la lista de problemas que se originan de casos de clientes resueltos para esta versión.

CAPÍTULO 7. CVE FIJOS

JBoss EAP 7.1 incluye correcciones para los siguientes problemas relacionados con la seguridad:

- CVE-2016-6311: La dirección IP interna se divulga en la redirección cuando no se establece el campo de Host del encabezado del pedido
- CVE-2016-2141: Adición de verificaciones de autorización en forma predeterminada al recibir mensajes de JGroups
- CVE-2016-5406: Los transformadores descartan las configuraciones de RBAC para esclavos de legado que ejecutan las versiones 1.8 y anteriores de la API de administración
- CVE-2016-4993: Inyección de encabezado HTTP/división de respuestas
- CVE-2015-0254: XXE y RCE vía extensión de XSL en las etiquetas JSTL XML
- CVE-2016-7046: Solicitud de proxy de URL extensa deriva en java.nio.BufferOverflowException y DoS
- CVE-2016-8627: Posible ataque DOS de escasez de recursos EAP vía solicitudes GET para archivos de registro de servidores
- CVE-2016-7061: Los datos sensibles se pueden exponer a nivel del servidor en el modo de dominio
- CVE-2016-8656: Chown no seguro de server.log en el script jboss init permite escalamiento de privilegios
- CVE-2016-9589: ParseState headerValuesCache se puede explotar para llenar el heap con residuos
- CVE-2017-2595: Archivo arbitrario leído vía traspaso de rutas
- CVE-2016-9606: Resteasy: Desclasificación de Yaml vulnerable a RCE
- CVE-2017-2666: Vulnerabilidad de contrabando de solicitudes HTTP por permitir caracteres no válidos en solicitudes HTTP
- CVE-2017-2670: Un cierre inadecuado de Websocket puede hacer que el hilo de IO quede atrapado en un bucle
- CVE-2016-4978: JMSObjectMessage deserializa los posibles objetos maliciosos, lo que permite la Ejecución del código remoto
- CVE-2017-7525: jackson-databind: Vulnerabilidad de deserialización vía el método readValue de ObjectMapper
- CVE-2017-2582: El analizador de solicitudes SAML reemplaza cadenas especiales con propiedades del sistema
- CVE-2014-9970: jasypt: Vulnerable a un ataque sincronizado en relación con la comparación del hash de contraseña
- CVE-2015-6644: bouncycastle: Divulgación de información en GCMBlockCipher
- CVE-2017-5645: log4j: Vulnerabilidad de deserialización del receptor de socket

- CVE-2017-7536: hibernate-validator: Escalamiento de privilegios al ejecutarse en el administrador de seguridad
- CVE-2017-12165: Un análisis de espacios en blanco inadecuado puede generar un posible contrabando de solicitudes HTTP
- CVE-2017-7559: Posible contrabando de solicitudes http cuando Undertow analiza los encabezados http con espacios en blanco inusuales
- CVE-2016-7066: Permiso ejecutable en todo el mundo en bin/jboss-cli después de la instalación. Cualquier usuario del sistema puede provocar daños o apagar la instancia de JBoss EAP en ejecución
- CVE-2017-12167: Privilegios equivocados en múltiples archivos de propiedades

CAPÍTULO 8. PROBLEMAS CONOCIDOS

Consulte Problemas conocidos para JBoss EAP 7.1.0 para ver la lista de problemas conocidos para esta versión.

Asimismo, tenga en cuenta lo siguiente:

- El paquete **`jboss-jaxrpc-api_1.1_spec`** indica una licencia incorrecta en el archivo **`licenses.xml`** de JBoss EAP. La información de licencia correcta es CDDL o GPLv2 con la excepción de Classpath.
- Existen algunas discrepancias en las licencias del artefacto entre el RPM y la instalación del ZIP. La información de licencias de la instalación ZIP es válida, excepto en el caso de la información de licencia del paquete **`jboss-jaxrpc-api_1.1_spec`**, mencionada en el apartado anterior.
- Existe un problema al intentar usar un almacén de credenciales de tipo PKCS12 con el JDK de IBM o el JDK de HP. La solución temporal es usar un almacén de credenciales JCEKS. Para obtener más información, consulte JBEAP-13586.
- Los siguientes JIRA son causados por errores de JDK y solucionarlos está fuera del alcance de JBoss EAP:
  - JBEAP-8207: Situación requerida para la continuación de Elytron, IBM java y SPNEGO
  - JBEAP-10483: HTTP2 vía JSSE y el motor wildfly ALPN hack ssl están averiados en Solaris 11
    JBoss EAP resuelve temporalmente este problema deshabilitando el proveedor de OracleUcrypto en la configuración predeterminada de JBoss EAP. No obstante, esto puede generar problemas en la plataforma Solaris 10 con HTTP por TLS. Si encuentra problemas, habilite el proveedor OracleUcrypto o actualice su máquina Solaris 10 con el parche 150401-52 o uno posterior.

Revised on 2018-01-11 04:54:10 EST