Red Hat JBoss Enterprise Application Platform 7.2.Beta

7.2 Beta Release Notes

For Use with Red Hat JBoss Enterprise Application Platform 7.2.Beta

Last Updated: 2018-08-06

Red Hat JBoss Enterprise Application Platform 7.2.Beta 7.2 Beta Release Notes

For Use with Red Hat JBoss Enterprise Application Platform 7.2.Beta

Legal Notice

Abstract

These release notes contain important information related to Red Hat JBoss Enterprise Application Platform 7.2.Beta.

Table of Contents

CHAPTER 1. ABOUT RED HAT JBOSS ENTERPRISE APPLICATION PLATFORM 7.2 BETA

Red Hat JBoss Enterprise Application Platform 7.2 Beta (JBoss EAP) is a middleware platform built on open standards and compliant with the Java Enterprise Edition 7 specification.

JBoss EAP includes a modular structure that allows service enabling only when required, improving startup speed.

The management console and management command-line interface (CLI) make editing XML configuration files unnecessary and add the ability to script and automate tasks.

JBoss EAP provides two operating modes for JBoss EAP instances: standalone server or managed domain. The standalone server operating mode represents running JBoss EAP as a single server instance. The managed domain operating mode allows for the management of multiple JBoss EAP instances from a single control point.

In addition, JBoss EAP includes APIs and development frameworks for quickly developing secure and scalable Java EE applications.

CHAPTER 2. SUPPORT STATEMENT AND RESOURCES

The JBoss EAP 7.2 Beta release is provided as a service to customers who want to try the latest major release features and work with support when problems are encountered. Support for Beta releases is limited to commercially reasonable effort and non-production use cases, and all support cases should be opened with a severity of 4. Patches will not be provided, but bug fixes may be incorporated in future releases. To contact support, please visit the support case creation page Open a Support Case .

CHAPTER 3. NEW FEATURES AND ENHANCEMENTS

3.1. JAVA EE 8

Java EE 8 Preview Mode

By default, this JBoss EAP 7.2 Beta release uses Java EE 7 APIs.

You can preview Java EE 8 functionality by setting the **`ee8.preview.mode`** system property to **`true`** when starting the JBoss EAP server. For example:

```
$ EAP_HOME/bin/standalone.sh -Dee8.preview.mode=true
```

This enables support for the following Java EE 8 standards:

- JSR 250: Common Annotations 1.3
- JSR 338: JPA 2.2
- JSR 365: CDI 2.0
- JSR 367: JSON-B 1.0
- JSR 369: Servlet 4.0
- JSR 370: JAX-RS 2.1
- JSR 372: JSF 2.3
- JSR 374: JSON-P 1.1
- JSR 380: Bean Validation 2.0
- JSR 919: JavaMail 1.6

Java EE 8 Security Support

Java EE 8 includes support for JSR 375, which defines portable, plug-in interfaces for authentication and identity stores, and a new **`injectable-type SecurityContext`** interface that provides an access point for programmatic security. You can use the built-in implementations of these APIs, or define custom implementations.

JBoss EAP 7.2 Beta now supports JSR 375.

3.2. SECURITY

Enable SASL Authentication for the Management Interfaces Using the CLI Security Commands

SASL authentication can now be enabled for the management interfaces using the **`security enable-sasl-management`** CLI command. This command creates all of the non-existing resources necessary to configure authentication.

For more information, see Enable SASL Authentication for the Management Interfaces Using the CLI Security Command in *How to Configure Server Security.*

Enable HTTP Authentication Using the CLI Security Commands

HTTP authentication can now be enabled for the Undertow security domain and the management

interfaces using the **security** CLI commands.

- For the Undertow security domain, use the **security enable-http-auth-http-server** CLI command.
- For the management interfaces, use the **security enable-http-auth-management** CLI command.

For more information, see Enable HTTP Authentication for Applications Using the CLI Security Command and Enable HTTP Authentication for the Management Interfaces Using the CLI Security Command in *How to Configure Server Security*.

3.3. MANAGEMENT CLI

Enhanced Help

The management CLI **help** functionality has been updated to provide easier access to help information. The **help** command now features tab completion and can also show help information for management CLI operations and command actions.

See the *Management CLI Guide* for more information on using the management CLI **help** command.

Indicator for Required Attributes

When using tab completion in the management CLI, attributes that are required for the current operation are marked with a * character.

```
/subsystem=naming/binding=test:add( [TAB]
!              class          module
binding-type*  environment    type
cache          lookup         value
```

In the above example, pressing Tab after entering **/subsystem=naming/binding=test:add(** lists the available attributes and indicates that **binding-type** is a required attribute for this operation.

Viewing Multi-page Output

When you run the management CLI in interactive mode and the operation results in multiple pages of output, the command processor pauses the screen at the end of the first page. This allows you to page through the output one line or page at a time. The occurrence of multiple pages of output is indicated by a line of text displaying **--More(*NNN*%)--** at the end of the output.

See the *Management CLI Guide* for the options available if you encounter multiple page output when running a management CLI command.

Using for-done Control Flow

You can use **for-done** control flow in the management CLI to iterate over a collection returned from an operation and execute commands on each item in the collection.

For more information, see Use for-done Control Flow in the *Management CLI Guide*.

Output Operation Responses in JSON Format

You can configure the management CLI to output operation responses in pure JSON format by setting the **output-json** element to **true** in the ***EAP_HOME*/bin/jboss-cli.xml** file or by passing the **--output-json** flag in when starting the management CLI. By default, operation responses are displayed in DMR format.

Redirecting Output

Instead of printing output from a management CLI operation to the terminal, you can redirect the output using the following operators:

- **>**: Write output to a file on the file system.
- **>>**: Append output to a file on the file system.
- **|**: Redirect output to the **`grep`** command for searching the output.

For more information, see Redirect Output in the *Management CLI Guide*.

Unified Deployment Command

The management CLI **`deployment`** command allows you to manage your deployments using a unified interface to deploy, undeploy, enable, disable or list information about the deployments.

For more information, see Deploy an Application to a Standalone Server Using the Management CLI and Deploy an Application in a Managed Domain Using the Management CLI in the *Configuration Guide*.

Printing CLI Output in Color

You can now configure the management CLI to print the CLI log output in color based on the log message output type. For more information about the available colors and how to enable and disable color printing, see Configuring the Management CLI in the *Management CLI Guide*.

3.4. MANAGEMENT CONSOLE

Topology View

In a managed domain, you can now see an overview of the hosts, server groups, and servers in the domain, and the status of each server. This is available from the **Runtime** tab by selecting **Topology**.

Breadcrumb Bar

When viewing resources, a breadcrumb bar is available at the top that allows you to easily switch between resources. From the breadcrumb bar, you can also open the resource in a separate window or switch to expert mode to browse the management model.

Navigation Enhancements

This release introduces a new interface for navigating JBoss EAP resources. You can use the arrow keys to navigate through the resource finder, pin frequently used items to stay at the top of the list, filter to quickly find items, and view the main attributes of a resource from its preview.

Deployment Enhancements

This release adds more support for deploying and managing your applications through the management console. You can drag and drop to add or replace deployments, browse deployment content to preview text and images, download deployments, and create exploded deployments.

Enable SSL Wizard for the Management Console

A wizard is now available to help you enable SSL for the HTTP management interface, which is used by the management console. Using the wizard, you can optionally create a truststore for mutual authentication as well as choose from the following keystore scenarios:

- You want to create a certificate store and generate a self-signed certificate.
- You already have the certificate store on the file system, but no keystore configuration.
- You already have a keystore configuration that uses a valid certificate store.

To access the wizard for a standalone server, select the **Runtime** tab, click **View** on the appropriate server, select **HTTP Management Interface** and click the **Enable SSL** button.

To access the wizard for a managed domain, select the **Runtime** tab, click **Hosts** and select the appropriate host, select **View** → **Management Interface** → **HTTP** and click the **Enable SSL** button.

Enable SSL Wizard for Undertow HTTPS Listeners

A wizard is now available to help you enable SSL for Undertow HTTPS listeners. Using the wizard, you can optionally create a truststore for mutual authentication as well as choose from the following keystore scenarios:

- You want to create a certificate store and generate a self-signed certificate *(not available in a managed domain)*.
- You already have the certificate store on the file system, but no keystore configuration.
- You already have a keystore configuration that uses a valid certificate store.

To access the wizard for a standalone server, click the **Configuration** tab, select **Subsystems** → **Web (Undertow)** → **Server**, click **View** on the appropriate server, select **Listener** → **HTTPS Listener**, select the appropriate HTTPS listener and click the **Enable SSL** button.

To access the wizard for a managed domain server, click the **Configuration** tab, click **Profiles** and select the appropriate profile, select **Web (Undertow)** → **Server**, click **View** on the appropriate server, select **Listener** → **HTTPS Listener**, select the appropriate HTTPS listener and click the **Enable SSL** button.

Configuring Logging Profiles

You can now use the management console to configure logging profiles in the `logging` subsystem.

Configuring the Security Manager Subsystem

It is now supported to configure the `security-manager` subsystem from the management console.

Additional Subsystem Configuration

The following subsystems have been enhanced to include additional configuration options, available from the **Configuration** tab:

- EJB
- Infinispan
- JGroups
- JMX
- Messaging (ActiveMQ)
- Resource Adapters
- Security (Legacy)
- Web (Undertow)

Additional Subsystem Monitoring Support

This release provides new and enhanced monitoring support for the following subsystems, available from the **Runtime** tab:

- Batch (JBeret)
- Datasources
- JNDI
- EJB
- IO
- JAX-RS
- Messaging (ActiveMQ)
- Transaction
- Web (Undertow)
- Webservices

3.5. WEB SERVER

Forwarded HTTP Extension
This JBoss EAP 7.2 Beta release introduces the **`Forwarded`** handler, which implements RFC 7239, allowing servers behind a reverse proxy to receive peer and local addresses within the header.

Typically, this handler should not be used in conjunction with any of the **`X-Forwarded-*`** headers enabled on the reverse proxy. This means that you should either use this handler or enable the **`proxy-address-forwarding`** attribute in Undertow listeners.

Session Manager Operations
The following operations to get detailed session information are now available from the management CLI at **`/deployment=`*`DEPLOYMENT_NAME`*`/subsystem=undertow`**.

- **`get-session-attribute`**: Return a specific attribute for a session.
- **`get-session-creation-time`**: Get the session creation time in ISO-8601 format.
- **`get-session-creation-time-millis`**: Get the session creation time in millseconds since the UNIX Epoch.
- **`get-session-last-accessed-time`**: Get the session last accessed time in ISO-8601 format.
- **`get-session-last-accessed-time-millis`**: Get the session last accessed time in milliseconds since the UNIX Epoch.
- **`list-session-attribute-names`**: List the session attribute names.
- **`list-session-attributes`**: List all attributes in a session.
- **`list-sessions`**: List all active sessions.

Undertow Byte Buffer Pools

You can now use Undertow byte buffer pools to allocate pooled NIO **`ByteBuffer`** instances. All listeners have a byte buffer pool and you can use different buffer pools and workers for each listener. Byte buffer pools can be shared between different server instances.

For more information, see Configuring Byte Buffer Pools in the *Configuration Guide*.

Setting the Default Cookie Version

Undertow now provides a way to set the default cookie version to use for cookies created by the application. For information about the new **`default-cookie-version`** attribute, see **`servlet-container`** Attributes in the *Configuration Guide*.

Allowing Unescaped Characters in a URL

You can now configure Undertow to allow non-escaped characters in a URL by setting the **`allow-unescaped-characters-in-url`** attribute for the HTTP, HTTPS, and AJP listeners. When this attribute is set to **`true`**, the listener processes any URL containing non-escaped, non-ASCII characters. When set to **`false`**, the listener rejects any URL containing non-escaped, non-ASCII characters with an **`HTTP Bad Request 400`** response code.

For more information about listener attributes, see Undertow Server Attributes in the *Configuration Guide*.

PROXY Protocol

Undertow now supports the PROXY protocol Version 1, as defined by The PROXY protocol Versions 1 & 2 specification. This option is disabled by default and must only be enabled for listeners that are behind a load balancer that supports the same protocol. It is configured using the new **`proxy-protocol`** attribute on the Undertow HTTP and HTTPS listeners.

For more information about listener attributes, see Undertow Server Attributes in the *Configuration Guide*.

3.6. EJB

EJB and JNDI over HTTP/HTTPS with HTTP Load Balancer

Performing EJB and JNDI invocations using the HTTP protocol, so that requests are mapped directly to HTTP requests, is now fully supported in JBoss EAP 7.2 Beta. In addition, you can invoke EJBs over an HTTP load balancer. For more information, see EJB Invocation Over HTTP in the *Developing EJB Applications*.

3.7. JSF

Disallowing DOCTYPE Declarations in JSF Deployments

You can use the management CLI to disallow **`DOCTYPE`** declarations in JSF deployments.

For more information, see Disallowing DOCTYPE Declarations in the *Configuration Guide*.

3.8. DATASOURCES

New Datasource Attribute

The **`datasource-class-info`** attribute provides the list of datasource connection properties that can be set for the datasource class.

For more information, see the Datasource Attributes table in the *Configuration Guide*.

3.9. INFINISPAN

Scattered Cache Mode

The **infinispan** subsystem now supports scattered cache mode. Scattered mode is similar to distributed mode in that it uses a consistent hash algorithm to determine ownership. However, ownership is limited to two members, and the originator, or node receiving the request for a given session, always assumes ownership for coordinating locking and cache entry updates. The cache write algorithm used in scattered mode guarantees that a write operation results in only a single RPC call. This can potentially reduce contention and improve performance following a cluster topology change.

For more information, see Clustering Modes in the *Configuration Guide*.

Externalize HTTP Sessions Using the Remote Cache Store

A new method of externalizing HTTP sessions to JBoss Data Grid is included in this release. This method utilizes a remote cache container in the **infinispan** subsystem of JBoss EAP that has a client SSL context defined for security.

You can configure remote cache containers from the management CLI and the management console.

For more information, see Externalize HTTP Sessions to JBoss Data Grid in the *Configuration Guide*.

3.10. IO

New Worker Attribute

In previous releases of JBoss EAP, the core threads size was always equal to the max threads size. This meant that threads would never die, even if the **task-keepalive** attribute was set. In this release, the number of threads for the core thread pool can be configured separately using the **task-core-threads** attribute, allowing the keepalive setting to work as expected.

For more information, see Configuring a Worker and IO Subsystem Attributes in the *Configuration Guide* for JBoss EAP.

3.11. LOGGING

JSON and XML Formatter

You can use the JSON and XML log formatters to format log messages in JSON and XML.

For more information, see Log Formatters in the *Configuration Guide*.

3.12. MESSAGING

Connect to Red Hat AMQ Using the Integrated Artemis Resource Adapter

You can configure the integrated Artemis resource adapter to connect to a remote installation of Red Hat AMQ 7, which then becomes the JMS provider for your JBoss EAP 7.2 Beta applications. This allows JBoss EAP to be a client for the remote Red Hat AMQ 7 server.

For more information, see Configuring the Artemis Resource Adapter to Connect to Red Hat JBoss AMQ 7 in *Configuring Messaging* for JBoss EAP.

3.13. MODULES

Predefined Modules

A set of predefined modules, **org.jboss.modules**, which includes all of the JBoss Modules API, is

supported in JBoss EAP 7.2 Beta when you use the default module loader. This special module is always available and is provided by JBoss Modules. The standard Java Platform Module System (JPMS) modules, which are provided in Java 9 and later, are also available by their standard names. When using JDK 8, the JDK 9 modules are emulated by JBoss Modules.

For more information, see Predefined Modules in the *Configuration Guide*.

3.14. OPENSHIFT

KUBE_PING Integrated Natively In JBoss EAP

Previously, the **KUBE_PING** JGroups discovery protocol was implemented only in the JBoss EAP OpenShift image. **KUBE_PING** is now implemented natively in JBoss EAP, so users creating their own custom container images are now able to natively use **KUBE_PING** for clustered applications. For more information on using **KUBE_PING**, see the Clustering reference in *Getting Started with JBoss EAP for OpenShift Container Platform*.

3.15. RESTEASY

JAX-RS Client Support for HTTP Redirects

JAX-RS **ClientHttpEngine** implementations based on the Apache **HttpClient** support HTTP redirection. For more information, see HTTP Redirect in *Developing Web Services Applications*.

CHAPTER 4. UNSUPPORTED AND DEPRECATED FUNCTIONALITY

4.1. UNSUPPORTED FEATURES

Support for some technologies are removed due to the high maintenance cost, low community interest, and better alternative solutions. The following features are not supported in the JBoss EAP 7.2 Beta release.

NOTE

The unsupported features listed in the Unsupported Features section of the *7.1.0 Release Notes* also apply to the JBoss EAP 7.2 Beta release, unless they are mentioned in the New Features and Enhancements section of this document.

RPM Installation

RPM installation is not available for JBoss EAP the 7.2 Beta release. It will be available for the 7.2 GA release.

4.2. DEPRECATED FEATURES

Some features have been deprecated with this release. This means that no enhancements will be made to these features, and they may be removed in the future, usually the next major release.

Red Hat will continue providing full support and bug fixes under our standard support terms and conditions. For more information about the Red Hat support policy, see the Red Hat JBoss Middleware Product Update and Support Policy located on the Red Hat Customer Portal.

For details of which features have been deprecated, see the JBoss Enterprise Application Platform Component Details located on the Red Hat Customer Portal.

IO Subsystem

- IO buffer pools are deprecated in this release. They are replaced by Undertow byte buffer pools.

Platforms and Features

Support for the following platforms and features is deprecated:

Cloud

- Amazon EC2
- Microsoft Azure

Databases

- IBM DB2 e9.7
- MySQL 5.5
- Microsoft SQL Server 2012
- PostgreSQL 9.3

- Enterprise DB Postgres Plus Advanced Server 9.3
- Sybase 15

JDK

- HP-UX

JMS Providers/Adapters

- IBM WebSphere MQ 7.5
- TIBCO EMS

LDAP Servers

- Red Hat Directory Server 9.1
- Microsoft Active Directory 2008

Operating Systems and Related Web Servers

- Windows Server 2008 and associated Microsoft IIS web server
- Oracle Solaris 10 and Oracle Solaris 11 and associated web servers
- HP-UX
- Red Hat Enterprise Linux 6 32-bit

Tested Frameworks

- JQuery (all versions)
- AngularJS (all versions)

CHAPTER 5. RESOLVED ISSUES

See Resolved Issues for JBoss EAP 7.2 Beta to view the list of issues originating from customer cases that have been resolved for this release.

CHAPTER 6. FIXED CVES

JBoss EAP 7.2 Beta includes fixes for the following security related issues:

- CVE-2017-12174: **`artemis/hornetq`**: Memory exhaustion via UDP and JGroups discovery
- CVE-2017-12629: **`Solr`**: Code execution via entity expansion
- CVE-2017-15089: **`infinispan`**: Unsafe deserialization of malicious object injected into data cache
- CVE-2017-12196: **`undertow`**: Client can use bogus uri in Digest authentication
- CVE-2018-8088: **`slf4j`**: Deserialisation vulnerability in EventData constructor can allow for arbitrary code execution
- CVE-2018-1047: **`undertow`**: Path traversal in ServletResourceManager class
- CVE-2018-10237: **`guava`**: Unbounded memory allocation in **`AtomicDoubleArray`** and **`CompoundOrdering`** classes allow remote attackers to cause a denial of service
- CVE-2018-1067: **`undertow`**: HTTP header injection using CRLF with UTF-8 encoding
- CVE-2018-10862: **`wildfly-core`**: Path traversal can allow the extraction of **`.war`** archives to write arbitrary files
- CVE-2018-8039: **`cxf-core`**, **`apache-cxf`**: TLS hostname verification does not work correctly with **`com.sun.net.ssl.*`**

CHAPTER 7. KNOWN ISSUES

See Known Issues for JBoss EAP 7.2 Beta to view the list of known issues for this release.

Revised on 2018-08-06 10:27:26 EDT