



Red Hat JBoss Enterprise Application Platform 7.3.beta

JBoss EAP 7.3.Beta Release Notes

For Use with Red Hat JBoss Enterprise Application Platform 7.3.beta

Red Hat JBoss Enterprise Application Platform 7.3.beta JBoss EAP 7.3.Beta Release Notes

For Use with Red Hat JBoss Enterprise Application Platform 7.3.beta

Legal Notice

Copyright © 2019 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

These release notes contain important information related to Red Hat JBoss Enterprise Application Platform 7.3.beta.

Table of Contents

CHAPTER 1. NEW FEATURES AND ENHANCEMENTS	4
1.1. SECURITY	4
Elytron Audit Logging Performance and Reliability Tuning	4
JwtValidator Enhancements	4
Default SSLContext	4
Java Authentication SPI for Containers (JASPI) Security Using Elytron	4
Server SSL Server Name Indication (SNI) Contexts	4
Automatic Detection of Keystore Types	4
Java EE Security API Support in Elytron	5
Silent BASIC Authentication in Elytron	5
Utility to Migrate Properties-based Security Realm to Filesystem Realm in Elytron	5
Support for Hexadecimal Encoding in JDBC Realm	5
Support for Modular Crypt Passwords in JDBC Realm	5
1.2. SERVER MANAGEMENT	6
Support for Eclipse MicroProfile Metrics	6
Suspend Servers Managed by a Host Controller	6
Support for JBoss EAP Subsystem Metrics in Prometheus Format	6
1.3. MANAGEMENT CLI	6
Disable Output Paging	6
1.4. MANAGEMENT CONSOLE	6
Configure Socket Log Handlers from Management Console	6
View Logging Profile Logs from Management Console	6
View Active Management Operations from Management Console	6
Two New Resources Available for the Modcluster Subsystem	6
Configure SSL SNI Contexts from Management Console	7
View Non Progressing Operations	7
Configure Modcluster Proxies	7
Reinitialize a Trust Manager from Management Console	7
Configure JASPI Authentication from Management Console	7
Configure Remote ActiveMQ Server Resources from the Management Console	7
View Socket Binding Name and Open Ports for a Server from Management Console	8
Runtime Operations Supported on Management Console	8
Configure a Let's Encrypt Account	8
Keystore Certificate Authority Configuration Using the Management Console	8
Configure MicroProfile Metrics Using the Management Console	9
Obtain Certificate from Let's Encrypt CA in SSL Wizard	9
Ability to Customize Management Console Title	9
1.5. WEB SERVER	9
Console access logging	9
1.6. LOGGING	10
Ability to Format Syslog Messages	10
1.7. DEPLOYMENTS	10
Display Modules According to Deployment	10
1.8. EJB	10
Multiple Delivery Groups Support for Message-Driven Beans	10
1.9. CLUSTERING	10
New Attribute initial-load in the mod_cluster Subsystem	10
Ability to Determine the Primary Singleton Provider	10
Ability to Specify Distributable Session Manager Invocation	10
Ability to Notify Singleton Service Providers of the New Primary Provider	11
The distributable-web subsystem for Distributable Web Session Configurations	11

Ability to Store Session Data in a Remote Red Hat Data Grid Cluster	11
1.10. MESSAGING	11
Configure JMS Resources for a Remote Artemis-based Broker Using the resourceAdapter Element	11
Configure Global Resources Usage for Messaging Servers	11
Configure the Timeout Value for Opening a Message Journal File	11
Change in Artemis Logging Codes	11
Omit Prefix on Destination Names	12
Messaging Enhancements for Load Balancers	12
1.11. OPENSIFT	12
JBoss EAP 7.3 Beta JDK 8 OpenShift Image Available	12
JBoss EAP 7.3 Beta JDK 11 OpenShift Image Available	12
CHAPTER 2. TECHNOLOGY PREVIEW	13
Examine the Health Check Using the Management Console	13
CHAPTER 3. UNSUPPORTED AND DEPRECATED FUNCTIONALITY	14
3.1. UNSUPPORTED FEATURES	14
Internal Datasources and Drivers for OpenShift JDK 11 image	14
3.2. DEPRECATED FEATURES	14
3.2.1. Platforms and Features	14
Operating Systems and Related Web Servers	14
Databases and Database Connectors	14
CHAPTER 4. RESOLVED ISSUES	15
CHAPTER 5. FIXED CVES	16
CHAPTER 6. KNOWN ISSUES	17

CHAPTER 1. NEW FEATURES AND ENHANCEMENTS

1.1. SECURITY

Elytron Audit Logging Performance and Reliability Tuning

In JBoss EAP 7.2, the **synchronized** attribute for Elytron file audit logging defined whether to flush the output stream and synchronize the file descriptor after every audit event.

This release introduces a new **autoflush** attribute to separate stream flushing and file synchronizing, which allows for finer tuning of performance and reliability for Elytron audit logging.

For more information on configuring Elytron audit logging, see [Elytron Audit Logging](#) in *How to Configure Server Security* for JBoss EAP.

JwtValidator Enhancements

The JwtValidator in this release now includes support for multiple keys and for remote public keys. The **key-store** attribute can now be combined with the **certificate** attribute to be used as an alternate to the **public-key**. The **client-ssl-context** attribute defines the SSL context to use for a remote [JSON Web Key \(JWK\)](#). This enables you to use the URL from the **jku** (JSON Key URL) header parameter to fetch public keys for token verification.

For more information, see the [token-realm jwt Attributes](#) table in *How to Configure Server Security* for JBoss EAP.

Default SSLContext

This release now registers a default SSLContext on startup that is available for use by any libraries that support use of the default context.

For more information, see [Default SSLContext](#) in *How to Configure Server Security* for JBoss EAP.

Java Authentication SPI for Containers (JASPI) Security Using Elytron

The **elytron** subsystem in this release now provides an implementation of the **Servlet** profile from the Java Authentication SPI for Containers (JASPI). This allows tighter integration with the security features provided by Elytron.

For more information, see [Configure Java Authentication SPI for Containers \(JASPI\) Security Using Elytron](#) in the *Development Guide* for JBoss EAP.

Server SSL Server Name Indication (SNI) Contexts

The **server-ssl-sni-context** in this release is used for providing server-side SNI matching. It provides matching rules to correlate host names to SSL contexts, along with a default in case none of the provided host names are matched.

For more information, see [Using a server-ssl-sni-context](#) in the *How to Configure Server Security* for JBoss EAP.

Automatic Detection of Keystore Types

The following keystore types are now detected automatically:

- **JKS**
- **JCEKS**
- **PKCS12**
- **BKS**

- **BCFKS**
- **UBER**

The other keystore types must be specified manually.

For more information, see [Elytron Subsystem Components Reference](#) in the *How to Configure Server Security* for JBoss EAP.

Java EE Security API Support in Elytron

The **elytron** subsystem now supports the Java EE Security API as defined in JSR 375.

The Java EE Security API 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. For details about the specifications, see [Java EE Security API Specification](#).

You can enable the Java EE Security API in the **elytron** subsystem with minimal configuration steps using the management CLI.

For information on enabling Java EE Security API, see [About Java EE Security API](#) in the Development Guide.

Silent BASIC Authentication in Elytron

You can now configure the **elytron** subsystem to perform a silent **BASIC** authentication.

When the silent authentication is enabled, a user is not prompted to log in for accessing a web application if the user's request does not contain an authorization header.

For information about enabling the silent **BASIC** authentication, see [Configure Web Applications to Use Elytron or Legacy Security for Authentication](#) in *How to Configure Identity Management*.

Utility to Migrate Properties-based Security Realm to Filesystem Realm in Elytron

You can now migrate the legacy properties-based security realm to Elytron's filesystem-based realm using the **filesystem-realm** command of the **elytron-tool.sh** tool.

A filesystem-based realm is a filesystem-based identity store used by Elytron for storing user identities. The **filesystem-realm** command migrates the **properties-realm** files to **filesystem-realm** and also generates commands for adding this realm and a security domain to the **elytron** subsystem.

For information about the **filesystem-realm** command, see [Migrate to Filesystem-based Security Realm Using the filesystem-realm Command](#) in the *Migration Guide* for JBoss EAP.

Support for Hexadecimal Encoding in JDBC Realm

Elytron now supports hexadecimal encoding for password hashing algorithms in the JDBC realm.

For more information, see [Password Mappers](#) in *How to Configure Identity Management* guide for JBoss EAP.

Support for Modular Crypt Passwords in JDBC Realm

Modular Crypt password encoding is now supported in the JDBC realm.

The Modular Crypt encoding allows for multiple pieces of information such as the password type, the hash or digest, the salt, and the iteration count to be encoded in a single string.

For more information, see [Password Mappers](#) in *How to Configure Identity Management* guide for JBoss EAP.

1.2. SERVER MANAGEMENT

Support for Eclipse MicroProfile Metrics

This release now includes the [SmallRye Metrics](#) component, which provides [Eclipse MicroProfile Metrics](#) functionality using the **microprofile-metrics-smallrye** subsystem. This subsystem is used to provide monitoring data for the JBoss EAP instance, and is enabled by default.

For more information, see [Eclipse MicroProfile Metrics](#) in the *Configuration Guide* for JBoss EAP.

Suspend Servers Managed by a Host Controller

This release provides the ability to suspend and resume servers at the host level in a managed domain.

For more information, see [Suspend Servers](#) in the *Configuration Guide* for JBoss EAP.

Support for JBoss EAP Subsystem Metrics in Prometheus Format

The Eclipse MicroProfile Metrics functionality is used to provide monitoring data for the JBoss EAP instance. This release enhances the SmallRye Metrics component to provide the JBoss EAP metrics in the Prometheus format.

For information about Eclipse MicroProfile Metrics, see the [Eclipse MicroProfile Metrics](#) section in the *Configuration Guide* for JBoss EAP.

1.3. MANAGEMENT CLI

Disable Output Paging

By default, the JBoss EAP management CLI pauses after a page of output has been displayed, which allows you to browse and search the command output. You can now disable this behavior and print the entire output immediately by starting the management CLI with the **--no-output-paging** argument or by setting the **output-paging** element to **true** in the **EAP_HOME/bin/jboss-cli.xml** file.

1.4. MANAGEMENT CONSOLE

Configure Socket Log Handlers from Management Console

You can now configure socket log handlers using the management console by navigating to **Configuration** → **Subsystems** → **Logging** → **Configuration**, clicking **View**, and selecting **Handler** → **Socket Handler**.

For more information, see [Configure a Socket Log Handler](#) in the *Configuration Guide* for JBoss EAP.

View Logging Profile Logs from Management Console

You can now view the logging profile log files from the management console by navigating to **Runtime** → **Monitor** → **Log Files** → **Log File** and clicking **View** next to the logging profile for which you want to view the logs.

View Active Management Operations from Management Console

You can now view the active operations of all hosts and servers in a central location within the management console.

When running a standalone server, navigate to **Runtime** → **Server** → **Monitor** → **Management Operations** and click **View**.

In a managed domain, navigate to the **Runtime** → **Browse By** → **Management Operations** and click **View**.

Two New Resources Available for the Modcluster Subsystem

Now the **Modcluster** subsystem has two new resources: **load-provider=dynamic** and **load-provider=simple**. The **dynamic-load-provider=configuration** resource is an alias to **load-provider=dynamic**.

You can now view the mutually-exclusive resources from the management console by navigating to **Configuration** → **Configuration** → **Profile** → **full-ha** or **ha** → **Modcluster** → **Proxy** → **default (ajp)** and clicking **View**.

For more information, see [ModCluster Subsystem Attributes](#) in the *Configuration Guide* for JBoss EAP.

Configure SSL SNI Contexts from Management Console

You can now configure SSL SNI contexts from the management console by navigating to **Configurations** → **Subsystems** → **Security (Elytron)** → **Other Settings** and clicking **View**. Click **SSL** → **Server SSL SNI Context** to add, edit, or remove contexts.

For more information, see [Configuring SSL SNI Context](#) in the *How to Configure Server Security* guide for JBoss EAP.

View Non Progressing Operations

The management console now displays a notification when a non progressing operation occurs. The notification is accessible from the **Runtime** tab.

When running a standalone server, navigate to the **Runtime** → **Monitor** → **Management Operations** and click **View**. The **Cancel Non Progressing Operations** button is located in the upper right corner of the window, next to the **Reload** button. The notification will list any non progressing operations.

In a managed domain, this notification is accessible by navigating to the **Runtime** tab. In the **Browse By** column, click **Management Operations**.

Configure Modcluster Proxies

This release introduces multi-server support for the **Modcluster** subsystem, available from the **Configuration** tab of the console. The Modcluster column is now titled **Proxy** and lists the proxies under `/subsystem=modcluster/proxy=*`.

The **Add** and **Remove** actions make proxy management easier, and the **View** action opens the configuration options for the proxy selected.

For more information, see [ModCluster System Attributes](#) in the *Configuration Guide* for JBoss EAP.

Reinitialize a Trust Manager from Management Console

You can now reinitialize a trust-manager configured in JBoss EAP from the management console by navigating to **Runtime** → **Monitor** → **Security (Elytron)** → **SSL**, clicking **View**, and selecting **Trust Manager**. For more information, see [Reinitializing a Trust Manager from the management console](#) in the *How to Configure Server Security* for JBoss EAP

Configure JASPI Authentication from Management Console

You can now configure the JASPI authentication module from the management console by navigating to **Configuration** → **Subsystem** → **Security (Elytron)** → **Other Settings** and clicking **View**. Click **Other Settings** → **JASPI Configuration** to configure the module.

For more information, see [Security Management](#) in the *Security Architecture* guide for JBoss EAP.

Configure Remote ActiveMQ Server Resources from the Management Console

You can now configure the following Remote ActiveMQ server resources from the management console:

- Generic Connector

- In VM Connector
- HTTP Connector
- Remote Connector
- Discovery Group
- Connection Factory
- Pooled Connection Factory
- External JMS Queue
- External JMS Topic

For more information, see [Configure Remote ActiveMQ Server Resources Using the Management Console](#) in the *Configuring Messaging* guide for JBoss EAP.

View Socket Binding Name and Open Ports for a Server from Management Console

You can now view the socket binding name and the open ports for a server from the management console. The information is visible when the server is in the following states:

- **running**
- **reload-required**
- **restart-required**

For more information, see the [Viewing Socket Bindings and Open Ports for a Server](#) section in the *Configuration Guide* for JBoss EAP.

Runtime Operations Supported on Management Console

Some runtime operations that could be performed using only the management CLI are now available on the management console also.

For more information, see [Runtime Operations Using the Management Console](#) in the *Configuring Messaging* guide for JBoss EAP.

Configure a Let's Encrypt Account

You can now configure a Let's Encrypt account using the management console. The following configurations are available:

- Create an account with a certificate authority.
- Deactivate a certificate authority account.
- Update an account.
- View the certificate authority account information.
- Change certificate authority account key.

For information about configuring a Let's Encrypt account, see [Configure a Let's Encrypt Account Using Management Console](#) in the *How to Configure Server Security* guide for JBoss EAP.

Keystore Certificate Authority Configuration Using the Management Console

You can now perform the following keystore certificate authority configurations using the management console:

- Change the alias for the entry.
- Export a certificate from a keystore entry to a file.
- Generate a certificate signing request.
- Remove an alias from the keystore.
- View the details of the certificate associated with an alias.
- Revoke the certificate associated with an alias.
- Determine if a certificate is due for renewal.

For information about keystore certificate management, see [Keystore Certificate Authority Operations Using the Management Console](#) in the *How to Configure Server Security* guide for JBoss EAP.

Configure MicroProfile Metrics Using the Management Console

You can now configure MicroProfile metrics using the management console.

The configurations available in the management console are:

- Enable or disable exposing metrics.
- Edit prefix.
- Enable or disable security.
- Reset non required fields to initial or default values.

For information on configuring MicroProfile metrics, see [Configure MicroProfile Metrics using the Management Console](#) section in the *Configuration Guide* for JBoss EAP.

Obtain Certificate from Let's Encrypt CA in SSL Wizard

You can now obtain a certificate from Let's Encrypt Certificate Authority in the SSL Wizard.

See the following links for information:

- [Enable SSL Using the Management Console for applications](#) in the *How to Configure Server Security* for JBoss EAP.
- [Enable SSL Using the Management Console for management interface](#) in the *How to Configure Server Security* for JBoss EAP.

Ability to Customize Management Console Title

You can now customize the management console title so that each of your JBoss EAP instances can be identified at a quick glance.

For more information, see [Customizing the Management Console Title](#) in the *Configuration Guide* for JBoss EAP.

1.5. WEB SERVER

Console access logging

A new feature has been added that outputs access log data to the console. Console access logging data is written to **stdout** as a single line of JSON-structured data.

For more information, see [Configuring a Server](#) in the *Configuration Guide* for JBoss EAP.

1.6. LOGGING

Ability to Format Syslog Messages

You can now format the message of the syslog payload using the **named-formatter** attribute.

For more information about using the **named-formatter** attribute, see [Configure Syslog Handler Settings](#) in the *Configuration Guide*.

1.7. DEPLOYMENTS

Display Modules According to Deployment

You can now view a list of modules according to deployment using the **list-modules** management operation.

For more information about using the **list-modules** management operation, see the [Display Modules by Deployment](#) section in the *Development Guide* for JBoss EAP.

1.8. EJB

Multiple Delivery Groups Support for Message-Driven Beans

A message-driven bean (MDB) can now belong to more than one delivery groups. Message delivery is enabled only when all the delivery groups that an MDB belongs to are active.

For more information, see [Delivery Groups](#) in the *Developing EJB Applications* guide for JBoss EAP.

1.9. CLUSTERING

New Attribute **initial-load** in the **mod_cluster** Subsystem

The **mod_cluster** subsystem now defines a new attribute, **initial-load**.

The **initial-load** attribute helps to gradually increase the load value of a newly joined node to avoid overloading it while joining a cluster.

For information on this attribute, see the section [ModCluster Subsystem Attributes](#) in the *Configuration Guide* for JBoss EAP.

Ability to Determine the Primary Singleton Provider

You can now determine the primary singleton provider with the runtime resources that the **singleton** subsystem exposes for each singleton deployment or service created from a particular singleton policy.

For more information, see [Determine the Primary Singleton Service Provider Using the CLI](#) in the *Development Guide* for JBoss EAP.

Ability to Specify Distributable Session Manager Invocation

You can now specify that a distributable session manager be used when sharing sessions among subdeployments by adding **<distributable/>** tag under **<shared-session-config>** in **META-INF/jboss-all.xml** configuration file.

For more information, see [Configuring Session Sharing between Subdeployments in Enterprise Archives](#) in the *Development Guide* for JBoss EAP.

Ability to Notify Singleton Service Providers of the New Primary Provider

Every member of a cluster with a registered **SingletonElectionListener** receives a notification when a new primary singleton service provider is elected.

For more information, see [HA Singleton Service Election Listener](#) in the *Development Guide* for JBoss EAP.

The distributable-web subsystem for Distributable Web Session Configurations

The new **distributable-web** subsystem of JBoss EAP facilitates flexible and distributable web session configurations. The subsystem deprecates the **<replication-config>** element of **jboss-web.xml**.

For more information, see [The distributable-web subsystem for Distributable Web Session Configurations](#) in the *Development Guide* and [Overriding Default Distributable Session Management Behavior](#) in the *Migration Guide* for JBoss EAP.

Ability to Store Session Data in a Remote Red Hat Data Grid Cluster

The **distributable-web** subsystem can be configured to store web session data in a remote Red Hat Data Grid Cluster using the HotRod protocol. Storing web session data in a remote cluster allows the cache layer to scale independently of the application servers.

For information about configuring the **distributable-web** subsystem, see the [Storing Web Session Data In a Remote Red Hat Data Grid](#) in the *Development Guide* for JBoss EAP.

1.10. MESSAGING

Configure JMS Resources for a Remote Artemis-based Broker Using the resourceAdapter Element

You can configure JMS resources for a remote Artemis-based broker, such as Red Hat AMQ 7, using the **@JMSConnectionFactoryDefinition** annotation or the **@JMSDestinationDefinition** annotation. The **resourceAdapter** element defines which resource adapter is used for creating a JMS resource.

For more information, see [JMS Resources Configuration for a Remote Artemis-based Broker](#) in the *Configuring Messaging* book for JBoss EAP.

Configure Global Resources Usage for Messaging Servers

Three new attributes in the **address-setting** element help you control the global resources usage for messaging servers. For more information, see [Configure Global Resource Usage for Messaging Servers](#) in the *Configuring Messaging* book for JBoss EAP.

Configure the Timeout Value for Opening a Message Journal File

You can now configure the timeout value for opening message journal files using the **journal-file-open-timeout** attribute.

For more information about configuring the **journal-file-open-timeout** attribute, see [Configuring Message Journal Attributes](#) in the *Configuring Messaging* book for JBoss EAP.

Change in Artemis Logging Codes

Artemis logging codes for Artemis core protocol have changed, whereas the Advanced Message Queuing Protocol (AMQP) codes remain the same. This creates a problem if you are monitoring issues based on these codes.

The logging codes changed because the codes were duplicated between AMQP and the Artemis core protocol.

Omit Prefix on Destination Names

You can configure a connection factory or pooled connection factory to omit the destination name prefix when communicating with a remote Artemis server. Use this option when configuring communication with a remote Artemis 2.x that is not in compatibility mode.

For more information, see [Using the Integrated Artemis Resource Adapter for Remote Connections](#) , step 3, or [Configuring the Artemis Resource Adapter to Connect to Red Hat AMQ](#) , step 4, in in the *Configuring Messaging* book for JBoss EAP.

Messaging Enhancements for Load Balancers

In addition to existing support for static HTTP load balancers, load balancers using `mod_cluster` are now supported. For more information, see [Messaging Behind a Load Balancer](#) in the *Configuring Messaging* book for JBoss EAP.

Messaging to clusters behind load balancers is now fully supported. Clients communicating with clusters behind an HTTP load balancer must re-use the initial connection rather than using the cluster topology. For more information, see [Client configuration for messaging behind a load balancer](#) in the *Configuring Messaging* book for JBoss EAP.

1.11. OPENSIFT

JBoss EAP 7.3 Beta JDK 8 OpenShift Image Available

A new JBoss EAP 7.3 Beta JDK 8 OpenShift image is available: **`jboss-eap-7-tech-preview/eap73-openjdk8-openshift-rhel7`**. Unlike the JBoss EAP 7.2 JDK 8 OpenShift image, pre-packaged database drivers are not included with the JBoss EAP 7.3 Beta JDK 8 OpenShift image.

This image is provided as a technology preview.



NOTE

Related product documentation is incomplete at this time and will be updated shortly.

JBoss EAP 7.3 Beta JDK 11 OpenShift Image Available

A new JBoss EAP 7.3 Beta JDK 11 OpenShift image is available: **`jboss-eap-7-tech-preview/eap73-openjdk11-openshift-rhel8`**.

This image is provided as a technology preview.



NOTE

Related product documentation is incomplete at this time and will be updated shortly.

CHAPTER 2. TECHNOLOGY PREVIEW



IMPORTANT

The following configurations and features are provided as Technology Preview only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs), might not be functionally complete, and Red Hat does not recommend to use them for production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

See [Technology Preview Features Support Scope](#) on the Red Hat Customer Portal for information about the support scope for Technology Preview features.

Examine the Health Check Using the Management Console

You can now examine the health check of a server using the management console. This functionality is available only when running JBoss EAP as a standalone server.

See [Examine the Health Check Using the Management Console](#) in the *Configuration Guide* for details on using this feature.

CHAPTER 3. UNSUPPORTED AND DEPRECATED FUNCTIONALITY

3.1. UNSUPPORTED FEATURES

Support for some technologies are removed due to the high maintenance cost, low community interest, and better alternative solutions.

Internal Datasources and Drivers for OpenShift JDK 11 image

The following internal datasources and drivers are no longer provided with the JBoss EAP for OpenShift JDK 11 image:

- MySQL
- PostgreSQL
- MongoDB

It is recommended that you use JDBC drivers obtained from your database vendor for your JBoss EAP applications.

For more information about installing drivers, see the [Modules, Drivers, and Generic Deployments](#) section in [Getting Started with JBoss EAP for OpenShift Container Platform](#).

For more information on configuring JDBC drivers with JBoss EAP, see the [JDBC drivers](#) section in the JBoss EAP Configuration Guide.

3.2. 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.

3.2.1. Platforms and Features

Support for the following platforms and features is deprecated:

Operating Systems and Related Web Servers

- Windows Server 2012 R2 and associated IIS web server

Databases and Database Connectors

- Oracle 12c
- PostgreSQL 10
- SQL Server 2016

CHAPTER 4. RESOLVED ISSUES

See [Resolved Issues for JBoss EAP 7.3](#) to view the list of issues that have been resolved for this release.

CHAPTER 5. FIXED CVES

JBoss EAP 7.3 Beta includes fixes for the following security-related issues:

- [CVE-2018-7489](#): **jackson-databind**: incomplete fix for CVE-2017-7525 permits unsafe serialization via c3p0 libraries
- [CVE-2018-1000632](#): **dom4j**: XML Injection in Class: Element. Methods: addElement, addAttribute which can impact the integrity of XML documents

CHAPTER 6. KNOWN ISSUES

See [Known Issues for JBoss EAP 7.3 Beta](#) to view the list of known issues for this release.

Revised on 2019-08-23 11:18:51 UTC