



Red Hat JBoss Enterprise Application Platform 8-beta

Release notes for Red Hat JBoss Enterprise Application Platform 8.0 Beta

These release notes contain important information related to Red Hat JBoss
Enterprise Application Platform release 8.0 Beta

Red Hat JBoss Enterprise Application Platform 8-beta Release notes for Red Hat JBoss Enterprise Application Platform 8.0 Beta

These release notes contain important information related to Red Hat JBoss Enterprise Application Platform release 8.0 Beta

Legal Notice

Copyright © 2022 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 release 8.0 Beta.

Table of Contents

PREFACE	4
MAKING OPEN SOURCE MORE INCLUSIVE	5
CHAPTER 1. HOW TO READ THE RED HAT JBOSS ENTERPRISE APPLICATION PLATFORM 8.0 BETA DOCUMENTATION	6
CHAPTER 2. JBOSS EAP 8.0 BETA CERTIFICATION STATUS	7
2.1. JBOSS EAP 8.0 BETA AND JAKARTA EE 10	7
2.2. PACKAGE NAMESPACE CHANGE	7
CHAPTER 3. SUPPORTED CONFIGURATIONS	8
Red Hat Single Sign-On SAML adapters support	8
CHAPTER 4. NEW FEATURES AND ENHANCEMENTS	9
4.1. MANAGEMENT CONSOLE	9
Inclusive language, label changes	9
Adding, editing, and removing constant HTTP headers to response messages	9
Displaying Java Message Service bridge statistics for processed messages	9
Configuring enhanced audit logging	9
Starting servers in suspended mode	10
Configuring the certificate-authority attribute for the certificate-authority-account resource	10
Configuring the OCSP as an Elytron trust manager	10
Pausing Java Message Service topics	10
Non-heap memory usage added to server status preview	10
Automatically add or update credential store passwords when you add or update a datasource	10
Create, read, update, and delete Elytron resources	10
Viewing the deployment hash value	11
Adding and configuring interceptors in the EJB 3 subsystem	11
Configuring Infinispan distributed web session affinity	11
Configuring global directories in EE subsystem	11
Configuring cipher suites in Elytron	11
4.2. SECURITY	12
JAAS realm in the elytron subsystem	12
Configure multiple certificate revocation lists in Elytron and Elytron client	12
Native OpenID Connect client	12
New hash-encoding and hash-charset attributes for hashed passwords	13
SSLv2Hello	13
Updates to filesystem-realm	13
4.3. CLUSTERING	14
Configuring web session replication using a ProtoStream	14
4.4. DATASOURCE SUBSYSTEM	14
Configuring custom exception-sorter or valid-connection-checker for a datasource	14
4.5. EJB3 SUBSYSTEM	14
JBoss EAP 8.0 Beta server interoperability with JBoss EAP 7 and JBoss EAP 6	14
Infinispan-based distributed timers	14
Distributable EJB subsystem	14
4.6. OPENSIFT	15
RH-SSO SAML support for JBoss EAP 8.0 Beta	15
Provisioning a JBoss EAP server using the Maven plug-in	15
OpenID Connect support for JBoss EAP source-to-image	15
Building application images using Source-to-Image	15
Override management attributes with environment variables	15

Environment variable checks for resolving management model expressions	15
4.7. QUICKSTARTS AND BOMS	16
Supported EAP 8 quickstarts	16
New JBoss EAP BOMs for Maven	16
4.8. SERVER MIGRATION TOOL	16
JBoss EAP Server Migration Tool	16
CHAPTER 5. UNSUPPORTED, DEPRECATED, AND REMOVED FUNCTIONALITY	17
5.1. UNSUPPORTED FEATURES	17
EAP operator	17
Logging	17
5.2. DEPRECATED FEATURES	17
JDK 11	17
Security manager	17
5.3. REMOVED FEATURES	17
Jolokia and Prometheus	17
Environment variables	17
JDK 8	18
Legacy security realms	18
Picketbox	18
PicketBox vault	18
PicketLink Subsystem	18
discovery-group and broadcast-group resources	19
Quickstarts	19
Red Hat Single Sign-On Client Adapter	20
Java service on Red Hat Enterprise Linux	20
BOMs	20
CHAPTER 6. KNOWN ISSUES	22

PREFACE

These release notes contain important information related to Red Hat JBoss Enterprise Application Platform 8.0 Beta.

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Due to the enormity of this endeavor, these changes will be gradually implemented over upcoming releases. For more details on making our language more inclusive, see our [CTO Chris Wright's message](#).

CHAPTER 1. HOW TO READ THE RED HAT JBOSS ENTERPRISE APPLICATION PLATFORM 8.0 BETA DOCUMENTATION

We are in the process of modernizing the Red Hat JBoss Enterprise Application Platform 8.0 documentation. We are working to create more solution-centric documentation.

The JBoss EAP 8.0 Beta documentation contains content specific to the JBoss EAP 8.0 Beta release including new and enhanced features found in JBoss EAP 8.0 Beta. Functionality from previous releases that are still supported in JBoss EAP 8.0 Beta can be accessed in the JBoss EAP 7.4 documentation set. You can access the documentation set at [Product Documentation for Red Hat JBoss Enterprise Application Platform 7.4](#).

The following is a suggested approach for using the JBoss EAP 8.0 Beta documentation:

1. Read the JBoss EAP 8.0 Beta Release Notes to learn about new, enhanced, unsupported, and removed features.
2. Read the other JBoss EAP 8.0 Beta documentation set for detailed information about new and enhanced features.
3. Read the JBoss EAP 8.0 Beta Migration Guide for details on how to migrate applications to JBoss EAP 8.0 Beta.
4. If you need information on features supported from previous releases that have not been enhanced in JBoss EAP 8.0 Beta, see the JBoss EAP 7.4 documentation set at [Product Documentation for Red Hat JBoss Enterprise Application Platform 7.4](#). For example, development and configuration guides are available in the JBoss EAP 7.4 documentation set.

CHAPTER 2. JBOSS EAP 8.0 BETA CERTIFICATION STATUS

2.1. JBOSS EAP 8.0 BETA AND JAKARTA EE 10

JBoss EAP 8.0 Beta is a major milestone on the way to the planned full support for Jakarta EE 10 in JBoss EAP 8.0 GA. JBoss EAP 8.0 Beta provides implementations of the Jakarta EE 10 APIs. Compared to Jakarta EE 8, that is supported by JBoss EAP 7.4, Jakarta EE 10 comes with many changes to Jakarta EE. For more information, see [how to migrate your JBoss EAP applications from Jakarta EE 8 to Jakarta EE 10](#).

2.2. PACKAGE NAMESPACE CHANGE

The packages used for all EE APIs have changed from **javax** to **jakarta**. This follows the move of Java EE to the Eclipse Foundation and the establishment of Jakarta EE.



NOTE

This change does not affect **javax** packages that are part of Java SE.

Additional resources

- For more information, see [The javax to jakarta Package Namespace Change](#) .

CHAPTER 3. SUPPORTED CONFIGURATIONS

The [Red Hat JBoss Enterprise Application Platform 8.0 Beta supported configurations](#) knowledgebase article on the Red Hat Customer Portal lists the Java Virtual Machines (JVMs) that support JBoss EAP 8.0 Beta, as well as tested configurations that include but are not limited to commonly used operating systems, databases, and JMS brokers.

Red Hat Single Sign-On SAML adapters support

Using Red Hat Single Sign-On SAML adapters with JBoss EAP 8.0 will be supported when the adapters are released as a **.zip** file by Red Hat Single Sign-On. For information about Red Hat Single Sign-On, see the [Red Hat Single Sign-On product page](#) .

CHAPTER 4. NEW FEATURES AND ENHANCEMENTS

4.1. MANAGEMENT CONSOLE

Inclusive language, label changes

Toward Red Hat's commitment to replacing problematic language in our code, documentation, and web properties, beginning with 8.0 Beta, the JBoss EAP management console will display more inclusive wording and labels. Specifically, you will notice the following changes to the management console resource addresses and user interface elements:

New term	Previous term
primary	master
secondary	slave
blocklist	blacklist
allowlist	whitelist

Adding, editing, and removing constant HTTP headers to response messages

In the JBoss EAP 8.0 Beta management console, you can now add, edit, or remove constant HTTP response headers. To add a new path and header, from the Server page, select **Constant Headers**, then click **Add**. To edit or remove an existing path header, select the path whose header you want to modify, then click either **Edit** or **Remove**.

Displaying Java Message Service bridge statistics for processed messages

A message bridge consumes messages from a source queue or topic, then sends them on to a target queue or topic, usually on a different server. A bridge can also send messages from one cluster to another. The Java Message Service (JMS) bridge provides statistics about messages that the bridge processed. Specifically, it collects the following data:

- number of messages successfully committed (message count)
- number of messages aborted (messages aborted)

With this update, the JBoss EAP 8.0 Beta management console includes a new **JMS Bridge** column to display these statistics in the Runtime section. Note that this new feature affects the `/subsystem=messaging-activemq/jms-bridge=*` resource.

Configuring enhanced audit logging

In the JBoss EAP 8.0 Beta management console, you can configure the following two additional audit logging attributes in your `/subsystem=elytron/syslog-audit-log=*` resource:

- **syslog-format**
Define the format for your audit log messages. Supported values are **RFC3164** and **RFC5424**. ("RFC" stands for "request for comments.")
- **reconnect-attempts**
Define the maximum number of failed attempts JBoss EAP should make to connect to the syslog server before closing the endpoint.

Starting servers in suspended mode

You can now use the JBoss EAP 8.0 Beta management console to start servers in suspended mode. Select the new **Start in suspended mode** option, available in the following drop-down menus:

- **Runtime > Topology**
- **Runtime > Server Groups**
- **Runtime > Server Groups > Server**
- **Runtime > Host > Server**

Configuring the certificate-authority attribute for the certificate-authority-account resource

With JBoss EAP 8.0 Beta, you can use any certificate authority for your **certificate-authority-account** Elytron resource. Previously, JBoss EAP supported only the Let's Encrypt certificate authority, and the **certificate-authority** attribute was not configurable.

With this update, you can add, configure, or remove any certificate authority by opening the JBoss EAP management console and clicking **Configuration > Subsystems > Security > Other Settings > Other Settings > Certificate Authority**. From there, click **Add** to add a new certificate authority. To modify one you already have, select it, then click **Edit**. To remove a certificate authority, select it, then click **Remove**.

Configuring the OCSP as an Elytron trust manager

With JBoss EAP 8.0 Beta, you can configure the Online Certificate Status Protocol (OCSP) as the trust manager for the Elytron **undertow** subsystem. Previously, JBoss EAP supported only a certificate revocation list (CRL) as trust manager.

With this update, you can configure the OCSP as your trust manager by opening the JBoss EAP management console and clicking **Configuration > Subsystems > Elytron > Other Settings > SSL > Trust Manager**. Next, either select or create a trust manager and then, from the Trust Manager window, select the **OCSP** tab and click **Add**.

Pausing Java Message Service topics

From the JBoss EAP 8.0 Beta management console, you can now navigate to **Runtime > Messaging > Server > Server Name > Destination** to select and then pause a Java Message Service (JMS) topic. After you address the related messaging issue, you can also resume the paused topic. JMS previously sent messages to all active subscribers without any way to interrupt them.

Non-heap memory usage added to server status preview

With JBoss EAP 8.0 Beta, you can see more information in the server status preview about the memory consumption of your server. Previously, the preview displayed only heap memory usage: **Used** and **Committed**. With this update, it also displays the same information for non-heap memory usage.

Automatically add or update credential store passwords when you add or update a datasource

Beginning with JBoss EAP 8.0 Beta, when you create a datasource from the management console, you can automatically add a password for that datasource to your credential store. From the management console, select **Configuration > Subsystems > Datasources** then click **Add** to add a new datasource. Next, enter the credential store name where you want to save the password for the new datasource, an alias for the credential, and the plain text password you want to use. To modify an existing datasource, select it, then click **Edit**.

Create, read, update, and delete Elytron resources

From the JBoss EAP 8.0 Beta management console, you can now create, read, update, or delete any of the following four evidence decoders:

- Aggregate Evidence Decoders
- Custom Evidence Decoders
- X500 Subject Evidence Decoders
- X509 Subject Alt Name Evidence Decoder

To take one of these actions, navigate to **Configuration > Subsystems > Security > Mappers & Decoders > Evidence Decoder**.

Viewing the deployment hash value

The JBoss EAP 8.0 Beta management console can now display your deployment hash value in the deployment preview. This means that you can determine at a glance whether your deployment was valid and successful.

Adding and configuring interceptors in the EJB 3 subsystem

From the JBoss EAP 8.0 Beta management console, you can now add and configure system-wide, server-side interceptors in the **ejb3** subsystem. From the console, select **Configuration > EJB > Container** to make your additions or changes.

Configuring Infinispan distributed web session affinity

With JBoss EAP 8.0 Beta, in the **distributable-web** subsystem, you now have more control over the affinity, or load balancer "stickiness", of a distributed web session. To change your session affinity to something other than the **Primary-owner** default, in the management console, click **Configuration > Distributable Web > View > Infinispan Session**. Next, choose a session and select **Affinity** to make your changes. Affinity options now include the following:

- Local
- None
- Primary-owner
- Ranked

Previously, the only available affinity was **Primary-owner**.

Configuring global directories in EE subsystem

With the JBoss EAP 8.0 Beta management console, you can now configure a new **ee** subsystem resource, **/subsystem=ee/global-directory=***. You can use a global directory to add content to a deployment class path without listing the contents of the directory. To configure a global directory resource, navigate to **Configuration > Subsystems > EE > Globals**

Configuring cipher suites in Elytron

With the JBoss EAP 8.0 Beta management console, you can now enable TLS 1.3 cipher suites using the **cipher-suite-names** attribute to secure your network connection. Specifically, you can now configure the following **elytron** subsystem resources:

- **/subsystem=elytron/client-ssl-context=***
- **/subsystem=elytron/server-ssl-context=***

To configure the **cipher-suite-names** attribute for the `/subsystem=elytron/client-ssl-context=*` resource from the management console, navigate to **Configuration > Subsystems > Security > Other Settings > SSL > Client SSL Context**.

To configure the **cipher-suite-names** attribute for the `/subsystem=elytron/server-ssl-context=*` resource from the management console, navigate to **Configuration > Subsystems > Security > Other Settings > SSL > Server SSL Context**.

4.2. SECURITY

JAAS realm in the elytron subsystem

In JBoss EAP 8.0 Beta, the legacy security subsystem has been removed. To continue using your custom login modules with the **elytron** subsystem, use the new Java Authentication and Authorization Service (JAAS) security realm, **jaas-realm**.



NOTE

jaas-realm only supports JAAS-compatible login modules. For information about JAAS, see [Java Authentication and Authorization Service \(JAAS\) Reference Guide](#).

jaas-realm does not support custom login modules that extend or are dependent upon PicketBox APIs.

Although **elytron** subsystem provides **jaas-realm**, it is preferable to use other existing security realms that the subsystem provides. These include **jdbc-realm**, **ldap-realm**, **token-realm**, and others. You can also combine different security realms by configuring **aggregate-realm**, **distributed-realm**, or **failover-realm**. If none of these suits your purpose, implement a custom security realm and use it instead of custom login module.

The following are cases where you should use **jaas-realm** instead of implementing a custom security realm:

- You are migrating to the **elytron** subsystem from legacy security and already have custom login modules implemented.
- You are migrating from other application servers to JBoss EAP and already have the login modules implemented.
- You require combining multiple login modules with various flags and options provided to those login modules. These flags and options might not be configurable for the provided security realms in the **elytron** subsystem.

For more information, see [Creating a JAAS realm](#) in the *Securing applications and management interfaces using multiple identity stores* guide.

Configure multiple certificate revocation lists in Elytron and Elytron client

You can now configure multiple certificate revocation lists (CRL) in the **elytron** subsystem and WildFly Elytron client when you use several Certificate Authorities (CA). You can specify the list of CRLs to use in the **certificate-revocation-lists** attribute in the **trust-manager**.

For more information, see [Configuring certificate revocation checks in Elytron](#) in the *Configuring SSL/TLS in JBoss EAP* guide.

Native OpenID Connect client

You can now secure applications deployed to JBoss EAP with OpenID Connect (OIDC) using the new

native support for OIDC instead of installing the previously required Red Hat Single Sign-On Client Adapter. The new **elytron-oidc-client** subsystem provides the native support. The Red Hat Single Sign-On Client Adapter is not provided in this release.

For more information, see [OpenID Connect configuration in JBoss EAP](#) in the *Using single sign-on with JBoss EAP* guide.

New hash-encoding and hash-charset attributes for hashed passwords

You can now specify the character set and the string format for the hashed passwords that are stored in **elytron** subsystem security realms by using the **hash-charset** and **hash-encoding** attributes. The default **hash-charset** value is **UTF-8**. You can set the **hash-encoding** value to either **base64** or **hex**; **base64** is the default for all realms except the **properties-realm** where **hex** is the default.

The new attributes are included in the following security realms:

- **filesystem-realm**
- **jdbc-realm**
- **ldap-realm**
- **properties-realm**

For more information, see the [Securing applications and management interfaces using an identity store](#) guide.

SSLv2Hello

Beginning with JBoss EAP 8.0 Beta, you can specify the **SSLv2Hello** protocol for **server-ssl-context** and **client-ssl-context** in the **elytron** subsystem.



WARNING

- You must configure another encryption protocol if you want to configure **SSLv2Hello** because the purpose of the latter is to determine which encryption protocols the connected server supports.
- **IBM JDK** does not support **SSLv2Hello** in its client, although a server-side connection always accepts this protocol.

Updates to filesystem-realm

You can now encrypt the clear passwords, hashed passwords, and attributes associated with identities in a **filesystem-realm** for better security. You can do this in two ways:

- Create an encrypted **filesystem-realm** by referencing a secret key in the **add** operation.
- Encrypt an existing **filesystem-realm** using the new **filesystem-realm-encrypt** command in the WildFly Elytron Tool.

You can now also enable integrity checks for a **filesystem-realm** to ensure that the identities in the **filesystem-realm** were not tampered with since the last authorized write. You can do this by referencing a key pair when you create the **filesystem-realm** using the **add** operation. WildFly Elytron generates a

signature for the identity file using the key pair. An integrity check runs whenever an identity file is read.

For more information, see [Filesystem realm in Elytron](#) in the *Securing applications and management interfaces using an identity store* guide.

4.3. CLUSTERING

Configuring web session replication using a ProtoStream

You can now configure web session replication using a ProtoStream instead of JBoss Marshalling in JBoss EAP 8.0 Beta.

See [How to configure web session replication to use ProtoStream instead of JBoss Marshalling in JBoss EAP 8.0 Beta](#).

4.4. DATASOURCE SUBSYSTEM

Configuring custom exception-sorter or valid-connection-checker for a datasource

You can now configure a custom **exception-sorter** or **valid-connection-checker** for a datasource using a JBoss Module.

See [How to configure a custom exception-sorter or valid-connection-checker for a datasource in JBoss EAP 8](#).

4.5. EJB3 SUBSYSTEM

JBoss EAP 8.0 Beta server interoperability with JBoss EAP 7 and JBoss EAP 6

In JBoss EAP 8.0 Beta you can enable interoperability between JBoss EAP 8.0 Beta and older versions of your JBoss EAP server. JBoss EAP supports Jakarta EE 10 whose API class uses the **jakarta** package namespace. However, older versions of JBoss EAP use the **javax** package namespace.



IMPORTANT

- The older versions supported are JBoss EAP 6 and JBoss EAP 7
- interoperability between JBoss EAP 6 and JBoss EAP 7 is not affected by this issue as both servers support the **javax** package namespace.

For more information about how to enable interoperability between JBoss EAP 8.0 Beta and older versions of JBoss EAP see, [how to enable interoperability](#) .

Infinispan-based distributed timers

In JBoss EAP 8.0 Beta, you can now use Infinispan-based distributed timers to schedule persistent Jakarta Enterprise Bean timers within a cluster, which you can scale to large clusters. For more information, see [EAP 8 - how to configure Infinispan based distributed timers](#) .

Distributable EJB subsystem

Use the **distributable-ejb** subsystem to configure clustering abstractions providers required for **ejb3** subsystem functionalities, such as:

- Stateful session beans (SFSB) cache factories
- Client mappings registries for EJB client applications
- Distributed EJB timers

You can currently define these providers at a system-wide level. It is planned to develop functionality to enable deployment-specific providers by customizing the **ejb3** subsystem. For more information, see [What is the distributable-ejb subsystem in EAP 8](#).

4.6. OPENSIFT

RH-SSO SAML support for JBoss EAP 8.0 Beta

Using Red Hat Single Sign-On SAML adapters with JBoss EAP 8.0 Beta Source-to-Image (S2I) image will be supported when the adapters are released. For more information, see [OpenShift, SSO SAML support for EAP 8](#).

Provisioning a JBoss EAP server using the Maven plug-in

You can now use the JBoss EAP Maven plug-in on OpenShift to:

- Provision a trimmed server using Galleon.
- Install your application on the provisioned server.
- Tune the server configuration using the JBoss EAP management CLI.
- Package extra files into the server installation, such as a **keystore** file.
- Integrate the plug-in into your JBoss EAP 8.0 Beta source-to-image application build.

For more information, see [Provisioning a JBoss EAP server using the Maven plug-in](#).

OpenID Connect support for JBoss EAP source-to-image

You can now secure applications deployed to JBoss EAP with OpenID Connect (OIDC) using the new **elytron-oidc-client** subsystem instead of installing the previously required Red Hat Single Sign-On Client Adapter. You can configure an **elytron-oidc-client** subsystem by using the environment variables to secure the application with OIDC. The Red Hat Single Sign-On Client Adapter is not provided in this release. For more information, see [Using OpenID Connect to secure JBoss EAP applications on OpenShift](#).

Building application images using Source-to-Image

In JBoss EAP 8.0 Beta, an installed server has been removed from Source-to-Image (S2I) builder images. Galleon feature-packs and layers are now used to provision the server during the S2I build phase. To provision the server, include and configure the JBoss EAP Maven plug-in in the **pom.xml** file of your application. For more information, see [Building application images using source-to-image in OpenShift](#).

Override management attributes with environment variables

To more easily adapt your JBoss EAP server configuration to your server environment, you can use an environment variable to override the value of any management attribute, without editing your configuration file. You cannot override management attributes of type **LIST**, **OBJECT**, or **PROPERTY**. In JBoss EAP 8.0 Beta OpenShift runtime image, this feature is enabled by default. For more information, see [Overriding management attributes with environment variables](#).

Environment variable checks for resolving management model expressions

JBoss EAP now supports environment variable checks when resolving management model expressions. In previous versions of JBoss EAP, the JBoss EAP server only checked for Java system properties in the management expression. Now, the server will check for a relevant environment variable in addition to the system property. If you use both, JBoss EAP observes and uses the Java system property rather than the environment variable to resolve the management model expression. For more information about using environment variables to resolve management model expressions, see [Environment variables and model expression resolution](#).

4.7. QUICKSTARTS AND BOMS

Supported EAP 8 quickstarts

All supported JBoss EAP 8 quickstarts are located at [jboss-eap-quickstarts](#).

New JBoss EAP BOMs for Maven

JBoss EAP BOMs provide the Maven BOM files that specify the versions of JBoss EAP dependencies that are needed for building or testing your Maven projects. In addition, Jakarta EE 10 BOMs provide dependency management for related frameworks such as Hibernate, RESTasy, and proprietary components like Infinispan and Client BOMs.

4.8. SERVER MIGRATION TOOL

JBoss EAP Server Migration Tool

The Server Migration Tool is now a standalone migration tool and is no longer included with JBoss EAP 8.0 Beta. You can download the migration tool separately.

CHAPTER 5. UNSUPPORTED, DEPRECATED, AND REMOVED FUNCTIONALITY

5.1. UNSUPPORTED FEATURES

The following features are not supported by Red Hat.

EAP operator

Red Hat JBoss Enterprise Application Platform 8.0 Beta does not support the EAP operator. You cannot deploy your JBoss EAP applications using the EAP operator. For more information, see [JBoss EAP Operator Support Policy](#).

Logging

JBoss EAP 8.0 Beta does not support Apache Log4j version 1 APIs. If your applications do not package **log4j.jar** and Log4j configuration as part of the application, then you must update them. For more information about migrating or updating your applications, see the Red Hat Knowledgebase solution [Migration: Apache Log4j version 1 is no longer provided in EAP 8](#).

5.2. DEPRECATED FEATURES

Some features are deprecated with this release. This means that no enhancements will be made to these features, and they might be removed in a future 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.

Support for the following platforms and features is deprecated:

JDK 11

Support for JDK 11 was deprecated in JBoss EAP 7.4, and JDK 11 continues to be deprecated in JBoss EAP 8.0 Beta. JBoss EAP 8.0 Beta continues to support JDK 17.

Security manager

The Java Security Manager is deprecated.

5.3. REMOVED FEATURES

Version 8.0 Beta removes the following features from JBoss EAP.

Jolokia and Prometheus

Jolokia and **Prometheus** have been removed in this release. These features have been dropped and will no longer be supported by Red Hat. JBoss EAP server exposes metrics through the server metrics endpoint: **<server address>:<management port>/metrics**.

Environment variables

Red Hat has removed the following environment variables in JBoss EAP 8.0 Beta:

- **GALLEON_PROVISION_DEFAULT_FAT_SERVER**
- **AB_JOLOKIA_AUTH_OPENSIFT**

- **AB_JOLOKIA_CONFIG**
- **AB_JOLOKIA_DISCOVERY_ENABLED**
- **AB_JOLOKIA_HOST**
- **AB_JOLOKIA_HTTPS**
- **AB_JOLOKIA_ID**
- **AB_JOLOKIA_OFF**
- **AB_JOLOKIA_OPTS**
- **AB_JOLOKIA_PASSWORD**
- **AB_JOLOKIA_PASSWORD_RANDOM**
- **AB_JOLOKIA_PORT**
- **AB_JOLOKIA_USER**
- **AB_PROMETHEUS_ENABLE**
- **AB_PROMETHEUS_JMX_EXPORTER_CONFIG**
- **AB_PROMETHEUS_JMX_EXPORTER_PORT**
- **JGROUPS_ENCRYPT_SECRET**

JDK 8

JDK 8 has been removed from Red Hat JBoss Enterprise Application Platform 8.0 Beta. JDK 11 or JDK 17 is now required.

Legacy security realms

The legacy security realms have been removed from JBoss EAP 8.0 Beta. Use the security realms provided in the **elytron** subsystem instead.

For more information, see the [Securing applications and management interfaces using an identity store](#) , and [Securing applications and management interfaces using multiple identity stores](#) guides.

Picketbox

PicketBox has been removed from Red Hat JBoss Enterprise Application Platform 8.0 Beta. Any legacy security configurations must be migrated to the **elytron** subsystem. For more information about migrating your security configurations to the **elytron** subsystem, see [Migrating to Elytron](#).

PicketBox vault

PicketBox vault has been removed from JBoss EAP 8.0 Beta. Use the credential store provided by the **elytron** subsystem to store sensitive strings instead.

For more information, see [Credentials and credential stores in Elytron](#) in the *Secure storage of credentials in JBoss EAP* guide.

PicketLink Subsystem

**NOTE**

Using Red Hat Single Sign-On SAML adapters with JBoss EAP 8.0 will be supported when the adapters are released as a **.zip** file by Red Hat Single Sign-On.

The PicketLink subsystem has been removed from JBoss EAP 8.0 Beta. Use Red Hat Single Sign-On instead of the PicketLink identity provider, and the Red Hat Single Sign-On SAML adapter instead of the PicketLink service provider.

For more information, see the following resources:

- Using Red Hat Single Sign-On - [Red Hat Single Sign-On product page](#) .
- Using the Red Hat Single Sign-On SAML adapter with JBoss EAP - [JBoss EAP adapter](#) in the *Securing Applications and Services Guide* .

discovery-group and broadcast-group resources

Red Hat JBoss Enterprise Application Platform 7.4 removed the **discovery-group** and **broadcast-group** resources. These resources are still removed in JBoss EAP8.0 Beta.

Additionally, Red Hat JBoss Enterprise Application Platform 7.4 reduced the impact to its web console by replacing all instances of **discovery-group** and **broadcast-group** resources with **jgroups-discovery-group** and **socket-discovery-group** resources.

JBoss EAP 7.3 deprecated the following resources in the **messaging** subsystem:

- **/subsystem=messaging-activemq/discovery-group=***
- **/subsystem=messaging-activemq/server=default/broadcast-group=***
- **/subsystem=messaging-activemq/server=default/discovery-group=***

JBoss EAP 7.3 replaced these deprecated resources with **jgroups-discovery-group** and **socket-discovery-group** resources. Each deprecated resource included an attribute from each replacement resource, with one attribute set to **null** and the other attribute set to a value greater than **0**. These settings caused both **discovery-group** and **broadcast-group** to remain active, but still assign all their functionality to the **jgroups-discovery-group** and **socket-discovery-group** resources.

Quickstarts

The following outdated or redundant quickstarts have been removed from JBoss EAP 8.0 Beta:

- **app-client**
- **bean-validation**
- **ejb-asynchronous**
- **ejb-in-ear**
- **ejb-in-war**
- **ejb-security**
- **ejb-security-jaas**
- **greeter**

- **helloworld-html5**
- **helloworld-mbean**
- **helloworld-mdb-propertysubstitution**
- **helloworld-rs**
- **helloworld-ssl**
- **inter-app**
- **jaxws-addressing**
- **jaxws-pojo**
- **jts-distributed-crash-rec**
- **kitchensink-angularjs**
- **kitchensink-ear**
- **kitchensink-jsp**
- **kitchensink-ml**
- **logging-tools**
- **managed-executor-service**
- **messaging-clustering**
- **payment-cdi-event**
- **resteasy-jaxrs-client**
- **spring-greeter**
- **spring-kitchensink-basic**
- **spring-kitchensink-springmvctest**
- **tasks-rs**
- **websocket-client**
- **xml-jaxp**

Red Hat Single Sign-On Client Adapter

Red Hat JBoss Enterprise Application Platform 8.0 Beta does not provide the Red Hat Single Sign-On Client Adapter. Use the new **elytron-oidc-client** subsystem to secure applications deployed to JBoss EAP with OpenID Connect (OIDC).

Java service on Red Hat Enterprise Linux

Java service (JSVC) running on Red Hat Enterprise Linux (RHEL) has been removed from JBoss EAP 8.0 Beta.

BOMs

The following BOMs have been removed:

- The **JBoss Jakarta EE 8 Specification APIs** BOM is removed. Use the **JBoss EAP EE** BOM in your Maven project.
- The **EAP Runtime Artifacts** BOM is removed. Use the **JBoss EAP EE** BOM in your Maven project.

For more information, see [changes relating to JBoss EAP 8 BOM updates](#) .

CHAPTER 6. KNOWN ISSUES

See [Known Issues for Red Hat JBoss Enterprise Application Platform 8.0 Beta](#) to view the list of known issues for this release.

Revised on 2022-12-16 12:18:18 UTC