



Red Hat JBoss Enterprise Application Platform 7.3

7.3.0 Release Notes

For Use with Red Hat JBoss Enterprise Application Platform 7.3

Red Hat JBoss Enterprise Application Platform 7.3 7.3.0 Release Notes

For Use with Red Hat JBoss Enterprise Application Platform 7.3

Legal Notice

Copyright © 2020 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.

Table of Contents

CHAPTER 1. JBOSS EAP 7.3 CERTIFICATION STATUS	5
JBoss EAP 7.3 is a Jakarta EE 8 Compatible Implementation	5
CHAPTER 2. SUPPORTED CONFIGURATIONS	6
Databases and Database Connectors	6
Java Development Kits	6
CHAPTER 3. NEW FEATURES AND ENHANCEMENTS	7
3.1. SECURITY	7
Elytron Audit Logging Performance and Reliability Tuning	7
JwtValidator Enhancements	7
Default SSLContext	7
Java Authentication SPI for Containers (JASPI) Security Using Elytron	7
Server SSL Server Name Indication (SNI) Contexts	7
Automatic Detection of Keystore Types	7
Java EE Security API Support in Elytron	8
Silent BASIC Authentication in Elytron	8
Utility to Migrate Properties-based Security Realm to Filesystem Realm in Elytron	8
Support for Hexadecimal Encoding in JDBC Realm	8
Support for Modular Crypt Passwords in JDBC Realm	8
Ability to Combine Multiple Security Realms for Authorization in an Aggregate Realm	9
Ability to Use the Subject Alternative Name Extension From X.509 Certificate as the Principal	9
Ability to Combine Multiple Evidence Decoders with Aggregate Evidence Decoder	9
Certificate Revocation Capability using OCSP	9
Syslog Audit Logging Enhancements	9
Elytron Support for Masked Passwords	9
Obtaining Server Certificates from Let's Encrypt	9
Principal Transformer Added to Aggregate Realm	9
Elytron Resource filesystem-realm Support	10
AJP Connector Enabled by Default in this Release	10
Custom Headers for HTTP Management Endpoints	10
3.2. SERVER MANAGEMENT	10
Changes to Maven Artifact and Module Names	10
Support for Eclipse MicroProfile Metrics	10
Suspend Servers Managed by a Host Controller	10
Support for JBoss EAP Subsystem Metrics in Prometheus Format	10
3.3. MANAGEMENT CLI	11
Disable Output Paging	11
Upgraded MicroProfile Health Check 2.0.1 Attributes for Liveness and Readiness Probes	11
3.4. MANAGEMENT CONSOLE	11
Configure Socket Log Handlers from Management Console	11
View Logging Profile Logs from Management Console	11
View Active Management Operations from Management Console	11
Two New Resources Available for the ModCluster Subsystem	11
Configure SSL SNI Contexts from Management Console	12
View Non Progressing Operations	12
Configure ModCluster Proxies	12
Reinitialize a Trust Manager from Management Console	12
Configure JASPI Authentication from Management Console	12
Configure Remote ActiveMQ Server Resources from the Management Console	12
View Socket Binding Name and Open Ports for a Server from Management Console	13

Runtime Operations Supported on Management Console	13
Configure a Let's Encrypt Account	13
Keystore Certificate Authority Configuration Using the Management Console	13
Configure MicroProfile Metrics Using the Management Console	14
Obtain Certificate from Let's Encrypt CA in SSL Wizard	14
Ability to Customize Management Console Title	14
3.5. WEB SERVER	14
Console access logging	14
Changes to the Behavior of the <code>HttpServletRequest.getServletPath</code> Method	14
3.6. LOGGING	15
Ability to Format Syslog Messages	15
Custom Log Filters	15
3.7. DEPLOYMENTS	15
Display Modules According to Deployment	15
3.8. EJB	15
Multiple Delivery Groups Support for Message-Driven Beans	15
Client and Server Interceptors	15
3.9. CLUSTERING	15
New Attribute <code>initial-load</code> in the <code>mod_cluster</code> Subsystem	15
Ability to Determine the Primary Singleton Provider	15
Ability to Specify Distributable Session Manager Invocation	16
Ability to Notify Singleton Service Providers of the New Primary Provider	16
The <code>distributable-web</code> subsystem for Distributable Web Session Configurations	16
Ability to Store Session Data in a Remote Red Hat Data Grid Cluster	16
Ability to Specify Ranked Multiple Routes Session Affinity	16
3.10. INFINISPAN	16
Enabling Statistics for Remote Cache Containers	16
3.11. WEB SERVICES	16
Optional <code><T></code> Parameter Types Available for RESTEasy	16
Support for HTTP Proxy in RESTEasy	17
Disable Processing of Client Providers	17
3.12. MESSAGING	17
Configure JMS Resources for a Remote Artemis-based Broker Using the <code>resourceAdapter</code> Element	17
Configure Global Resources Usage for Messaging Servers	17
Configure the Timeout Value for Opening a Message Journal File	17
Change in Artemis Logging Codes	17
Omit Prefix on Destination Names	18
Messaging Enhancements for Load Balancers	18
Processed Message Statistics Added to Apache Artemis	18
Use of Discovery Groups with JGroups in Standalone JMS Client	18
3.13. OPENSIFT	18
Reduce Memory Footprint with Galleon Feature-packs	18
EAP Operator for Automating Application Deployment on OpenShift	18
EAP Operator for Safe Transaction Recovery and EJB Remoting	19
Calculate JVM Memory Settings	19
Secure Artifact Repository Mirror URLs	19
New Version of ASYM-ENCRYPT	19
3.14. QUICKSTARTS AND BOMS	19
New Client BOM for JAX-WS	19
Changes to BOMs for Jakarta EE 8	19
CHAPTER 4. TECHNOLOGY PREVIEW	21
Examine the Health Check Using the Management Console	21

Support for MicroProfile Rest Client 1.3.2 and Later	21
4.1. SUPPORT FOR MICROPROFILE OPENTRACING 1.3.0	21
4.2. SUPPORT FOR MICROPROFILE METRICS 2.0.1	21
CHAPTER 5. UNSUPPORTED AND DEPRECATED FUNCTIONALITY	22
5.1. UNSUPPORTED FEATURES	22
Databases and Database Connectors	22
Internal Datasources and Drivers for OpenShift JDK 11 image	22
Eclipse MicroProfile Capabilities	22
5.2. DEPRECATED FEATURES	23
5.2.1. Platforms and Features	23
Operating Systems and Related Web Servers	23
Databases and Database Connectors	23
Java APIs	23
RHEL 6 AMI images	23
CHAPTER 6. RESOLVED ISSUES	24
CHAPTER 7. FIXED CVES	25
CHAPTER 8. KNOWN ISSUES	26

CHAPTER 1. JBOSS EAP 7.3 CERTIFICATION STATUS

JBoss EAP 7.3 is a Jakarta EE 8 Compatible Implementation

The 7.3 release of JBoss EAP is a Jakarta EE 8 compatible implementation for both Web Profile and Full Platform specifications. The release is also a certified implementation of the Java EE 8 Web Profile and the Full Platform specifications, like the previous releases.

For information about Jakarta EE, see [Jakarta EE FAQ](#).

CHAPTER 2. SUPPORTED CONFIGURATIONS

The following configurations are newly supported in JBoss EAP 7.3.

Databases and Database Connectors

- MySQL 8
- Oracle 19c
- PostgreSQL 11
- EnterpriseDB Postgres Plus Advanced Server 11
- SQL Server 2017

Java Development Kits

- Eclipse OpenJ9 (JDK 11)

CHAPTER 3. NEW FEATURES AND ENHANCEMENTS

3.1. 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.

Ability to Combine Multiple Security Realms for Authorization in an Aggregate Realm

You can now use multiple security realms for authorization in an **aggregate-realm** with the **authorization-realms** attribute.

For more information, see [Configure Authentication and Authorization Using Multiple Identity Stores](#) in the *How to Configure Identity Management* guide for JBoss EAP.

Ability to Use the Subject Alternative Name Extension From X.509 Certificate as the Principal

You can now configure an evidence decoder to use a subject alternative name from an X.509 certificate as the principal associated with that certificate.

For more information, see [Configuring Evidence Decoder for X.509 Certificate with Subject Alternative Name Extension](#) in the *How to Configure Server Security* guide.

Ability to Combine Multiple Evidence Decoders with Aggregate Evidence Decoder

Elytron now provides an aggregate evidence decoder to combine two or more evidence decoders into a single decoder.

For more information, see [Configuring an Aggregate Evidence Decoder](#) in the *How to Configure Server Security* guide.

Certificate Revocation Capability using OCSP

Elytron now provides certificate revocation capability using Online Certificate Status Protocol (OCSP), defined in [RFC6960](#), when undertow is used as a load balancer.

For more information, see [Using Online Certificate Status Protocol for Certificate Revocation](#) in the *How to Configure Server Security* guide for JBoss EAP.

Syslog Audit Logging Enhancements

Elytron syslog audit logging now supports log formats defined in [RFC5424](#) and [RFC3164](#) to describe audit events.

A new attribute, **reconnect-attempts**, is now available to configure the maximum number of times Elytron attempts to send successive messages to a syslog server before closing the connection when using UDP.

For more information about the enhancements, see [Syslog Audit Logging](#) in *How to Configure Server Security* guide for JBoss EAP.

Elytron Support for Masked Passwords

The original implementation of Elytron did not support masked passwords.

In JBoss EAP 7.3, masked password types are supported for backward compatibility with PicketBox passwords.

Obtaining Server Certificates from Let's Encrypt

In JBoss EAP 7.2, basic CLI commands were added to manage SSL.

In JBoss EAP 7.3, these commands have been enhanced to derive server certificates from the Let's Encrypt certificate authority.

Principal Transformer Added to Aggregate Realm

Elytron includes an aggregate security realm, which is a combination of two or more realms: an authentication realm and one or more authorization realms.

In JBoss EAP 7.2 and earlier, the capability of transforming the principal after loading the authentication identity and before loading the authorization identity did not exist.

Now an aggregate realm can be configured with a principal transformer, which is defined in the mappers configuration, to perform this transformation.

Elytron Resource filesystem-realm Support

In JBoss EAP 7.1 and 7.2, usage of the **filesystem-realm** was technology preview.

In this release, the **filesystem-realm** as an Elytron resource definition backed by a file system is now supported.

AJP Connector Enabled by Default in this Release

In JBoss EAP 7.3, the AJP connector in the **undertow** subsystem is enabled by default. The AJP connector has been identified as a potential security risk for this subsystem.

See <https://access.redhat.com/solutions/4851251> for recommended methods to resolve this risk.

Custom Headers for HTTP Management Endpoints

Previous releases of JBoss EAP did not include the ability to define custom HTTP headers for endpoints in the management interface.

In JBoss EAP 7.3 a new attribute, **constant-headers**, is added to the HTTP management interface resource definition. Administrators can use this attribute to specify additional HTTP headers for JBoss EAP to return when responding to requests made against the HTTP management interface.

3.2. SERVER MANAGEMENT

Changes to Maven Artifact and Module Names

In JBoss EAP 7.3 artifact **org.jboss.resteasy:resteasy-validator-provider-11** is renamed as **org.jboss.resteasy:resteasy-validator-provider**.

Additionally, module **org.jboss.resteasy.resteasy-validator-provider-11** is now classified as an alias of module **org.jboss.resteasy.resteasy-validator**. Newly created applications should reference module **org.jboss.resteasy.resteasy-validator**. Existing applications can still reference the alias with no effect to their functionality.

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.

3.3. 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.

Upgraded MicroProfile Health Check 2.0.1 Attributes for Liveness and Readiness Probes

In previous releases, it was not possible to obtain the MicroProfile health status of **liveness** and **readiness** probes individually using the management CLI.

It is now possible to obtain the status of **liveness** and **readiness** probes separately using the **:check-live** and **:check-ready** operations respectively, or by using the **/health/live** and **/health/ready** HTTP endpoints.

The existing **/health** HTTP endpoint and **:check** management operation are now used to obtain **all** check probes (both **liveness** and **readiness** probes).

The current MicroProfile Health Check 2.0.1 capabilities are not fully backwards compatible with the previous version at this time.

For more information, see [MicroProfile Health Check](#) in the *Configuration Guide*.

3.4. 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.

3.5. 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.

Changes to the Behavior of the `HttpServletRequest.getServletPath` Method

The `HttpServletRequest.getServletPath` method behaves differently in Undertow than it did in the JBoss Web subsystem. Specifically, in Undertow, this method returns the JSP name rather than the action name.

An attribute has been added to configure the `HttpServletRequest.getServletPath` method to behave as it did in the JBoss Web subsystem.

3.6. LOGGING

Ability to Format Syslog Messages

You can now configure the **named-formatter** attribute using the management console.

Custom Log Filters

In JBoss EAP 7.2 and earlier, users were limited to the provided log filters.

In JBoss EAP 7.3, users can implement custom log filters.

3.7. 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*.

3.8. 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.

Client and Server Interceptors

JBoss EAP 7.2 and earlier only supported EJB interceptors configured in the container.

In JBoss EAP 7.3, client interceptors and server interceptors are now supported. Client and server interceptors can be configured globally.

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

3.9. 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.

Ability to Specify Ranked Multiple Routes Session Affinity

You can now specify session affinity as an ordered list of nodes. If your load balancer supports multiple, ordered routes, in the event of a primary node failure, it can choose the optimal nodes in the order defined. It also ensures a definite failover target, if the primary owner of a specific session is inactive.

For information about the ranked affinity options, see [The distributable-web subsystem for Distributable Web Session Configurations](#) in the *Development Guide* for JBoss EAP. For information on how to enable ranked session affinity in your load balancer, see [Enabling Ranked Session Affinity in Your Load Balancer](#) in the *Configuration Guide* for JBoss EAP.

3.10. INFINISPAN

Enabling Statistics for Remote Cache Containers

You can now use the HotRod client to expose remote cache container statistics. The `statistics-enabled` attribute can be configured for remote cache containers using the management CLI. For more information, see [Configuring Remote Cache Containers](#) in the *Configuration Guide* for JBoss EAP.

3.11. WEB SERVICES

Optional `<T>` Parameter Types Available for RESTEasy

RESTEasy now supports the following `java.util.Optional` parameters as wrapper object types:

- **@QueryParam**
- **@MatrixParam**
- **@FormParam**
- **@HeaderParam**
- **@CookieParam**

For more information, see [java.util.Optional Parameter Types](#) in the *Developing Web Services Applications* book for JBoss EAP.

Support for HTTP Proxy in RESTEasy

The original implementation of RESTEasy did not include support for HTTP proxy.

In JBoss EAP 7.3, an HTTP proxy can be set up on the client builder using the JAX-RS API (Java API for RESTful Services).

Disable Processing of Client Providers

Client providers annotated using **@Provider** must be registered for every instance of the JAX-RS container runtime. The system property **resteasy.client.providers.annotations.disabled** disables the default processing of client providers that are annotated with **@Provider** to prevent issues with undesired or duplicated client provider registrations.

For more information, see [Content Marshalling with @Provider Classes](#) in the *Developing Web Services Applications* book for JBoss EAP.

3.12. 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 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.

Processed Message Statistics Added to Apache Artemis

The Apache Artemis project added the following statistics:

- messages processed
- messages aborted/rolled back

These statistics are now available in JBoss EAP using the following CLI commands:

```
/subsystem=messaging-activemq/jms-bridge=bridge:read-attribute(name=message-count)
```

```
/subsystem=messaging-activemq/jms-bridge=bridge:read-attribute(name=aborted-message-count)
```

Use of Discovery Groups with JGroups in Standalone JMS Client

The use of discovery groups with JGroups in a standalone JMS client is deprecated.

Discovery groups should only be used with Netty UDP.

3.13. OPENSIFT

Reduce Memory Footprint with Galleon Feature-packs

You can now customize the main JBoss EAP for OpenShift image configuration to include only the capabilities that you require, thereby reducing the memory footprint. The provisioning tool, [Galleon](#), offers several layers that you can select to control the capabilities present in the JBoss EAP server.

Additionally, you can package customized capabilities as Galleon feature-packs that are installed during the JBoss EAP server Galleon provisioning. For JBoss EAP for OpenShift Source-to-Image (S2I), you can build your feature-packs offline, deploy them to Maven and reference them in your **provisioning.xml** file.

EAP Operator for Automating Application Deployment on OpenShift

JBoss EAP now offers EAP operator, a JBoss EAP-specific controller, to automate common deployment-related tasks. You can install the EAP operator using OperatorHub, the graphical interface that OpenShift cluster administrators use to discover, install, and upgrade operators.

For information about how to install, uninstall and use the EAP operator to deploy Java applications on OpenShift, see [EAP Operator for Automating Application Deployment on OpenShift](#) in the *Getting Started with JBoss EAP for OpenShift Container Platform* book.

EAP Operator for Safe Transaction Recovery and EJB Remoting

The EAP operator ensures safe transaction recovery in your application cluster by verifying that all transactions are completed before scaling down the replicas and marking the pod as **clean** for termination.

The EAP operator uses [StatefulSet](#) for the appropriate handling of EJB remoting and transaction recovery processing. The **StatefulSet** ensures persistent storage and network hostname preservation even after the pods are restarted.

For information about safely recovering transactions using the EAP operator, see [EAP Operator for Safe Transaction Recovery](#). For information about configuring EJB remoting using the EAP operator, see [Configuring EJB on OpenShift](#) in the *Getting Started with JBoss EAP for OpenShift Container Platform* book.

Calculate JVM Memory Settings

JBoss EAP 7.2 and earlier did not address conditions where JVM memory settings are higher than the container limit.

The OpenShift JBoss EAP image can now calculate default JVM memory settings when a container limit has been defined and the JVM memory settings are higher than the container limit.

For more information, see [JVM Memory Configuration](#) in the *Getting Started with JBoss EAP for OpenShift Container Platform* book.

Secure Artifact Repository Mirror URLs

To prevent "man-in-the-middle" attacks through the Maven repository, JBoss EAP requires the use of secure URLs for artifact repository mirror URLs.

For more information, see the subsection "Secure Artifact Repository Mirror URLs" in [Artifact Repository Mirrors](#) in *Getting Started with JBoss EAP for OpenShift Container Platform* .

New Version of ASYM-ENCRYPT

JBoss EAP 7.3 includes a new version of the **ASYM_ENCRYPT** protocol. The previous version of the protocol is deprecated. If you specify the **JGROUPS_CLUSTER_PASSWORD** environment variable, the deprecated version of the protocol is used and a warning is printed in the pod log.

For more information, see the section [Configuring ASYM_ENCRYPT](#) in the guide *Getting Started with JBoss EAP for OpenShift Container Platform* for JBoss EAP.

3.14. QUICKSTARTS AND BOMS

New Client BOM for JAX-WS

JBoss EAP now provides a new client BOM, **wildfly-jaxws-client-bom**, to manage JAX-WS dependencies. For information on how to add the **wildfly-jaxws-client-bom** dependencies to your project, see [JBoss EAP Client BOMs](#) in the *Development Guide* for JBoss EAP.

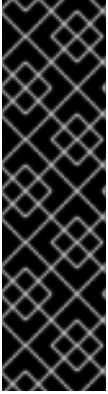
Changes to BOMs for Jakarta EE 8

Some JBoss EAP BOMs in the Group ID **org.jboss.bom** were replaced as a result of the move to

Jakarta EE 8 platform in JBoss EAP 7.3. If your applications use the BOMs that were replaced, update the project POMs to contain the Artifact IDs of the new BOMs, when migrating the applications to the JBoss EAP 7.3 release.

For information about changes to EAP BOMs, see [Changes to BOMs for Jakarta EE 8](#) in the *Migration Guide* for JBoss EAP.

CHAPTER 4. 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.

Support for MicroProfile Rest Client 1.3.2 and Later

JBoss EAP now supports MicroProfile Rest Client 1.3.2 and later versions. See [MicroProfile REST Client](#) in the *Developing Web Services Applications* guide for JBoss EAP for information about MicroProfile Rest Client.

If you were using the previous version of the MicroProfile REST client, you need to make some updates in your code. For more information about the code changes, see [Changes Required in MicroProfile Rest Client Code](#).

4.1. SUPPORT FOR MICROPROFILE OPENTRACING 1.3.0

JBoss EAP now supports MicroProfile OpenTracing 1.3.0. See [Tracing Requests with the MicroProfile OpenTracing SmallRye Subsystem](#) in the Configuration Guide for information about the **microprofile-opentracing-smallrye** subsystem.

4.2. SUPPORT FOR MICROPROFILE METRICS 2.0.1

JBoss EAP now supports MicroProfile Metrics 2.0.1. See [Eclipse MicroProfile Metrics](#) in the Configuration Guide for information about the **microprofile-metrics-smallrye** subsystem.

CHAPTER 5. UNSUPPORTED AND DEPRECATED FUNCTIONALITY

5.1. UNSUPPORTED FEATURES

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

The content set forth herein does not constitute a binding agreement or impose any legal obligation on Red Hat. This information is provided for discussion purposes only and is subject to change.

Databases and Database Connectors

- MySQL 5
- Oracle 12c
- PostgreSQL 10
- EnterpriseDB Postgres Plus Advanced Server 10
- SQL Server 2016

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.

Eclipse MicroProfile Capabilities

The following Eclipse MicroProfile capabilities that were included as technology preview in JBoss EAP 7.3 CD releases and in the JBoss EAP 7.3 beta release are no longer available:

- microprofile-smallrye-health
- microprofile-smallrye-metrics
- microprofile-smallrye-config
- microprofile-smallrye-opentracing

We plan to deliver JBoss EAP support of Eclipse MicroProfile APIs in a future release via an expansion mechanism.

5.2. 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.

5.2.1. 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
- The use of Red Hat JBoss Operations Network (JON) for managing JBoss EAP is deprecated. The use of Red Hat JBoss Operations Network (JON) for managing JBoss EAP was deprecated in the JBoss EAP 7.2 release. With the JBoss EAP 7.3 release, it is still deprecated.

The latest JON plugin update has received limited testing and bug fixing for JBoss EAP 7.3, in accordance with the limited support provided during the migration support phase of the JON lifecycle. Critical JON fixes for production JBoss EAP and other Red Hat Middleware workloads are provided in this phase of the lifecycle, however the plugins are not updated for new JBoss EAP capabilities. New capabilities may be unavailable through the plugin, or may introduce incompatibilities.

JON 3.3 requires that users install the JON EAP Management plug-in pack update 11 or newer to be compatible with JBoss EAP 7.3.

Databases and Database Connectors

- Oracle 12c

Java APIs

- SAAJ 1.3 was deprecated and SAAJ 1.4 is the default in JBoss EAP 7.3. The change in the default SAAJ version may cause issues with user defined SOAP handlers on migrating to JBoss EAP 7.3 from a previous release. To resolve issues arising due to SAAJ version, set the system property **-Djboss.saaj.api.version=1.3** to use the deprecated API.

RHEL 6 AMI images

Red Hat Enterprise Linux version 6 AMI images are deprecated. This means that while RHEL 6 AMI images are still included and supported, no enhancements will be made to these features and they may be removed in the future. Red Hat will continue providing full support and bug fixes under our standard support terms and conditions.

CHAPTER 6. RESOLVED ISSUES

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

CHAPTER 7. FIXED CVES

- [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
- [CVE-2019-9511](#): **undertow**: HTTP/2: large amount of data requests leads to denial of service
- [CVE-2019-9512](#): **undertow**: HTTP/2: flood using PING frames results in unbounded memory growth
- [CVE-2019-9514](#): **undertow**: HTTP/2: flood using HEADERS frames results in unbounded memory growth
- [CVE-2019-9515](#): **undertow**: HTTP/2: flood using SETTINGS frames results in unbounded memory growth
- [CVE-2019-10219](#): **hibernate-validator**: safeHTML validator allows XSS
- [CVE-2019-19343](#): **undertow**: Memory Leak in Undertow HttpOpenListener due to holding remoting connections indefinitely
- [CVE-2019-14838](#): **wildfly-core**: Incorrect privileges for 'Monitor', 'Auditor' and 'Deployer' user by default
- [CVE-2019-14885](#): **JBoss EAP**: Vault system property security attribute value is revealed on CLI 'reload' command
- [CVE-2019-16869](#): **netty**: HTTP request smuggling by mishandled whitespace before the colon in HTTP headers
- [CVE-2019-16942](#): **jackson-databind**: Serialization gadgets in classes of the commons-dbcp package
- [CVE-2019-16943](#): **jackson-databind**: Serialization gadgets in classes of the commons-dbcp package

CHAPTER 8. KNOWN ISSUES

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

Additionally, be aware of the following:

- In messages defined in **wildfly-core-eap** that have more than one parameter, the order of parameters may be incorrect in Japanese and Chinese.
A fix for this problem is planned for JBoss EAP 7.3.1.

For example:

Original English text:

Could not start app client <Parameter 1> as no main method was found on main class <Parameter 2>

Current (incorrect) Japanese translation:

メインクラス <Parameter 1> main メソッドが見つからなかったため、アプリケーションクライアント <Parameter 2> を起動できませんでした。

Correct Japanese translation:

メインクラス <Parameter 2> main メソッドが見つからなかったため、アプリケーションクライアント <Parameter 1> を起動できませんでした。

Revised on 2020-03-20 18:38:12 UTC