JBoss Enterprise Application Platform Continuous Delivery 20

JBoss EAP Continuous Delivery 20 Release Notes

For Use with JBoss Enterprise Application Platform Continuous Delivery 20

Last Updated: 2020-07-23

JBoss Enterprise Application Platform Continuous Delivery 20 JBoss EAP Continuous Delivery 20 Release Notes

For Use with JBoss Enterprise Application Platform Continuous Delivery 20

Legal Notice

Abstract

These release notes contain important information related to JBoss Enterprise Application Platform continuous delivery release 20, which is available as a Technology Preview release in the cloud only.

Table of Contents

CHAPTER 1. ABOUT JBOSS EAP CONTINUOUS DELIVERY 20

IMPORTANT

The JBoss Enterprise Application Platform continuous delivery stream (JBoss EAP CD) has been provided as a Technology Preview offering for the entirety of its availability. Based upon user feedback, and in accordance with the terms of the Technology Preview Features Support Scope, Red Hat has decided to deprecate the JBoss EAP CD stream.

The JBoss Enterprise Application Platform continuous delivery (JBoss EAP CD) release 20 is a Technology Preview release available in the cloud only. This JBoss EAP CD release introduces a new delivery stream of JBoss EAP. For JBoss EAP CD20, only release note documentation is provided. Additional documentation will be provided in following releases.

The purpose of this new delivery model is to quickly introduce new features ahead of the traditional JBoss EAP GA release. The JBoss EAP CD releases are only available in the OpenShift image format and can be accessed from the Red Hat Container Catalog.

Traditional JBoss EAP GA releases, the next being JBoss EAP 7.4, are based on an aggregate of JBoss EAP CD releases. They are available through the normal distribution methods.

IMPORTANT

This continuous delivery release for JBoss EAP is 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.

1.1. DIFFERENCES BETWEEN JBOSS EAP AND JBOSS EAP CONTINUOUS DELIVERY

There are notable differences between the JBoss EAP product and the continuous delivery release for JBoss EAP.

Table 1.1. Differences between JBoss EAP and JBoss EAP Continuous Delivery

JBoss EAP Feature	Status in JBoss EAP Continuous Delivery	Description
JBoss EAP management console	Not included	The JBoss EAP management console is not included in this release of JBoss EAP Continuous Delivery.

JBoss EAP Feature	Status in JBoss EAP Continuous Delivery	Description
JBoss EAP management CLI	Not recommended	The JBoss EAP management CLI is not recommended for use with JBoss EAP running in a containerized environment. Any configuration changes made using the management CLI in a running container will be lost when the container restarts.
Managed domain	Not supported	
Default root page	Disabled	The default root page is disabled, but you can deploy your own application to the root context as **ROOT.war**.
Remote messaging	Supported	Red Hat AMQ for inter-pod and remote messaging is supported. JBoss EAP CD releases only support client messaging, and Red Hat AMQ provides the messaging broker.
Transaction recovery	Partially supported	

CHAPTER 2. NEW FEATURES AND ENHANCEMENTS

2.1. SECURITY

Support for automatic update of credentials in a credential store

Elytron now automates adding and updating a credential to a previously defined credential store when you configure a credential reference that specifies both the **store** and **clear-text** attributes.

With this update, you do not need to add a credential to an existing credential store before you can reference it from a **credential-reference**. The automated process reduces the number of steps you need to perform for referencing new credentials in different subsystems.

New role mapper regex-role-mapper in Elytron

Elytron now provides a new role mapper, **regex-role-mapper**, to define a regular expression (regex) based mapping of security roles.

You can use **regex-role-mapper** to translate a list of roles to simpler roles. For example:

- ***-admin** to **admin**
- ***-user** to **user**

With **regex-role-mapper**, you do not need to implement your own custom component to translate security roles.

Accessing IP address of remote client

In the JBoss EAP CD 20 release, you can add the **source-address-role-decoder** role decoder to the **elytron** subsystem. By configuring this role decoder, you can gain additional information from a remote client when making authorization decisions.

The **source-address-role-decoder** extracts the IP address of a remote client and checks that it matches the IP address specified in the **pattern** attribute or the **source-address** attribute. If the IP address of the remote client matches the IP address specified in either attribute, the **roles** attribute then assigns roles to the user. When you have configured **source-address-role-decoder**, you can reference it in the **role-decoder** attribute of the **security domain**.

The aggregate-role-decoder role decoder

The **aggregate-role-decoder** consists of two or more role decoders. After each specified role decoder completes its operation, it adds roles to the **aggregate-role-decoder**.

You can use **aggregate-role-decoder** to make authorization decisions by adding role decoders that assign roles for a user. Further, **aggregate-role-decoder** provides you with a convenient way to aggregate the roles returned from each role decoder.

2.2. WEB SERVER

Configuring SameSite cookie attribute

You can now configure the **SameSite** attribute for cookies in the current JBoss EAP release with a **samesite-cookie** predicated handler in the **undertow** subsystem. With this handler, you can update your server configuration without having to change your applications. This enhancement supports changes to the processing of cookies that were recently implemented in major web browsers to improve security.

2.3. EJB3 SUBSYSTEM

Default global stateful session bean timeout value in the **ejb3** subsystem

In the **ejb3** subsystem, you can now configure a default global timeout value for all stateful session beans (SFSBs) that are deployed on your server instance by using the **default-stateful-bean-session-timeout** attribute. This attribute is located in the JBoss EAP server configuration file. You can configure the attribute using the Management CLI.

Attribute behavior varies according to the server mode. For example:

- When running in the standalone server, the configured value gets applied to all SFSBs deployed on the application server.
- When running in the managed domain, all SFSBs that are deployed on server instances within server groups receive concurrent timeout values.

NOTE

When you change the global timeout value for the attribute, the updated settings only apply to new deployments. Reload the server to apply the new settings to current deployments.

By default, the attribute value is set at **-1** milliseconds, which means that deployed SFSBs are configured to never time out. However, you can configure two other types of valid values for the attribute, as follows:

- When the value is **0**, SFSBs are eligible for immediate removal by the **ejb** container.
- When the value is greater than **0**, the SFSBs remain idle for the specified time before they are eligible for removal by the **ejb** container.

You can still use the pre-existing **@StatefulTimeout** annotation or the stateful-timeout element, which is located in the **ejb-jar.xml** deployment descriptor, to configure the timeout value for an SFSB. However, setting such a configuration overrides the default global timeout value to the SFSB.

Forcing Jakarta Enterprise Beans timer refresh in **database-data-store**

You can now set the **wildfly.ejb.timer.refresh.enabled** flag using the EE interceptor. When an application calls the **TimerService.getAllTimers()** method, JBoss EAP checks this flag. If this flag is set to **true**, JBoss EAP refreshes the Jakarta Enterprise Beans timers from database before returning the result.

In the previous JBoss EAP releases, the Jakarta Enterprise Beans timer reading could be refreshed in a database using the **refresh-interval** attribute found in **database-data-store**. Users could set the **refresh-interval** attribute value in milliseconds to refresh the Jakarta Enterprise Beans timer reading.

Access to runtime information from Jakarta Enterprise Beans

The **ejb3** subsystem includes the ability to expose runtime data using annotations or deployment descriptors. Prior versions of JBoss EAP did not include the ability to retrieve this runtime information.

For JBoss EAP CD 20, the **ejb3** includes the ability to retrieve this runtime information.

2.4. HIBERNATE

Configuring the **wildfly.jpa.skipquerydetach** persistence unit property

You can configure the **wildfly.jpa.skipquerydetach** persistence unit property from the **persistence.xml** file of a container-managed persistence context.

The default value for **wildfly.jpa.skipquerydetach** is **false**. Use this setting to set a transaction-scoped persistence context to immediately detach query results from an open persistence context.

Configure **wildfly.jpa.skipquerydetach** as **true**, to set a transaction-scoped persistence context to detach query results when a persistence context is closed. This enables a non-standard specification extension.

For applications that have the non-standalone specification extension **jboss.as.jpa.deferdetach** set as **true**, you can also set **wildfly.jpa.skipquerydetach** as **true**.

2.5. WEB SERVICES

Ability for RESTEasy 3.x to access all standard MicroProfile ConfigSources

RESTEasy 3.x can now access all standard MicroProfile **ConfigSources**. The following additional **ConfigSources** are also added to RESTEasy 3.x:

- **servlet init-params** (ordinal 60)
- **filter init-params** (ordinal 50)
- **servlet context-params** (ordinal 40)

Previously, these capabilities were only included in RESTEasy 4.x. With this update, RESTEasy can access configuration parameters with or without the MicroProfile **ConfigSources**. In the absence of a MicroProfile Config implementation, RESTEasy falls back to the older method of gathering parameters from **ServletContext** parameters and **init** parameters.

CHAPTER 3. UNSUPPORTED FUNCTIONALITY

3.1. UNSUPPORTED FEATURES

Support for some technologies are removed due to the high maintenance cost, low community interest, and better alternative solutions. This release does not introduce any newly unsupported features.

However, the unsupported features listed in the Unsupported Features section of the release notes for JBoss EAP CD 19 also apply to this continuous delivery release for JBoss EAP, unless they are mentioned in the New Features and Enhancements section of this document.

CHAPTER 4. RESOLVED ISSUES

See Resolved Issues for JBoss EAP CD 20 to view the list of issues that have been resolved for this release.

CHAPTER 5. FIXED CVES

JBoss EAP Continuous Delivery 20 includes fixes for the following security-related issues:

- CVE-2020-10740: **wildfly**: Unsafe deserialization in Wildfly Enterprise Java Beans.
- CVE-2020-10714: **wildfly-elytron**: Session fixation when using FORM authentication.
- CVE-2020-6950 **Mojarra**: Path traversal using either the **loc** parameter or the **con** parameter, incomplete fix of CVE-2018-14371.
- CVE-2020-1954: **cxf-core**: **cxf**: JMX integration is vulnerable to a MITM attack.
- CVE-2018-14371: **jsf-impl**: **Mojarra**: Path traversal in **ResourceManager.java:getLocalePrefix()** using the **loc** parameter.
- CVE-2020-10683: **dom4j**: XML External Entity vulnerability in default SAX parser.
- CVE-2020-10705: **undertow**: Memory exhaustion issue in **HttpReadListener** with "Expect: 100-continue" header.
- CVE-2020-11612: **netty**: Compression/decompression codecs do not enforce limits on buffer allocation sizes.
- CVE-2020-1719: **wildfly**: The **EJBContext** principal is not popped back after invoking another EJB using a different security domain.
- CVE-2019-10172: **jackson-mapper-asl**: XML external entity similar to CVE-2016-3720.
- CVE-2020-10719: **undertow**: Invalid HTTP request with large chunk size.
- CVE-2020-10673**jackson-databind**: The interaction between serialization gadgets and typing is mishandled and this could result in remote command execution.

CHAPTER 6. KNOWN ISSUES

See Known Issues for JBoss EAP CD 20 to view the list of known issues for this release.

Revised on 2020-07-23 15:02:50 UTC