JBoss Enterprise Application Platform Continuous Delivery 19

JBoss EAP Continuous Delivery 19 Release Notes

For Use with JBoss Enterprise Application Platform Continuous Delivery 19

Last Updated: 2020-04-24

JBoss Enterprise Application Platform Continuous Delivery 19 JBoss EAP Continuous Delivery 19 Release Notes

For Use with JBoss Enterprise Application Platform Continuous Delivery 19

Legal Notice

Abstract

These release notes contain important information related to JBoss Enterprise Application Platform continuous delivery release 19, which is available as a Technology Preview release in the cloud only.

Table of Contents

CHAPTER 1. ABOUT JBOSS EAP CONTINUOUS DELIVERY 19

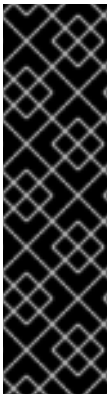
IMPORTANT

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 19 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 CD19, 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

Using TLS Protocol Version 1.3 with JDK 11

Elytron now provides the ability to use Transport Layer Security (TLS) Protocol version 1.3 for JBoss EAP running against JDK 11.

TLS 1.3 is disabled by default. You can enable TLS 1.3 by configuring the new **cipher-suite-names** attribute in the SSL Context resource definition in the **elytron** subsystem.

Compared with TLS 1.2, you might experience reduced performance when running TLS 1.3 with JDK 11. Diminished performance might occur when a very large number of TLS 1.3 requests are being made. A system upgrade to a newer JDK version can improve performance. Test your setup with TLS 1.3 for performance degradation before enabling it in production.

2.2. SERVER MANAGEMENT

Use a Global Directory to Distribute Shared Libraries Across Deployments

In JBoss EAP 7.3 and earlier versions, you could not create and configure a global directory to distribute shared libraries across deployments running on a server. These capabilities have been added to the **ee** subsystem.

A global directory offers a better alternative to the global module approach. For example, if you want to change the name of a library listed in a global module, you must remove the global module, change the library's name, and then add the library to a new global module. If you change the name of a library that is listed in the global directory, you only need to restart the server to make the library name change available for all deployments.

Using a global directory is also a better solution if you want to share multiple libraries across deployed applications.

2.3. MANAGEMENT CLI

Exposing Runtime Statistics for Managed Executor Services

In the previous JBoss EAP release, runtime statistics were not available for managed executor services in the **ee** subsystem.

You can now monitor the performance of managed executor services by viewing the runtime statistics generated with the new management CLI attributes. The following management CLI attributes have been added:

- **active-thread-count**: the approximate number of threads that are actively executing tasks
- **completed-task-count**: the approximate total number of tasks that have completed execution
- **hung-thread-count**: the number of executor threads that are hung
- **max-thread-count**: the largest number of executor threads
- **current-queue-size**: the current size of the executor's task queue
- **task-count**: the approximate total number of tasks that have been submitted for execution

- **thread-count**: the current number of executor threads

Using Property Replacement for Permissions Files

Users upgrading from JBoss EAP 6 to JBoss EAP 7 were unable to migrate file permissions in the Java policy file to the **permissions.xml** or **jboss-permissions.xml** files. It was not possible to use property replacement to migrate file permissions in the **permissions.xml** and **jboss-permissions.xml** files.

You can now use property replacement for the **permissions.xml** and **jboss-permissions.xml** files.

The property replacement for **jboss-permissions.xml** and **permissions.xml** files can be enabled or disabled using the **jboss-descriptor-property-replacement** and **spec-descriptor-property-replacement** attributes in the **ee** subsystem.

Configuring RESTEasy Parameters

You can now use the JBoss EAP management CLI to change the settings for RESTEasy parameters. A global change applies the updated settings to new deployments as **web.xml** context parameters.

You can modify the settings of a parameter by using the **:write-attribute** operation with the **/subsystem=jaxrs** resource in the management CLI. For example:

```
/subsystem=jaxrs:write-attribute(name=resteasy-add-charset, value=false)
```

NOTE

When you change the settings of a parameter, the updated settings only apply to new deployments. Restart the server to apply the new settings to current deployments.

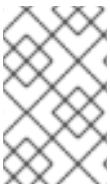
Configuring RESTEasy Providers

In RESTEasy, certain built-in providers are enabled by default. You can now use the new RESTEasy parameter **resteasy.disable.providers** in the JBoss EAP management CLI to disable specific built-in providers.

The following example demonstrates how to disable the built-in provider **FileProvider**:

```
/subsystem=jaxrs:write-attribute(name=resteasy-disable-providers, value=
[org.jboss.resteasy.plugins.providers.FileProvider])
```

You can use the **resteasy.disable.providers** parameter with the pre-existing parameter **resteasy.use.builtin.providers** to customize a specific provider configuration that applies to all new deployments.



NOTE

When you change the settings of the **resteasy.disable.providers** parameter, the updated settings only apply to new deployments. Restart the server to apply the new settings to current deployments.

2.4. WEB SERVICES

Integrating Elytron with Web Services Clients

You can now configure web services clients to use Elytron automatically to obtain the credentials, the authentication method, and the SSL context.

If you use the web services client and assign configuration properties to it using the JBossWS API, you are not prompted for credentials or required to accept server certificates if the valid configuration is in the Elytron client. The following authentication methods are supported:

- Username Token Profile authentication
- HTTP Basic authentication
- TLS protocol

The configuration is specified by the **<webservices/>** element in **wildfly-config.xml**.

2.5. ECLIPSE MICROPROFILE

Support for Eclipse MicroProfile Fault Tolerance 2.1

JBoss EAP supports the Eclipse MicroProfile Fault Tolerance 2.1 specification.

The Eclipse MicroProfile Fault Tolerance 2.1 specification defines the following patterns for handling a failure:

- Timeout
- Fallback
- Retry
- CircuitBreaker
- Bulkhead

A new subsystem, **microprofile-fault-tolerance-smallrye**, provides the Eclipse MicroProfile Fault Tolerance 2.1 integration in JBoss EAP.

Support for Eclipse MicroProfile JWT RBAC 1.1

JBoss EAP supports the Eclipse MicroProfile JWT RBAC 1.1 specification.

With Eclipse MicroProfile JWT RBAC, you can authenticate an identity using a cryptographically-signed JSON Web Token (JWT) token that is received in an HTTP request. The claims of the authenticated identity are verified using role-based access control (RBAC) for accessing microservice endpoints.

Eclipse MicroProfile JWT RBAC provides the following benefits:

- Eclipse MicroProfile JWT RBAC requires only minimal configuration within a deployment for establishing an identity.
- Eclipse MicroProfile JWT RBAC does not rely on access to external repositories of identities, such as databases or directory servers.

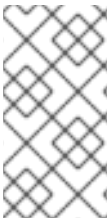
A new subsystem, **microprofile-jwt-smallrye**, provides the Eclipse MicroProfile JWT RBAC integration in JBoss EAP.

Support for Eclipse MicroProfile OpenAPI 1.1

JBoss EAP supports the Eclipse MicroProfile OpenAPI 1.1 specification.

The Eclipse MicroProfile OpenAPI specification defines an HTTP GET **/openapi** endpoint that returns an OpenAPI v3 compliant document. This document describes the RESTful services provided by an application. The supported document formats are YAML and JSON.

A new subsystem, **microprofile-openapi-smallrye**, provides the Eclipse MicroProfile OpenAPI integration in JBoss EAP.



NOTE

Currently, the /**openapi** endpoint for a virtual host can only document a single JAX-RS deployment. To use OpenAPI with multiple JAX-RS deployments that are registered with different context paths on the same virtual host, each deployment must use a distinct endpoint path.

Support for Eclipse MicroProfile Config 1.4

JBoss EAP supports the Eclipse MicroProfile Config 1.4 specification.

The **microprofile-config-smallrye** subsystem has been updated to integrate Eclipse MicroProfile version 1.4.

Support for Eclipse MicroProfile Health 2.2

JBoss EAP supports the Eclipse MicroProfile Health 2.2 specification.

The **microprofile-health-smallrye** subsystem has been updated to integrate Eclipse MicroProfile Health 2.2 in JBoss EAP.

NOTE

Health checks in subdeployments of an Enterprise Application Archive (EAR) deployment are not supported.

Support for Eclipse MicroProfile Metrics 2.3

JBoss EAP supports the Eclipse MicroProfile Metrics 2.3 specification.

The **microprofile-metrics-smallrye** subsystem has been updated to integrate Eclipse MicroProfile Metrics 2.3. The updated subsystem provides a new optional base metric **ProcessCpuTime**.

Eclipse MicroProfile OpenTracing 1.3

JBoss EAP supports the Eclipse MicroProfile OpenTracing 1.3 specification.

The **microprofile-opentracing-smallrye** subsystem has been updated to provide the Eclipse MicroProfile OpenTracing 1.3 integration in JBoss EAP.

The updated **microprofile-opentracing-smallrye** subsystem includes support for tracing JAX-RS and CDI. The subsystem also allows configuration of Jaeger Java Client.

Support for Eclipse MicroProfile REST Client 1.4

JBoss EAP now supports the MicroProfile REST Client 1.4 specification. MicroProfile REST Client 1.4 adds the Contexts and Dependency Injection (CDI) capability to the class **org.eclipse.microprofile.rest.client.ext.ClientHeadersFactory**.

CHAPTER 3. UNSUPPORTED AND DEPRECATED FUNCTIONALITY

3.1. UNSUPPORTED FEATURES

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

RESTEasy Parameters

RESTEasy provides a Servlet 3.0 **ServletContainerInitializer** integration interface that performs an automatic scan of resources and providers for a servlet. Containers can use this integration interface to start an application. Therefore, use of the following RESTEasy parameters is no longer supported:

- resteasy.scan
- resteasy.scan.providers
- resteasy.scan.resources

CHAPTER 4. RESOLVED ISSUES

See Resolved Issues for JBoss EAP CD 19 to view the list of issues that have been resolved for this release.

CHAPTER 5. FIXED CVES

JBoss EAP Continuous Delivery 19 includes fixes for the following security-related issues:

- CVE-2019-14540: REST: jackson-databind: Polymorphic typing issue related to com.zaxxer.hikari.HikariConfig.
- CVE-2019-16942: REST: jackson-databind: Serialization gadgets in classes of the commons-dbcp package.
- CVE-2019-10086: Server: commons-beanutils: apache-commons-beanutils: does not suppress the class property in PropertyUtilsBean by default.
- CVE-2019-16943: REST: jackson-databind: Serialization gadgets in classes of the p6spy package.
- CVE-2019-20445: JMS: netty: **HttpObjectDecoder.java** allows the content-length header to be accompanied by a second content-length header.
- CVE-2019-17531: REST: jackson-databind: Polymorphic typing issue when enabling default typing for an externally exposed JSON endpoint and having **apache-log4j-extra** in the classpath leads to code execution.
- CVE-2019-20444: JMS: netty: HTTP request smuggling.
- CVE-2019-14888: Web (Undertow): undertow: Possible Denial Of Service (DOS) in Undertow HTTP server listening on HTTPS.
- CVE-2019-12423: Web Services: cxf-core: cxf: OpenId Connect token service does not properly validate the clientId.
- CVE-2019-14887: Management: wildfly: The **enabled-protocols** value in legacy security is not respected if OpenSSL security provider is in use.
- CVE-2019-0210: MP OpenTracing: libthrift: thrift: Out-of-bounds read related to **TJSONProtocol** or **TSimpleJSONProtocol**.
- CVE-2019-16869: JMS: netty: HTTP request smuggling by mishandled whitespace before the colon in HTTP headers.
- CVE-2020-1732: Security: wildfly: Soteria: Security identity corruption across concurrent threads.
- CVE-2020-7238: JMS: netty: HTTP request smuggling due to Transfer-Encoding whitespace mishandling.
- CVE-2020-1695: REST: resteasy-jaxrs: resteasy: Improper validation of response header in **MediaTypeHeaderDelegate.java** class.
- CVE-2019-14893: REST: jackson-databind: Serialization gadgets in classes of the xalan package.
- CVE-2019-16335: REST: jackson-databind: Polymorphic typing issue related to **com.zaxxer.hikari.HikariDataSource**.
- CVE-2019-14892: REST: jackson-databind: Serialization gadgets in classes of the commons-configuration package.

- CVE-2019-10174: Clustering: infinispan-core: infinispan: The **invokeAccessibly** method from the **ReflectionUtil** class allows to invoke private methods.
- CVE-2019-17267: REST: jackson-databind: Serialization gadgets in classes of the ehcache package.
- CVE-2020-10688: REST: resteasy: RESTEASY003870 exception in RESTEasy can lead to a reflected XSS attack.
- CVE-2019-12419: Web Services: xf-core: cxf: OpenId Connect token service does not properly validate the clientId.
- CVE-2020-1745: Web (Undertow): undertow: AJP File Read/Inclusion Vulnerability.
- CVE-2019-0205: MP OpenTracing: libthrift: thrift: Endless loop when fed with specific input data.
- CVE-2019-17573: Web Services: cxf: Reflected XSS in the services listing page.

CHAPTER 6. KNOWN ISSUES

See Known Issues for JBoss EAP CD 19 to view the list of known issues for this release.

Revised on 2020-04-24 16:45:53 UTC