Red Hat Fuse 7.13

Release Notes for Red Hat Fuse 7.13

What's new in Red Hat Fuse

Last Updated: 2024-06-05

Red Hat Fuse 7.13 Release Notes for Red Hat Fuse 7.13

What's new in Red Hat Fuse

Legal Notice

Abstract

These notes provide an overview of the changes between Red Hat Fuse releases.

Table of Contents

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. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message.

CHAPTER 1. FUSE 7.13 PRODUCT OVERVIEW

1.1. FUSE DISTRIBUTIONS

Fuse 7.13 is provided in the form of two different distributions, as follows:

Fuse standalone

The classic distribution of Fuse, supported on multiple operating systems. This distribution is supported for the following container types:

- Apache Karaf
- JBoss Enterprise Application Platform (EAP)
- Spring Boot

Fuse on OpenShift

The distribution of Fuse for running integration applications on OpenShift (supported on the Red Hat Enterprise Linux operating system). In this case, the supported container types are provided in the form of docker-formatted container images:

- Java image (for Spring Boot)
- Apache Karaf image
- JBoss EAP image

1.2. SUPPORTED CONFIGURATIONS

IMPORTANT

For users running Fuse with Java 8 on Karaf, it is recommended to use OpenJDK 8u282 or OpenJDK 8u302. Do not use OpenJDK 8u292, which has a known issue affecting the credential store (see ENTESB-16417). OracleJDK 1.8.0_291 is also affected by this issue.

For information about supported configurations, standards, and components in version 7.13, see the following Customer Portal articles:

- Red Hat Fuse Supported Configurations
- Red Hat Fuse Supported Standards
- Red Hat Fuse Component Details

CHAPTER 2. FUSE ON OPENSHIFT

Fuse on OpenShift enables you to deploy Fuse applications on OpenShift Container Platform.

2.1. SUPPORTED VERSION OF OPENSHIFT

For details of the supported version (or versions) of OpenShift Container Platform to use with Fuse on OpenShift, see the Supported Configurations page.

2.2. SUPPORTED IMAGES

Fuse on OpenShift provides the following Docker-formatted images:

Image	Platform	Supported architectures
fuse7/fuse-java-openshift-rhel8	Spring Boot	AMD64 and Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk11-rhel8	Spring Boot	AMD64 and Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk17-rhel8	Spring Boot	AMD64 and Intel 64 (x86_64)
fuse7/fuse-java-openshift-openj9-11-rhel8	Spring Boot	IBM Z and LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-karaf-openshift-rhel8	Apache Karaf	AMD64 and Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk11-rhel8	Apache Karaf	AMD64 and Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk17-rhel8	Apache Karaf	AMD64 and Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk11-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 and Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk17-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 and Intel 64 (x86_64)
fuse7/fuse-console-rhel8	Fuse console	AMD64 and Intel 64 (x86_64) IBM Z and LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-console—rhel8-operator	Fuse console operator	AMD64 and Intel 64 (x86_64) IBM Z and LinuxONE (s390x) IBM Power Systems (ppc64le)

Image	Platform	Supported architectures
fuse7/fuse-apicurito-generator-rhel8	Apicurito REST application generator	AMD64 and Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8	Apicurito REST API editor	AMD64 and Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8-operator	API Designer Operator	AMD64 and Intel 64 (x86_64)

CHAPTER 3. FUSE STANDALONE

3.1. SUPPORTED CONTAINERS

Fuse standalone 7.13 is supported on the following runtime containers:

- Spring Boot 2 (standalone)
- Apache Karaf
- Red Hat JBoss Enterprise Application Platform (JBoss EAP)

3.2. TECHNOLOGY PREVIEW FEATURES

The following features of Fuse standalone are *Technology Preview* only and are not supported in Fuse 7.13:

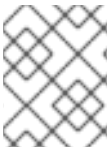
Saga EIP

The Saga Enterprise Integration Pattern (EIP) is a technology preview feature and features only the *In-Memory* Saga service (which is not suitable for a production environments). The LRA Saga service is *not* supported. For more details, see section Saga EIP of the "Apache Camel Development Guide".

3.2.1. Fuse Tooling support for Apache Camel

Fuse Tooling provides a cross-platform, cross-IDE approach to Camel application development, with Apache Camel language support extensions or plugins for Visual Studio Code, Eclipse IDE, and Eclipse Che.

Visual Studio Code features



NOTE

VS Code Apache Camel extensions are community features. They are not supported by Red Hat.

The Language Support for Apache Camel extension provides features for Camel URIs, such as the following:

For XML DSL and Java DSL:

- You can navigate to endpoints in the VS Code **Outline** panel and in the **Go > Go to Symbol in File** navigation panel.
- When you type, the editor provides code completion for Camel components, attributes, and the list of attribute values.
- When you hover over a Camel component, the editor shows a brief description of the component (from the Apache Camel component reference).
- As you edit the file, the editor performs an Apache Camel validation check on the Camel code.
- You can specify a specific Camel Catalog version by selecting **File → Preferences → Settings → Apache Camel Tooling → Camel catalog version**.

- You can use "Quick fix" features to address invalid enum values and unknown Camel URI component properties.

For XML DSL only:

- You can navigate to Camel contexts and routes in the VS Code **Outline** panel and in the **Go > Go to Symbol in File** navigation panel.
- When you type, the editor provides code completion for referenced IDs of **direct**, **direct VM**, **VM** and **SEDA** components.
- You can find references for **direct** and **direct VM** components in all open Camel files.

For Properties:

- Completion for Camel component property
- Diagnostic

To access the **Language Support for Apache Camel**features, you add one or more extensions.

The Apache Camel Extension Pack installs the following VS Code extensions:

- Language Support for Apache Camel
- OpenShift Connector
- Java Extension Pack
- Spring Boot extension pack
- Project initializer by Red Hat
- XML Language Support
- AtlasMap Data Transformation editor
- Didact Tutorial
- Tooling for Apache Camel K

Optionally, you can install the extensions individually.

For more details, see the following readme files:

- Readme for Apache Camel Extension Pack
- Readme for Apache Camel Language Server Protocol for Visual Studio Code
- Readme for AtlasMap Data Transformation editor

Eclipse IDE features

The **Language Support for Apache Camel**Eclipse plug-in provides the following features for Camel URIs:

In the generic Eclipse text editor for both XML DSL and Java DSL:

- When you type, the editor provides code completion for Camel components, attributes, and the list of attribute values.
- When you hover over a Camel component, the editor shows a brief description of the component (from the Apache Camel component reference).

To access the **Language Support for Apache Camel**features, you install the Eclipse plug-in from the Eclipse Marketplace. For more details, see the readme file for Apache Camel Language Server Protocol for Eclipse IDE.

Eclipse Che features

The **Language Support for Apache Camel**plugin for Eclipse Che 7 provides features for Camel URIs in XML DSL and Java DSL.

- When you type, the editor provides code completion for Camel components, attributes, and the list of attribute values.
- When you hover over a Camel component, the editor shows a brief description of the component (from the Apache Camel component reference).
- When you save the file, the editor performs an Apache Camel validation check on the Camel code.

To activate this plugin for Eclipse Che, you can use the "Apache Camel based on Spring Boot" stack or edit your workspace configuration.

3.3. BOM FILES FOR FUSE 7.13

To configure your Maven projects to use the supported Fuse 7.13 artifacts, use the BOM versions documented in this section.

3.3.1. BOM File for Fuse 7.13

To upgrade your Fuse standalone applications to use the 7.13 dependencies, edit the Maven **pom.xml** and change the versions of the BOMs and Maven plugins listed in the following table:

Table 3.1. Maven BOM and plugin versions for 7.13 using the BOM

Container Type	Maven BOM or Plugin Artifact groupId/artifactId	Version for Fuse 7.13
Spring Boot 2	**org.jboss.redhat-fuse/fuse-springboot-bom**	**7.13.0.fuse-7_13_0-00012-redhat-00001**
	org.jboss.redhat-fuse/spring-boot-maven-plugin	**7.13.0.fuse-7_13_0-00012-redhat-00001**
Apache Karaf	**org.jboss.redhat-fuse/fuse-karaf-bom**	**7.13.0.fuse-7_13_0-00012-redhat-00001**
	org.jboss.redhat-fuse/karaf-maven-plugin	**7.13.0.fuse-7_13_0-00012-redhat-00001**

Container Type	Maven BOM or Plugin Artifact groupId/artifactId	Version for Fuse 7.13
JBoss EAP	**org.jboss.redhat-fuse/fuse-eap-bom**	**7.13.0.fuse-7_13_0-00012-redhat-00001**

For more details about using the BOM, see the Migration Guide.

CHAPTER 4. DEPRECATED AND REMOVED FEATURES

If you need any assistance or have any questions about the upcoming changes in Fuse 7, contact support@redhat.com.

4.1. DEPRECATED

The following features are deprecated in Fuse 7.13 and may be removed in a future release:

NOTE

Fuse Online is removed in Fuse 7.13

Support for Karaf OSGi runtime and JBoss Enterprise Application Platform (EAP) is deprecated

support for the Karaf OSGi runtime and for JBoss Enterprise Application Platform (EAP) will stop when Fuse 7 moves out of support on June 30, 2024. Camel will no longer be supported on Karaf OSGi or JBoss EAP when Fuse 7 moves out of support.

OpenWire protocol is deprecated

Since Fuse 7.10, use of the OpenWire protocol (which could be used to connect AMQ Broker instances) is deprecated. Note that the OpenWire protocol is also deprecated in AMQ Broker since AMQ Broker version 7.9.0.

wsdl2rest tool is deprecated

Since Fuse 7.10, the **wsdl2rest** command line tool is deprecated. The WSDL 2 Camel Rest DSL extension for VS Code is also deprecated.

PHP, Python, and Ruby scripting languages are deprecated in Camel applications

The PHP, Python, and Ruby scripting languages are deprecated in Camel applications since Fuse 7.4 and will be removed in a future release. The Camel community has deprecated PHP, Python, and Ruby since Camel 2.19 (see CAMEL-10973). This applies to all Fuse containers types: Apache Karaf, JBoss EAP, and Spring Boot.

HP-UX OS is deprecated

The HP-UX operating system is deprecated since Fuse 7.2 and support for this operating system could be removed in a future release of Fuse. In particular, note that the JBoss EAP 7.2 container has already dropped support for HP-UX and, consequently, any future version of Fuse on JBoss EAP that runs on JBoss EAP 7.2 will *not* be supported on HP-UX.

Camel MQTT component is deprecated

The Camel MQTT component is deprecated in Fuse 7.0 and will be removed in a future release of Fuse. You can use the Camel Paho component instead, which supports the MQTT messaging protocol using the popular Eclipse Paho library.

Camel LevelDB component is deprecated on all operating systems except for Linux

Since Fuse 6.3, the Camel LevelDB (**camel-leveldb**) component is deprecated on all operating systems except for Red Hat Enterprise Linux. In the future, the Camel LevelDB component will be supported only on Red Hat Enterprise Linux.

BatchMessage class from the Camel SJMS component is deprecated

The BatchMessage class from the Camel SJMS component is deprecated in Fuse 7 (deprecated in Apache Camel since version 2.17) and may be removed from a future version of Apache Camel and Fuse.

4.2. REMOVED IN FUSE 7.11

Installation of Fuse Online on OCP 3.11

Installing Fuse online environment 7.13 on OCP 3.11 is not supported. The Fuse Online install script is completely removed for installing Fuse Online on OCP 3.11.

RSA/SHA-1 Ciphers Not Supported by Default by camel-ftp and camel-ssh

From Fuse 7.11, the **camel-ftp** and **camel-ssh** components will no longer support TLS with RSA/SHA-1 cipher by default. Other Camel components that depend on the JSch library may also be affected.
For more information, see this Red Hat Customer Portal Article .

4.3. REMOVED IN FUSE 7.10

fabric8-maven-plugin

The **fabric8-maven-plugin** has been completely removed from Fuse 7.10. We recommend that you use the **openshift-maven-plugin** instead for building and deploying Maven projects in Fuse on OpenShift. The plugin is maintained by Eclipse JKube, which provides extensive documentation for the plugin.

4.4. REMOVED IN FUSE 7.8

Spring Boot 1

Spring Boot 1 is no longer supported in Fuse 7.8. We recommend that you migrate your Spring Boot applications to Spring Boot 2, following the guidance in the Spring Boot 2.0 Migration Guide .

Camel K runtime in Fuse Online

Camel K runtime in Fuse Online (technology preview feature) is no longer supported in Fuse 7.8.

Camel XmlJson component has been removed in 7.8

The Camel XmlJson (**camel-xmljson**) component has been removed in Fuse 7.8.

4.5. REMOVED IN FUSE 7.5

The following features were removed in Fuse 7.5:

Support for integration with MS SQL Server 2014 has been dropped in 7.5

MS SQL Server 2014 is no longer tested and supported for integrations with Fuse 7.5. We recommend that you use one of the more recent versions of MS SQL Server instead – for example, MS SQL Server 2016 or 2017.

Camel LinkedIn component has been removed in 7.5

The **camel-linkedin** component has been removed in Fuse 7.5.

IMPORTANT

Although removed from Fuse 7.5, the **camel-linkedin** component is likely to be restored in a later release.

4.6. REMOVED IN FUSE 7.3

The following features were removed in Fuse 7.3:

Camel YQL component has been removed in 7.3

The Camel YQL component has been removed in Fuse 7.3.

OpenJPA and OpenJPA3 Karaf features have been removed in 7.3

The **openjpa** feature and the **openjpa3** feature have been removed from the Apache Karaf container in 7.3. For a Java Persistence Architecture (JPA) implementation, use the supported **hibernate** feature instead.

camel-jetty Karaf feature has been removed in 7.3

The **camel-jetty** feature has been removed from the Apache Karaf container in 7.3, because it uses Jetty 8. Use the **camel-jetty9** feature instead.

pax-jms-oracleaq Karaf feature has been removed in 7.3

The **pax-jms-oracleaq** feature has been removed from the Apache Karaf container in 7.3, because it requires 3rd party, non-free Oracle AQ libraries.

camel-elasticsearch component has been removed from Fuse on EAP (Wildfly Camel) in 7.3

The **camel-elasticsearch** component has been removed from Fuse on EAP (Wildfly Camel) in 7.3. Use the newer **camel-elasticsearch-rest** component instead.

4.7. REMOVED IN FUSE 7.2

The following features were removed in Fuse 7.2:

Camel XMLRPC component has been removed in 7.2

The Camel XMLRPC component has been removed in Fuse 7.2.

Camel Netty component has been removed in 7.2

The Camel Netty component has been removed in Fuse 7.2. It is recommended that you use the Camel Netty4 component instead.

4.8. REMOVED IN FUSE 7.0

The following features were removed in Fuse 7.0:

Support for Red Hat JBoss Operations Network (JON) has been removed in 7.0

Since Fuse 7.0, Fuse on Karaf no longer supports JON and no longer provides JON plugins for integrating with the JON runtime.

Embedded ActiveMQ broker has been removed in 7.0

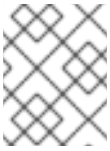
Since Fuse 7.0, Fuse on Karaf no longer provides an embedded ActiveMQ Broker. Customers should connect to a supported remote broker directly. For more information on our supported brokers, refer to the "Supported Messaging Providers" section of the Red Hat Fuse Supported Configurations page.

Fuse integration pack has been removed in 7.0

Support for running rules and processes is provided by components shipped with Red Hat JBoss BPM Suite and Red Hat JBoss BRMS.

Karaf console commands for child container administration have been removed in 7.0

Since Fuse 7.0, the Karaf console commands for child container administration are *not* supported. That is, the console commands prefixed by **instance:** (Karaf 4.x syntax) and the console commands prefixed by **admin:** (Karaf 2.x syntax) are not supported.



NOTE

In the Fuse 7.0 GA release, the **instance:** commands are not removed. This is a known issue.

SwitchYard has been removed in 7.0

Since Fuse 7.0, SwitchYard has been removed, and you should use Apache Camel directly instead. For more detailed information, see the knowledge base article, SwitchYard Support Plan After Releasing Fuse 7.

Support for Fabric8 1.x has been removed in 7.0

Since Fuse 7.0, Fabric8 v1 has been replaced by Fuse on OpenShift (previously, Fuse Integration Services), which includes components of Fabric8 v2 technology. Fuse on OpenShift provides a set of tools and Docker-formatted images that enable development, deployment, and management of integration microservices within OpenShift.
Although Fuse on OpenShift has a different architecture, it fulfills the same provisioning, automation, central configuration and management requirements that Fabric8 v1 provides. For more information, see Fuse on OpenShift Guide.

Camel components for Google App Engine have been removed in 7.0

The Camel components for Google App Engine (**camel-gae**) have been removed in Fuse 7.0.

Camel jBPM component has been removed in 7.0

The Camel jBPM component (**camel-jbpm**) has been removed in Fuse 7.0.

Tanuki based wrapper for installing Fuse as a service has been removed in 7.0

The Tanuki based wrapper scripts – generated using the **wrapper:install** Karaf console command – for installing Fuse as a service have been removed in Fuse 7.0. To install the Apache Karaf container as a service, it is recommended that you use the new **karaf-service-*.sh** scripts from the **bin/contrib** directory instead.

Smooks has been removed in 7.0

Since Fuse 7.0, the Smooks component for SwitchYard has been removed.

BPEL has been removed in 7.0

BPEL (based on the Riftsaw project) has been removed from Fuse 7.0. If you are currently using BPEL, it is recommended that you consider migrating to the Red Hat JBoss BPM Suite.

Design Time Governance has been removed in 7.0

The Design Time Governance component has been removed in 7.0.

Runtime Governance has been removed in 7.0

Since Fuse 7.0, the Runtime Governance (RTGov) component has been removed.

S-RAMP has been removed in 7.0

The SOA Repository Artifact Model and Protocol (S-RAMP) component has been removed in Fuse 7.0.

bin/patch script has been removed in 7.0

The **bin/patch** script (**bin\patch.bat** on Windows O/S) has been removed in a Fuse 7.0.

Spring Dynamic Modules (Spring-DM) is not supported in 7.0

Spring-DM (which integrates Spring XML with the OSGi service layer in Apache Karaf) is not supported in Fuse 7.0 and you should use the Blueprint framework instead. Using Blueprint XML does not prevent you from using the Java libraries from the Spring framework: the latest version of Spring is compatible with Blueprint.

Apache OpenJPA is not supported in 7.0

The Apache OpenJPA implementation of the Java Persistence API (JPA) is not supported in Fuse7.0. It is recommended that you use the Hibernate implementation instead.

4.9. REPLACED IN FUSE 7.0

The following features were replaced in Fuse 7.0:

Geronimo transaction manager has been replaced in 7.0

In Fuse 7.0, the Geronimo transaction manager in the Karaf container has been replaced by Narayana.

Jetty container has been replaced in 7.0

In Fuse 7.0, the Jetty container has been replaced by Undertow. Initially, this change applies only to internal use of the Jetty container (for example, in the Karaf container). Other Jetty components might be removed in a future release.

CHAPTER 5. UNSUPPORTED FEATURES IN FUSE 7.13

The following features are unsupported in Red Hat Fuse 7.13.

camel-leveldb component is not supported for Fuse on the IBM PowerPC and Z platforms

When Fuse is installed on the IBM PowerPC or IBM Z platforms, the Camel LevelDB component is not supported.

Installing Fuse Console using the Operator is not supported on OCP 3.11

Installing Fuse Console using the Operator is not supported and does not work on OpenShift Container Platform (OCP) 3.11. The recommended way to install Fuse Console on OCP 3.11 is to use templates.

Apache Karaf EclipseLink feature is unsupported

The Apache Karaf EclipseLink feature is **not** supported in Fuse, because this feature depends on JPA 2.2, while the Karaf container for Fuse 7.2 is aligned with JPA 2.1.

Apache Aries Blueprint Web module is unsupported

The Apache Aries Blueprint Web module is **not** supported in Fuse. The presence of an example featuring Blueprint Web in the community edition of Apache Camel (provided as a separate download) does **not** imply that this feature is supported in Fuse.

The PHP scripting language is not supported in Apache Camel on Apache Karaf

The PHP scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for PHP. The PHP scripting language is deprecated in Camel applications on the JBoss EAP container and on the Spring Boot container.

The Python scripting language is not supported in Apache Camel on Apache Karaf

The Python scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for Python. The Python scripting language is deprecated in Camel applications on the JBoss EAP container and on the Spring Boot container.

CHAPTER 6. KNOWN ISSUES

The following subsections describe the known issues in version 7.13.

6.1. CVE SECURITY VULNERABILITIES

As a middleware integration platform, Fuse can potentially be integrated with a large number of third-party components. It is not always possible to exclude the possibility that some third-party dependencies of Fuse could have security vulnerabilities. This section documents known common vulnerabilities and exposures (CVEs) related to security that affect third-party dependencies of Fuse 7.13.

CVE-2020-13936 **CVE-2020-13936 velocity: arbitrary code execution when attacker is able to modify templates**

An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.
Dependencies for Fuse 7.9 (and later) ensure that it uses only the fixed Velocity version (2.3) that protects against this security vulnerability. If your application code has any explicit dependencies on the Apache Velocity component, we recommend that you upgrade these dependencies to use the fixed version.

CVE-2018-10237 **CVE-2018-10237 guava: Unbounded memory allocation in AtomicDoubleArray and CompoundOrdering classes allow remote attackers to cause a denial of service [fuse-7.0.0]**

Google Guava versions 11.0 through 24.1 are vulnerable to unbounded memory allocation in the **AtomicDoubleArray** class (when serialized with Java serialization) and the **CompoundOrdering** class (when serialized with GWT serialization). An attacker could exploit applications that use Guava and deserialize untrusted data to cause a denial of service – for more details, see CVE-2018-10237.
To avoid this security vulnerability, we recommend that you:

- Never deserialize an **AtomicDoubleArray** instance or a **CompoundOrdering** instance from an unknown source.
- Avoid using Guava versions 24 and earlier (although in some cases it is not possible to avoid the earlier versions).

To make it easier to avoid the earlier (vulnerable) versions of Guava, Fuse 7.7 (and later) has configured its Maven Bill of Materials (BOM) files for all containers to select Guava 27 by default. This means that if you incorporate a Fuse BOM into your Maven project (by adding a dependency on the BOM to the **dependencyManagement** section of your POM file) and then specify a dependency on the Guava artifact *without* specifying an explicit version, the Guava version will default to the version specified in the BOM, which is version 27 for the Fuse 7.7 BOMs.

But there is at least one common use case involving the Apache Karaf (OSGi) container, where it is not possible to avoid using a vulnerable version of Guava: if your OSGi application uses Guava and Swagger together, you are obliged to use Guava 20, because that is the version required by Swagger. Here we explain why this is the case and how to configure your POM file to revert the earlier (vulnerable) Guava 20 library. First, you need to understand the concept of a *double OSGi chain*.

Double OSGi chain

Bundles in the OSGi runtime are *wired* together using package constraints (package name + optional version/range) – imports and exports. Each bundle can have multiple imports and usually those imports wire a given bundle with multiple bundles. For example:

```
BundleA
+-- BundleB
|   +-- BundleCa
+-- BundleCb
```

Where **BundleA** depends on **BundleB** and **BundleCb**, while **BundleB** depends on **BundleCa**. **BundleCa** and **BundleCb** should be the same bundle, if the export the same packages, but due to version (range) constraints, **BundleB** uses (*wires to*) a different revision/version of **BundleC** than **BundleA**.

Rewriting the preceding diagram to reflect what happens when you include dependencies on both Guava and Swagger in an application:

```
org.jboss.qe.cxf.rs.swagger-deployment
+-- Guava 27
+-- Swagger 1.5
   +-- reflections 0.9.11
      +-- Guava 20
```

If you try to deploy this bundle configuration, you get the error, **org.osgi.framework.BundleException: Uses constraint violation**.

Reverting to Guava 20

If your project uses both Guava and Swagger libraries (directly or indirectly), you should configure the **maven-bundle-plugin** to use an explicit version range (or no range at all) for the Guava bundle import, as follows:

```
<Import-Package>
   com.google.common.base;version="[20.0,21.0)",
   com.google.common.collect;version="[20.0,21.0)",
   com.google.common.io;version="[20.0,21.0)"
</Import-Package>
```

This configuration forces your OSGi application to revert to the (vulnerable) Guava 20 library. It is therefore particularly important to avoid deserializing **AtomicDoubleArray** instances in this case.

CVE-2017-12629 Solr/Lucene -security bypass to access sensitive data - CVE-2017-12629

Apache Solr is a popular open source search platform that uses the Apache Lucene search engine. If your application uses a combination of Apache Solr with Apache Lucene (for example, when using the Camel Solr component), it could be affected by this security vulnerability. Please consult the linked security advisory for more details of this vulnerability and the mitigation steps to take.

NOTE

The Fuse runtime does *not* use Apache Solr or Apache Lucene directly. The security risk only arises, if you are using Apache Solr and Apache Lucene together in the context of an integration application (for example, when using the Camel Solr component).

CVE-2021-30129 mina-sshd-core: Memory leak denial of service in Apache Mina SSHD Server

A vulnerability in sshd-core of Apache Mina SSHD allows an attacker to overflow the server causing an OutOfMemory error. This issue affects the SFTP and port forwarding features of Apache Mina SSHD version 2.0.0 and later versions. It was addressed in Apache Mina SSHD 2.7.0
This vulnerability in Apache Mina SSHD was addressed by SSHD-1004, which deprecates certain cryptographic algorithms that have this vulnerability. In Fuse 7.10 on Karaf and Fuse 7.10 on JBoss EAP, these deprecated algorithms are still supported (for reasons of backwards compatibility). However, if you are using one of these deprecated algorithms, it is strongly recommended that you refactor your application code to use a different algorithm instead.

In Fuse 7.10, the default cipher algorithms have changed as follows.

Fuse 7.9	Fuse 7.10	Deprecated in Fuse 7.10?
aes128-ctr	**aes128-ctr**	
	aes192-ctr	
	aes256-ctr	
	aes128-gcm@openssh.com	
	aes256-gcm@openssh.com	
arcfour128	**arcfour128**	yes
aes128-cbc	**aes128-cbc**	
	aes192-cbc	
	aes256-cbc	
3des-cbc	**3des-cbc**	yes
blowfish-cbc	**blowfish-cbc**	yes

In Fuse 7.10, the default key exchange algorithms have changed as follows.

Fuse 7.9	Fuse 7.10	deprecated in 7.10?
diffie-hellman-group-exchange-sha256	**diffie-hellman-group-exchange-sha256**	
ecdh-sha2-nistp521	**ecdh-sha2-nistp521**	
ecdh-sha2-nistp384	**ecdh-sha2-nistp384**	
ecdh-sha2-nistp256	**ecdh-sha2-nistp256**	

Fuse 7.9	Fuse 7.10	deprecated in 7.10?
	diffie-hellman-group18-sha512	
	diffie-hellman-group17-sha512	
	diffie-hellman-group16-sha512	
	diffie-hellman-group15-sha512	
	diffie-hellman-group14-sha256	
diffie-hellman-group-exchange-sha1	**diffie-hellman-group-exchange-sha1**	yes
diffie-hellman-group1-sha1	**diffie-hellman-group1-sha1**	yes

6.2. FUSE ON OPENSHIFT

This section lists issues that affect the deployment of Fuse applications on OpenShift. For details of issues affecting specific containers, see also the sections for Spring Boot, Fuse on Apache Karaf, and Fuse on JBoss EAP. The Fuse on OpenShift distribution has the following known issues:

ENTESB-21281 **Update FoO images with add-opens**

Without **add-opens** Fuse on Open Shift does not work properly with jdk17. These flags cannot be delivered automatically, so you have to specify them yourself, by adding the flags to a script that defines **add-opens**.
Since Java 17, the Java Platform Module System is *mandatory*. It implements strong encapsulation, which restricts access. You can use the **--add-opens** option to allow access, providing deep reflection, and allowing a specified module to open the named package.:

```
--add-opens module/package=target-module(,target-module)*
```

ENTESB-21281 **[Fuse on Openshift] QS karaf-cxf-rest - JavaDoc no longer supported on jdk17**

The **cxf java2wadl-plugin** in Red Hat FUSE 7.x doesn't work with JDK17.

ENTESB-17895 **[Fuse Console] Upgrade subscription does not update Hawtio**

In Fuse 7.10, if you update the Fuse Console by changing the Operator subscription channel to version 7.10, the Fuse Console remains on vesion 7.9. Even if the Fuse Console containers and pods have the label 7.10, they are still using the 7.9 images. To work around this problem, perform the upgrade by removing the older version of Fuse Console and then making a fresh installation of Fuse Console version 7.10.

ENTESB-17861 **Apicurito generator cannot generate Fuse Camel Project**

In Fuse 7.10, the API Designer (Apicurito) does not work properly, if it is installed via the Apicurito Operator (giving an Invalid Cert Error). To work around this problem:

1. Open a new tab to **https://apicurito-service-generator-apicurito.apps.cluster-name.openshift.com**
(Replace **cluster-name.openshift.com** with your cluster name.)

2. Accept the certificates.

3. Switch to the application and click on the generate button again.

ENTESB-17836 **[Fuse Console] A newly added route is not displayed in the Camel tree**

In Fuse 7.10, after deploying an application, the route (or routes) is not displayed in the Camel tree on the Fuse Console. You can work around this issue by refreshing the page, which should make the route appear.

ENTESB-19351 FIPS on OCP - Jolokia agent doesn't start due to unsupported security encoding

In Fuse 7.11, in OCP FIPS-enabled Jolokia agent becomes unavailable due to unsupported security encoding.

ENTESB-19352 FIPS on OCP - karaf-maven-plugin assembly goal fails to unsupported security provider

In Fuse 7.11, a binary stream deploy strategy fails on OCP FIPS enabled, with Karaf applications, if we use **karaf-maven-plugin** with assembly goal.

6.3. FUSE ON APACHE KARAF

Fuse on Apache Karaf has the following known issues:

ENTESB-16417 **Credential store is using PBEWithSHA1AndDESede by default**

The security API in OpenJDK 8u292 and in OracleJDK 1.8.0_291 returns an incomplete list of security providers, which causes the credential store in Apache Karaf to fail (because the required security provider appears to be unavailable). The underlying issue that causes this problem is https://bugs.openjdk.java.net/browse/JDK-8249906. We recommend that you use the earlier OpenJDK version, OpenJDK 8u282, or the later OpenJDK version, OpenJDK 8u302, which do not have this bug.

ENTESB-16526 **fuse-karaf on Windows cannot restart during patch:install**

While running **patch:install** in the Apache Karaf container on the Windows platform, under certain circumstances you might encounter the following error when the **patch:install** command attempts an automatic restart of the container:

```
Red Hat Fuse starting up. Press Enter to open the shell now...
100%
[==========================================================================]
Karaf started in 18s. Bundle stats: 235 active, 235 total
'.tmpdir' is not recognized as an internal or external command,
operable program or batch file.
There is a Root instance already running with name ~14 and pid ~13. If you know what you are doing and want to force the run anyway, SET CHECK_ROOT_INSTANCE_RUNNING=false and re run the command.
```

If you encounter this error, simply restart the Karaf container manually.

ENTESB-8140 **Start level of hot deploy bundles is 80 by default**

Starting in the Fuse 7.0 GA release, in the Apache Karaf container the start level of hot deployed bundles is 80 by default. This can cause problems for the hot deployed bundles, because there are many system bundles and features that have the same start level. To work around this problem and ensure that hot deployed bundles start reliably, edit the **etc/org.apache.felix.fileinstall-deploy.cfg** file and change the **felix.fileinstall.start.level** setting as follows:

```
felix.fileinstall.start.level = 90
```

ENTESB-7664 **Installing framework-security feature kills karaf**

The **framework-security** OSGi feature must be installed using the **--no-auto-refresh** option, otherwise this feature will shut down the Apache Karaf container. For example:

```
feature:install -v --no-auto-refresh framework-security
```

6.4. FUSE ON JBOSS EAP

Fuse on JBoss EAP has the following known issues:

ENTESB-21314 **[Fuse on EAP] Support jdk17 modularity**

Without **add-opens** Fuse on EAP does not work properly with jdk17. These flags cannot be delivered automatically, so you have to specify them yourself, by adding the flags to a script that defines **add-opens**.
Since Java 17, the Java Platform Module System is *mandatory*. It implements strong encapsulation, which restricts access. You can use the **--add-opens** option to allow access, providing deep reflection, and allowing a specified module to open the named package.:

```
--add-opens module/package=target-module(,target-module)*
```

ENTESB-20833 **java.security.acl.Group was removed for jdk17**

java.security.acl.Group is removed in versions jdk14 or later.

ENTESB-13168 **Camel deployment on EAP domain mode is not working on Windows**

Starting in Fuse 7.6.0, for Fuse on JBoss EAP, the Camel subsystem cannot be deployed on JBoss EAP in domain mode on Windows OS.

6.5. FUSE ON SPRING BOOT

Fuse on Spring Boot has the following known issues:

ENTESB-21315 **[Fuse on Spring-boot] Support jdk17 modularity**

Without **add-opens** Fuse does not work properly with jdk17. These flags cannot be delivered automatically, so you have to specify them yourself, by adding the flags to a script that defines **add-opens**.
Since Java 17, the Java Platform Module System is *mandatory*. It implements strong encapsulation, which restricts access. You can use the **--add-opens** option to allow access, providing deep reflection, and allowing a specified module to open the named package.:

```
--add-opens module/package=target-module(,target-module)*
```

ENTESB-21421 / *ENTESB-20842* **Spring Boot 2.6 does not allow circular dependencies**

Spring Boot 2.6 may be unable to resolve circular dependencies. If you use XML DSL in Spring Boot to instantiate a customized **HealthCheckRegistry** in your beans file, the build fails.
As a workaround, you can add the property **spring.main.allow-circular-references=true** to **application.properties**.

6.6. FUSE TOOLING

Fuse Tooling has the following known issues:

ENTESB-20965 **[Hawtio] Login failed due to: No LoginModules configured for hawtio-domain**

Hawtio can only work with the old security system with WildFly. If you attempt to login to Hawtio with Elytron security, the console displays the following error message.

```
11:30:21,039 WARN  [io.hawt.system.Authenticator] (default task-2) Login failed due to: No LoginModules configured for hawtio-domain
```

ENTESB-19668 **The Hawtio management console does not display a message on the UI when client certificate authentication is rejected**

The Hawtio component does not show any message on the login page, after rejecting authentication from a client certificate. Hawtio only redirects the web browser to the login page, without showing any message.

ENTESB-17705 **[Hawtio] Logout button disappears**

In Fuse 7.10, after logging in and logging out several times in a row, the **Logout** button is not shown. To work around this issue, you can refresh the page one or more times and the **Logout** button should reappear.

ENTESB-17839 **Fuse + AtlasMap: Unrecognized field "dataSourceType"**

In Fuse 7.11, if user wants to use AtlasMap vscode extension, then they must use version 0.0.9 as Fuse 7.11 is with AtlasMap 2.3.x. Otherwise use AtlasMap standalone 2.3.x but not the vscode-extension.

6.7. APACHE CAMEL

Apache Camel has the following known issues:

ENTESB-19361 / *UNDERTOW-2206* **Access logging support by cxf with embedded undertow server on karaf does not log URI**

If the **DECODE_URL** option is **true** (this is the default value for Fuse 7.11.1 karaf runtime), and use **HttpServerExchange** to decode **relativePath** and **requestPath**, the **requestURI** parameter remains encoded.
The dispatch methods (**forward, include**, **async** and **error**) assign the path without decoding it, for **requestPath** and **relativeURL**, which causes dispatching to a path such as **/some%20thing**.

ENTESB-15343 **XSLT component not working properly with IBM1.8 JDK**

In Fuse 7.8, the Camel XSLT component does not work properly with the IBM 1.8 JDK. The problem occurs because the underlying Apache Xerces implementation of XSLT does not support the **javax.xml.XMLConstants#FEATURE_SECURE_PROCESSING** property (see XERCESJ-1654).

ENTESB-11060 **[camel-linkedin] V1 API is no longer supported**

Since Fuse 7.4.0, the Camel LinkedIn component is no longer able to communicate with the LinkedIn

server, because it is implemented using the LinkedIn Version 1.0 API, which is no longer supported by LinkedIn. The Camel LinkedIn component will be updated to use the Version 2 API in a future release of Fuse.

ENTESB-7469 **Camel Docker component cannot use Unix socket connections on EAP**

Since Fuse 7.0, the **camel-docker** component can connect to Docker only through its REST API, not through UNIX sockets.

ENTESB-5231 **PHP script language does not work**

The PHP scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for PHP.

ENTESB-5232 **Python language does not work**

The Python scripting language is **not** supported in Camel applications on the Apache Karaf container, because there is no OSGi bundle available for Python.

ENTESB-2443 **Google Mail API - Sending of messages and drafts is not synchronous**

When you send a message or draft, the response contains a Message object with an ID. It may not be possible to immediately get this message via another call to the API. You may have to wait and retry the call.

ENTESB-2332 **Google Drive API JSON response for changes returns bad count of items for the first page**

Google Drive API JSON response for changes returns bad count of items for the first page. Setting **maxResults** for a list operation may not return all the results in the first page. You may have to go through several pages to get the complete list (that is by setting **pageToken** on new requests).

CHAPTER 7. FIXED ISSUES IN FUSE 7.13

The following sections list the issues that have been fixed in Fuse 7.13:

- Section 7.1, “Bugs resolved in Fuse 7.13”

7.1. BUGS RESOLVED IN FUSE 7.13

The following tables list the resolved bugs in Fuse 7.13.

Table 7.1. Fuse 7.13 Resolved Bugs

Issue	Description
ENTESB-22629	Fuse 7.12 blueprint properties not getting resolved
ENTESB-22511	infinispan-hibernate-cache-commons is not defined in fuse 7.12.1 bom
ENTESB-22498	Transaction rollback set in <doCatch> block does not work if "handled true" is set in the onException block
ENTESB-22490	Backport CAMEL-13092 for camel 2.x
ENTESB-22375	CAMEL-11750 was not completely implemented in Fuse
ENTESB-22272	Exception during Karaf start: java.lang.IllegalStateException: Resource has no uri
ENTESB-22175	Camel-openapi-java RestModelConverters.processSchema() ignores Swagger @Schema annotations
ENTESB-21958	camel-http4 HttpComponent logs a raw password unsafe characters
ENTESB-21878	NullPointerException when logging is at WARN level
ENTESB-21874	CamelBatchComplete is always true for PollEnrich File component
ENTESB-21858	Karaf won’t start when using JDK 11.0.20
ENTESB-21776	Fuse on Openshift image uses very old jmx_prometheus_javaagent.jar
ENTESB-21763	camel-http4 with toD does not work on Karaf
ENTESB-21757	[JDG-4351][JBMAR-235] camel-infinispan requires jboss-marshalling update from 2.0.9.Final to 2.0.11.Final onwards
ENTESB-21756	Improve logging of JSch library

Issue	Description
ENTESB-21752	Getting error "The dependencies of some of the beans in the application context form a cycle"
ENTESB-21742	New Fuse Console deployments don't work after yearly "openshift-service-serving-signer" certificate rotation
ENTESB-20503	Build fails with "-Dorg.slf4j.simpleLogger.defaultLogLevel=trace" option
ENTESB-22700	CVE-2024-22201 jetty: stop accepting new connections from valid clients [fuse-7]
ENTESB-22698	CVE-2024-22243 springframework: URL Parsing with Host Validation [fuse-7]
ENTESB-22514	CVE-2024-21733 tomcat: Leaking of unrelated request bodies in default error page [fuse-7]
ENTESB-22510	CVE-2023-46749 shiro: path traversal attack may lead to authentication bypass [fuse-7]
ENTESB-22509	CVE-2023-50290 solr: : Apache Solr: Host environment variables are published via the Metrics API [fuse-7]
ENTESB-22385	CVE-2023-6481 logback: A serialization vulnerability in logback receiver [fuse-7]
ENTESB-22384	CVE-2023-6378 logback: serialization vulnerability in logback receiver [fuse-7]
ENTESB-22381	CVE-2022-41678 activemq: Apache ActiveMQ: Deserialization vulnerability on Jolokia that allows authenticated users to perform RCE [fuse-7]
ENTESB-22379	CVE-2023-46589 tomcat: HTTP request smuggling via malformed trailer headers [fuse-7]
ENTESB-22376	CVE-2023-34055 spring-boot: org.springframework.boot:spring-boot-actuator class vulnerable to denial of service [fuse-7]
ENTESB-22373	CVE-2023-33202 bcpkix: bc-java: Out of memory while parsing ASN.1 crafted data in org.bouncycastle.openssl.PEMParser class [fuse-7]
ENTESB-22280	CVE-2023-5072 JSON-java: parser confusion leads to OOM [fuse-7]
ENTESB-22715	CVE-2024-22257 spring-security: Broken Access Control With Direct Use of AuthenticatedVoter [fuse-7]

Issue	Description
ENTESB-22712	CVE-2024-22259 springframework: URL Parsing with Host Validation [fuse-7]
ENTESB-22719	CVE-2024-28752 cxf-core: Apache CXF SSRF Vulnerability using the Aegis databinding [fuse-7]
ENTESB-22356	CVE-2023-36478 http2-hpack: jetty: hpack header values cause denial of service in http/2 [fuse-7]
ENTESB-22164	CVE-2023-39410 avro: apache-avro: Apache Avro Java SDK: Memory when deserializing untrusted data in Avro Java SDK [fuse-7]
ENTESB-22877	CVE-2024-30171 org.bouncycastle-bcprov-jdk18on: BouncyCastle vulnerable to a timing variant of Bleichenbacher (Marvin Attack) [fuse-7]
ENTESB-21854	CVE-2023-3223 undertow: OutOfMemoryError due to @MultipartConfig handling [fuse-7]
ENTESB-21956	CVE-2023-40167 jetty-http: jetty: Improper validation of HTTP/1 content-length [fuse-7]
ENTESB-21953	CVE-2023-36479 jetty-servlets: jetty: Improper addition of quotation marks to user inputs in CgiServlet [fuse-7]