Red Hat Fuse 7.12

Red Hat Fuse 7.12 发行注记

Red Hat Fuse 的新内容

Last Updated: 2023-12-27

Red Hat Fuse 7.12 Red Hat Fuse 7.12 发行注记

Red Hat Fuse 的新内容

法律通告

Copyright © 2023 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.

摘要

这些备注提供了 Red Hat Fuse 版本之间的变化概述。

目录

使开源包含更多 4

第 1 章 FUSE 7.12 产品概述 5
1.1. FUSE 分发 5
1.2. 重要备注 5
1.3. 支持的配置 6

第 2 章 FUSE ONLINE 7
2.1. 关于 FUSE 在线发行版本 7
2.2. 从 FUSE ONLINE 7.11.X 升级到 7.12.X 需要手动升级步骤 7
2.3. 升级 FUSE 在线集成 8
2.4. FUSE ONLINE 的重要备注 8
2.5. 获取 FUSE ONLINE 的技术支持 13
2.6. FUSE ONLINE 中的技术预览功能 13

第 3 章 OPENSHIFT 上的 FUSE 15
3.1. 支持的 OPENSHIFT 版本 15
3.2. 支持的镜像 15
3.3. OPENSHIFT 上的 FUSE 7.12 的新功能 16
3.4. 重要备注 17

第 4 章 FUSE STANDALONE 19
4.1. 支持的容器 19
4.2. FUSE 7.12 中的新功能 19
4.3. 技术预览功能 19
4.4. FUSE 7.12 的 BOM 文件 23
4.5. 重要备注 24

第 5 章 弃用和删除的功能 26
5.1. 已弃用 26
5.2. 在 FUSE 7.11 中删除 27
5.3. 在 FUSE 7.10 中删除 27
5.4. 在 FUSE 7.8 中删除 27
5.5. 在 FUSE 7.5 中删除 28
5.6. 在 FUSE 7.3 中删除 28
5.7. 在 FUSE 7.2 中删除 29
5.8. 在 FUSE 7.0 中删除 29
5.9. 在 FUSE 7.0 中替换 31

第 6 章 FUSE 7.12 中不支持的功能 32

第 7 章 已知问题 33
7.1. CVE 安全漏洞 33
7.2. FUSE ONLINE 37
7.3. OPENSHIFT 上的 FUSE 37
7.4. APACHE KARAF 上的 FUSE 39
7.5. JBOSS EAP 上的 FUSE 40
7.6. SPRING BOOT 上的 FUSE 40
7.7. FUSE 工具 41
7.8. APACHE CAMEL 42

第 8 章 修复了 FUSE 7.12 中的问题 44
8.1. FUSE 7.12 中的增强 44

8.2. FUSE 7.12 中的组件升级 44
8.3. 在 FUSE 7.12 中解决的错误 45
8.4. FUSE 7.12.1 中解决的错误 51

使开源包含更多

红帽致力于替换我们的代码、文档和 Web 属性中存在问题的语言。我们从这四个术语开始：master、slave、黑名单和白名单。由于此项工作十分艰巨，这些更改将在即将推出的几个发行版本中逐步实施。详情请查看我们的 CTO Chris Wright 信息。

第 1 章 FUSE 7.12 产品概述

1.1. FUSE 分发

Fuse 7.12 以三种不同的发行版的形式提供，如下所示：

Fuse 独立

在多个操作系统上支持的 Fuse 的经典分发。以下容器类型支持以下发行版本：

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

OpenShift 上的 Fuse

在 OpenShift 上运行集成应用程序的 Fuse 发行版（在 Red Hat Enterprise Linux 操作系统上支持）。在这种情况下，支持的容器类型以 docker 格式的容器镜像的形式提供：

- Java 镜像（用于 Spring Boot）
- Apache Karaf 镜像
- JBoss EAP 镜像

Fuse Online

使用基于浏览器的 UI 访问简化的工作流，适用于非专家集成的 Fuse 发行版。此发行版可用于以下类型的部署：

- 在 OpenShift Dedicated (OSD)集群中。
- 用于在内部 OpenShift 集群上安装

1.2. 重要备注

从 JUnit 4 升级到 JUnit5

Red Hat Fuse 7.12 使用 Spring Boot 2.7.x，它将 JUnit 4 升级到 JUnit 5。使用 Fuse Spring Boot BOM 7.12 的所有项目都依赖于 JUnit 5。从 Fuse 7.x 迁移到 Fuse 7.12 的客户可能会发现，在 Spring Boot 上运行的单元测试不再作为 Maven 构建的一部分执行。要解决这个问题，将相关的依赖项添加到 **maven-surefire-plugin** 配置，如下所示。

```
<plugin>
  <groupId>org.apache.maven.plugins</groupId>
  <artifactId>maven-surefire-plugin</artifactId>
  <version>${maven-surefire-plugin.version}</version>
  <configuration>
    <testFailureIgnore>true</testFailureIgnore>
  </configuration>
  <dependencies>
    <dependency>
      <groupId>org.apache.maven.surefire</groupId>
      <artifactId>surefire-junit47</artifactId>
```

```
      <version>${maven-surefire-plugin.version}</version>
    </dependency>
  </dependencies>
</plugin>
```

有关从 JUnit4 迁移的更多信息，请参阅从 JUnit 4 迁移。

CVE-2020-8908 guava

30.0 之前的 Guava 版本中存在临时目录创建漏洞。我们建议将 Guava 更新至 30.0 或更高版本，或更新到 Java 7 或更高版本，或者在创建目录后显式更改权限（如果不可能）。

为 sunset 调度 Red Hat CodeReady studio

为 sunset 调度 Red Hat CodeReady studio。JBoss 工具（社区）是成功的工具包。

1.3. 支持的配置

重要

要在 Apache Karaf 中运行 Fuse，我们推荐使用 OpenJDK 8u282 或 OpenJDK 8u302。不要使用 OpenJDK 8u292，它有一个影响凭证存储的已知问题（请参阅 ENTESB-16417）。OracleJDK 1.8.0_291 也会受到此问题的影响。

有关版本 7.12 中支持的配置、标准和组件的详情，请查看以下客户门户网站文章：

- Red Hat Fuse 支持的配置
- Red Hat Fuse 支持的标准
- Red Hat Fuse 组件详情

第 2 章 FUSE ONLINE

Fuse Online 提供了一个 Web 浏览器界面，让企业专家能够在不编写代码的情况下集成两个或多个不同应用程序或服务。它还提供一些功能，允许在复杂用例需要时添加代码。

Fuse Online 在 OpenShift 上作为使用 Apache Camel 的 Spring Boot 应用程序运行集成。

2.1. 关于 FUSE 在线发行版本

Fuse Online 是红帽基于 Web 的集成平台。Syndesis 是 Fuse Online 的开源项目。Fuse Online 在这些 OpenShift 环境中运行：

主机环境	安装
OpenShift Dedicated	红帽在红帽基础架构上安装并调配 Fuse Online。
OpenShift Container Platform	客户安装和管理。

2.2. 从 FUSE ONLINE 7.11.X 升级到 7.12.X 需要手动升级步骤

如果您安装了 Fuse Online 7.11.x 并希望升级到 Fuse Online 7.12.x.x，您必须手动升级到 Fuse Online 7.12.x.0。

1. 在 OpenShift Container Platform Web 控制台的 **Administrator** 视角中，进入到 **Operators** > **Installed Operators**。
2. 点 **Red Hat Integration Fuse Online 7.11.2** Operator。
3. 点 **Subscription** 标签页。
4. 验证 **Update approval** 是否已设置为 **Manual** ：
   - 如果 **Update approval** 设为 **Manual**，则跳至下一步。
   - 如果 **Update approval** 设置为 **Automatic** ：
     a. 单击 **Automatic**。
     b. 在 **Change Update Approval Strategy** 对话框中，选择 **Manual** 并点 **Save**。
5. 在 **Update channel** 下，单击 **7.11.2**。
6. 对于 **Change subscription 更新频道**，请选择 **7.12.x**。
   注： 最新的、candidate 和 **stable** 频道是技术预览功能。
7. 在 **Upgrade status** 下，单击 **Upgrade available**。
8. 点 **Preview InstallPlan**，然后点 **Approve**。
9. 验证 Operator 是否已完成到 Fuse Online 7.12.0 的升级：
   a. 进入到 **Operators** > **Installed Operators** 页面，然后点 **Red Hat Integration Fuse Online**。**Operator Details** 页面将打开。

b. 选择 **Syndesis** 选项卡。Fuse Online 实例的状态（默认名称为 **app**）最初显示 **Installed**（以指示安装了 Fuse Online 7.12.0）。然后，它将分为几个阶段(**安装**、**启动** 和 **Installed**)。当它再次到达 **Installed** 阶段时，升级到 7.12.0 已完成。

10. 返回到 Operators > **Installed Operators** 页面，然后点 **Red Hat Integration Fuse Online** operator 的 **Upgrade available**。

11. 点 **Preview InstallPlan**，然后点 **Approve**。

12. 验证 Operator 是否已完成到 Fuse Online 7.12.x 的升级：

    a. 导航到 **Networking** > **Routes** 并点击 **syndesis** 的位置链接来打开 Fuse Online web 控制台。

    b. 在 Fuse Online 控制台右上角，单击 **?** 图标，然后选择 **About**。

    c. 验证 **About** 页面是否在版本号中包含 **7_12_x**。

2.3. 升级 FUSE 在线集成

要升级在 OCP 现场运行的 Fuse Online 环境，您必须使用操作器更新 Fuse Online，然后重新发布任何正在运行的集成，如升级 Fuse Online 所述。

在 OCP 4.9 或更高版本中，当您使用 operator 升级到 7.11 时，Fuse Online Operator 升级过程中会显示以下警告：

W1219 18:38:58.064578 1 warning.go:70] extensions/v1beta1 Ingress 在 v1.14+ 中弃用，在 v1.22+ 中不可用；使用 networking.k8s.io/v1 Ingress

出现这个警告的原因是，客户端（用于 Kubernetes/OpenShift API 初始化代码的 Fuse Online 使用）访问已弃用的 Ingress 版本。这个警告 *不是* 使用已弃用 API 的指示器，且没有升级到 Fuse Online 7.11 的问题。

2.4. FUSE ONLINE 的重要备注

Fuse Online 发行版的 Fuse 7.12 版本的重要备注：

- 对 Fuse Online 的支持现已弃用，因为 Fuse 7 现在处于维护支持中。Fuse 7 结束支持时，不会有任何用于 Fuse Online 的开发。
- OCP 3.11 不再支持安装 Fuse Online。
- Fuse Online 不再支持 Camel K 运行时或 KNative 连接器。
- 当在红帽基础架构上安装和配置 Fuse Online 时，该帐户仅限于一次可以运行的特定数量集成。详情请查看定价计划。
- 上传到 Fuse Online 的 OpenAPI 模式可能无法定义输入/输出类型。当 Fuse Online 从 OpenAPI 模式创建自定义 API 客户端时，它没有指定输入/输出类型，则无法创建集成数据将集成数据映射到 API 客户端处理的字段或来自 API 客户端处理的字段。如果集成需要数据映射到自定义 API，那么当您上传 OpenAPI 模式时，点 **Review/Edit** 以打开 API Designer，它是一个 API 编辑工具，并添加输入/输出类型规格。
- 自 Fuse 7.8 起，用于自定义 API 客户端连接器或 API 供应商集成的 OpenAPI 文档不能具有 cyclic 模式引用。例如，指定请求或响应正文的 JSON 模式无法作为整体引用，也无法通过任意数量的中间模式引用其自身的任何部分。

- 在 OCP 4.9 （或更新版本）上，**application-monitoring** 项目不再有效。监控 Fuse 在线集成和基础架构组件与 Prometheus 和 Grafana 的先决条件。
  要临时解决这个问题，您可以使用 内置的监控堆栈（在 **openshift-monitoring** 命名空间中）使用 **openshift-user-workload-monitoring** 功能和 **grafana-operator** 来使用 **ops addon**，如以下在 *OCP 4.9 （或稍后的）上添加 Fuse Online 监控资源(Prometheus 和 Grafana)* 所述。

2.4.1. 在 OCP 4.9 （或更新版本）中添加 Fuse Online 监控资源(Prometheus 和 Grafana)

先决条件

- Fuse Online 在 OCP 4.9 （或更新版本）上安装并运行。
- 已安装 **oc** 客户端工具，并连接到安装了 Fuse Online 的 OCP 集群。
- 有 OCP 集群的 **admin** 访问权限。
- 您的 Fuse 在线安装启用了 **ops addon**。如果需要，您可以使用以下命令启用它：

```
oc patch syndesis/app --type=merge -p '{"spec": {"addons": {"ops": {"enabled": true}}}}'
```

步骤

1. 如果有现有的 **openshift-monitoring** 配置，请跳至第 2 步。
   否则，创建一个 **openshift-monitoring** 配置，将用户工作负载监控选项设置为 **true**，然后跳至第 3 步：

```
oc apply -f - <<EOF
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml:
    enableUserWorkload: true
EOF
```

2. 如果存在现有的 **openshift-monitoring** 配置：

   a. 检查现有的 **openshift-monitoring** 配置，以确定 **用户工作负载监控** 选项是否设置为 **true** ：

```
oc get -n openshift-monitoring cm/cluster-monitoring-config -
ojsonpath='{.data.config\.yaml}'
```

   如果结果为 **enableUserWorkload: true**，则用户工作负载监控选项设置为 **true**。**跳至第 3 步。**

   如果结果显示任何其他配置，请继续下一步，以便通过编辑 ConfigMap 来启用用户工作负载的监控。

   b. **在编辑器中打开 ConfigMap 文件，例如：**

```
oc -n openshift-monitoring edit cm/cluster-monitoring-config
```

c. 将 enableUserWorkload 设置为 true。例如：

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml:
   enableUserWorkload: true
```

d. 保存 ConfigMap 文件。

3. 使用以下命令监控 openshift-user-workload-monitoring 命名空间中的 pod 状态：

```
oc -n openshift-user-workload-monitoring get pods -w
```

等待 pod 的状态为 Running，例如：

```
prometheus-operator-5d989f48fd-2qbzd   2/2     Running
prometheus-user-workload-0             5/5     Running   prometheus-user-workload-1
5/5     Running
thanos-ruler-user-workload-0           3/3     Running
thanos-ruler-user-workload-1           3/3     Running
```

4. 验证 Prometheus 中是否启用了 Fuse Online 警报规则：

a. 访问内部 prometheus 实例

```
oc port-forward -n openshift-user-workload-monitoring pod/prometheus-user-workload-0
9090
```

b. 打开浏览器到 localhost:9090

c. 选择 Status> Targets。您应该会看到三个 复合 端点。

d. 按 CTRL-C 终止 端口转发 进程。

5. 在 OperatorHub 中，将 Grafana Operator 4.1.0 安装到您选择的命名空间，例如 grafana-middleware 命名空间。

6. 添加集群角色和集群角色绑定，以允许 grafana-operator 列出节点和命名空间：

a. 从 grafana-operator 网站下载集群角色 YAML 文件：

```
curl https://raw.githubusercontent.com/grafana-operator/grafana-
operator/master/deploy/cluster_roles/cluster_role_grafana_operator.yaml >
tmp_role.yaml
```

b. 为 grafana-operator 添加集群权限以读取其他命名空间和节点：

```
cat <<EOF >> tmp_role.yaml
  - apiGroups:
      - ""
    resources:
```

```
    - namespaces
    - nodes
  verbs:
    - get
    - list
    - watch
EOF
```

```
oc apply -f tmp_role.yaml
```

```
oc apply -f - <<EOF
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: grafana-operator
roleRef:
  name: grafana-operator
  kind: ClusterRole
  apiGroup: ""
subjects:
  - kind: ServiceAccount
    name: grafana-operator-controller-manager
    namespace: grafana-middleware
EOF
```

7. **使用 DASHBOARD_NAMESPACES_ALL 环境变量从其他命名空间中读取 Grafana 仪表板，以限制命名空间：**

```
oc -n grafana-middleware patch subs/grafana-operator --type=merge -p '{"spec":{"config":
{"env":[{"name":"DASHBOARD_NAMESPACES_ALL","value":"true"}]}}}'
```

8. **检查 grafana pod 是否已重新创建：**

```
oc -n grafana-middleware get pods -w
```

9. **另外，还可查看 grafana-operator 日志：**

```
oc -n grafana-middleware logs -f `oc -n grafana-middleware get pods -oname|grep grafana-
operator-controller-manager` -c manager
```

10. **添加 Grafana 自定义资源 以启动 Grafana 服务器 pod，例如：**

```
oc apply -f - <<EOF
apiVersion: integreatly.org/v1alpha1
kind: Grafana
metadata:
```

```
  name: grafana-middleware
  namespace: grafana-middleware
spec:
  config:
    auth:
      disable_signout_menu: true
    auth.anonymous:
      enabled: true
    log:
      level: warn
      mode: console
    security:
      admin_password: secret
      admin_user: root
  dashboardLabelSelector:
  - matchExpressions:
    - key: app
      operator: In
      values:
      - grafana
      - syndesis
  ingress:
    enabled: true
EOF
```

11. **允许 grafana-operator 读取监控信息：**

```
oc -n grafana-middleware adm policy add-cluster-role-to-user cluster-monitoring-view -z
grafana-serviceaccount
```

12. **添加 GrafanaDatasource 以查询 thanos-querier ：**

```
oc apply -f - <<EOF
apiVersion: integreatly.org/v1alpha1
kind: GrafanaDataSource
metadata:
  name: prometheus-grafanadatasource
  namespace: grafana-middleware
spec:
  datasources:
    - access: proxy
      editable: true
      isDefault: true
      jsonData:
        httpHeaderName1: 'Authorization'
        timeInterval: 5s
        tlsSkipVerify: true
      name: Prometheus
      secureJsonData:
      httpHeaderValue1: "Bearer $(oc -n grafana-middleware serviceaccounts get-token
grafana-serviceaccount)"
```

```
      type: prometheus
      url: "https://$(oc get route thanos-querier -n openshift-monitoring -
ojsonpath='{.spec.host}')"
  name: prometheus-grafanadatasource.yaml
EOF
```

13. 查看 **grafana** 服务器日志：

```
oc logs -f `oc get pods -l app=grafana -oname`
```

14. 访问 **grafana URL** 并查看 **Fuse** 在线仪表板：

```
echo "https://"$(oc -n grafana-middleware get route/grafana-route -ojsonpath='{.spec.host}')
```

2.5. 获取 FUSE ONLINE 的技术支持

要获得技术支持，请在 Fuse 在线控制台中，在左侧导航面板中点 Support。使用 Support 页面下载所有集成或您选择的一个或多个集成的诊断信息。该页面还提供打开支持问题单的链接，并提供您下载的诊断信息。

2.6. FUSE ONLINE 中的技术预览功能

此发行版本包括以下列出的技术预览功能。

重要

红帽产品服务级别协议(SLA)不支持技术预览功能，且其功能可能并不完善，红帽不建议在生产环境中使用它们。这些技术预览功能可以使用户提早试用新的功能，并有机会在开发阶段提供反馈意见。如需更多信息，请参阅红帽技术预览功能支持范围。

- **Fuse** 在线审计

  Fuse Online 支持对以下 **Fuse** 在线组件的任何用户所做的更改进行的基本审核：

  - **Connection - Fuse Online Web** 控制台的连接器 **Details** 页面中显示的 **Name** 和任何其他字段。

- 连接器 - Name 字段。
- 集成 - Name 字段。

- 用于映射数据字段的条件表达式

在数据映射程序中，您可以指定一个条件表达式并将其应用到数据映射。例如，一个条件表达式可以指定 source 字段的评估，以及如何填充 target 字段（如果 source 字段为空）。您可以指定的一组有限表达式与 Microsoft Excel 表达式类似。

- 数据映射程序中用户定义的属性的文档范围

在数据映射程序中，您可以指定您为源和目标映射定义的属性的范围。在 Mapping Details 面板中，单击 Properties 旁边的 Add (+)。在 Create Property 对话框中，用于新的 Scope 选项，您可以选择当前消息标头、上一步中的消息标头，或 Camel Exchange Property for Camel 特定属性。

- 对于使用 OAuth 的 REST API 客户端，当您创建 API 客户端连接器时，您可以更改您从该连接器创建的连接的默认 OAuth2 行为。对 OpenAPI 规格的 Fuse 在线供应商扩展支持以下内容：
  - 将客户端凭据作为参数提供。
  - 根据 HTTP 响应状态代码获取新的访问令牌。

第 3 章 OPENSHIFT 上的 FUSE

OpenShift 上的 Fuse 可让您在 OpenShift Container Platform 上部署 Fuse 应用程序。

3.1. 支持的 OPENSHIFT 版本

有关 OpenShift 上 Fuse 支持的 OpenShift Container Platform 版本（或版本）的详情，请查看 支持的配置页面。

3.2. 支持的镜像

OpenShift 上的 Fuse 提供以下 Docker 格式的镜像：

Image	平台	支持的构架
fuse7/fuse-java-openshift-rhel8	Spring Boot	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk11-rhel8	Spring Boot	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk17-rhel8	Spring Boot	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-java-openshift-openj9-11-rhel8	Spring Boot	IBM Z 和 LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-karaf-openshift-rhel8	Apache Karaf	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk11-rhel8	Apache Karaf	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk17-rhel8	Apache Karaf	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk8-rhel7	Red Hat JBoss Enterprise Application Platform	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk11-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 和 Intel 64 (x86_64)

Image	平台	支持的构架
fuse7/fuse-eap-openshift-jdk17-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-console-rhel8	Fuse 控制台	AMD64 和 Intel 64 (x86_64) IBM Z 和 LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-console—rhel8-operator	Fuse console operator	AMD64 和 Intel 64 (x86_64) IBM Z 和 LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-apicurito-generator-rhel8	Apicurito REST 应用生成器	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8	Apicurito REST API 编辑器	AMD64 和 Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8-operator	API Designer Operator	AMD64 和 Intel 64 (x86_64)

3.3. OPENSHIFT 上的 FUSE 7.12 的新功能

OpenShift 上的 Fuse 在版本 7.12 中提供以下新功能：

- **对 JDK 17 的支持**

  Fuse 7.12 支持使用 JDK 17 在 OpenShift 快速入门上构建 Fuse。

- **使用 openshift-maven-plugin运行快速入门**

  在使用 Maven archtypes 构建并运行 Fuse 时，Fuse 7.12 使用 openshift-maven-plugin。

- **支持 IBM Power 系统、IBM Z 和 LinuxONE**

  Fuse 7.12 添加了对 Red Hat OpenShift Container Platform 4.10 及之后的版本上的 IBM Power Systems (ppc64le)、IBM Z 和 LinuxONE (s390x)的支持。

注意

在 Fuse 7.12 中，不支持在 IBM Power Systems、IBM Z 和 LinuxONE 上的 OpenShift 镜像流和模板上安装 Fuse。IBM Power Systems、IBM Z 和 LinuxONE 仅支持在 OpenShift Operator 上使用 Fuse 安装的组件。

3.4. 重要备注

在 OpenShift 发行版上 Fuse 的 Fuse 7.12 版本的重要备注：

支持 OpenShift Container Platform (OCP) 4.11 或更高版本的 Fuse 7.12

Fuse 7.12 包含相应的更新，使其可用于 OpenShift Container Platform (OCP) 4.11 或更高版本。如果您计划升级到 OCP 4.11，则必须将 Fuse 升级到 7.12，然后才能将 OCP 升级到 4.11。早期版本的 Fuse (prior 到 7.10)不支持 OCP 4.9 或更高版本。

Data Virtualization 已被删除

从 Fuse 7.7 开始，数据虚拟化已被弃用，已从 Fuse 7.8 中删除。

Spring Boot 1 已被删除

从 Fuse 7.7 开始，Spring Boot 1 已被弃用，已从 Fuse 7.8 中删除。建议您按照 Spring Boot 2.0 迁移指南中的指导将 Spring Boot 应用程序迁移到 Spring Boot 2。

Fabric8 Maven 插件已被删除

Fabric8 Maven 插件从 Fuse 7.10 完全删除，并替换为自 Fuse 7.10 起的 OpenShift Maven 插件。使用 OpenShift Maven 插件构建和部署应用程序。

使用 JDK11 运行快速入门

如果要在运行时使用基于 JDK11 的镜像，请在编译时使用正确的 JDK11 配置集。使用 JDK11 构建和部署快速入门时，请确保已在构建机器上安装 JDK11，然后使用正确的 JDK11 配置集构建快速入门。

spring-boot 工件 Id 中的更改

在 Fuse 7.12 中，Spring Boot 升级到 2.7.12。

spring-Boot RHOSAK 因 spring-boot 升级而失败

eap-camel-jpa quickstart 已被删除

由于依赖项存在问题，eap-camel-jpa Quickstart 已从 Fuse 7.8 中删除。

自 Fuse 7.8 起，无法从外部访问 Jolokia

从 Fuse 7.8 开始，Jolokia 默认协议从 HTTP 切换到 HTTPS。

启用 FIPS 的 Jolokia 代理不可用

在启用了 OCP FIPS 的 Jolokia 代理中，因为不支持的安全编码而不可用。

第 4 章 FUSE STANDALONE

4.1. 支持的容器

以下运行时容器支持 Fuse 独立 7.12：

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

4.2. FUSE 7.12 中的新功能

在版本 7.12 中 Fuse 独立的主要新功能是：

支持 Java 17

Fuse 7.12 发行版本支持 Java 17、Java 11 和 Java 8。

4.3. 技术预览功能

Fuse 独立的以下功能 *只是技术预览*，在 Fuse 7.12 中不支持：

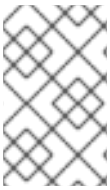
saga EIP

Saga Enterprise Integration Pattern (EIP)是一个技术预览功能，仅具有 *In-Memory* Saga 服务（不适用于生产环境）。不支持 LRA Saga 服务。*如需了解更多详细信息，请参阅"Apache Camel 开发指南"中的 Saga EIP 部分。*

4.3.1. Fuse Tooling 支持 Apache Camel

Fuse 工具为 Camel 应用程序开发提供了跨平台、跨 IDE 方法，支持 Visual Studio Code、Eclipse IDE 和 Eclipse Che 的 Apache Camel 语言支持扩展或插件。

Visual Studio Code 功能



注意

VS Code Apache Camel 扩展是社区功能。红帽不支持它们。

Apache Camel 扩展的语言支持为 Camel URI 提供功能，如下所示：

对于 XML DSL 和 Java DSL：

- *您可以在 VS Code outline 面板中导航到端点，并在 Go &gt ; Go to Symbol in File 导航面板中进入端点。*
- *当您输入时，编辑器为 Camel 组件、属性和属性值列表提供代码完成。*
- *将鼠标悬停在 Camel 组件上时，编辑器显示组件的简短描述（来自 Apache Camel 组件参考）。*
- *编辑文件时，编辑器对 Camel 代码执行 Apache Camel 验证检查。*
- *您可以选择 File → Preferences → Settings → Apache Camel Tooling → Camel catalog version 来指定特定的 Camel Catalog 版本。*
- *您可以使用 "Quick fix" 功能来处理无效的 enum 值和未知 Camel URI 组件属性。*

仅限 XML DSL：

- *您可以在 VS Code outline 面板中导航到 Camel 上下文和路由，并在 File 导航面板中的 Go &gt ; Go to Symbol 中 进入 Camel 上下文和路由。*

- 当您输入时，编辑器为直接 **ID**、 直接 虚拟机 、虚拟机和 **SEDA** 组件提供代码完成。
- 您可以在所有打开的 **Camel** 文件中找到 直接 和直接 虚拟机 组件的引用。

对于属性：

- **Camel** 组件属性的完成
- 诊断

要访问 **Apache Camel** 功能的语言支持，您可以添加一个或多个扩展。

Apache Camel 扩展包安装 以下 **VS Code** 扩展：

- **Apache Camel** 的语言支持
- **OpenShift Connector**
- **Java** 扩展包
- **Spring Boot** 扩展软件包
- 红帽项目初始化器
- **XML** 语言支持
- **AtlasMap Data Transformation** 编辑器

- Didact 教程
- Apache Camel K 工具

另外，您可以单独安装扩展。

如需了解更多详细信息，请参阅以下 readme 文件：

- Apache Camel 扩展包的 README
- Visual Studio Code 的 Apache Camel 语言服务器协议的 README
- README for AtlasMap Data Transformation 编辑器

Eclipse IDE 功能

Apache Camel Eclipse 插件的语言支持为 Camel URI 提供以下功能：

在 XML DSL 和 Java DSL 的通用 Eclipse 文本编辑器中：

- 当您输入时，编辑器为 Camel 组件、属性和属性值列表提供代码完成。
- 将鼠标悬停在 Camel 组件上时，编辑器显示组件的简短描述（来自 Apache Camel 组件参考）。

要访问 Apache Camel 功能的语言支持，您可以从 Eclipse Marketplace 安装 Eclipse 插件。详情请查看 Eclipse IDE 的 Apache Camel 语言服务器协议的 readme 文件。

Eclipse Che 功能

Eclipse Che 7 的 Apache Camel 插件的语言支持 在 XML DSL 和 Java DSL 中提供 Camel URI。

- 当您输入时，编辑器为 Camel 组件、属性和属性值列表提供代码完成。
- 将鼠标悬停在 Camel 组件上时，编辑器显示组件的简短描述（来自 Apache Camel 组件参考）。
- 保存文件时，编辑器对 Camel 代码执行 Apache Camel 验证检查。

要为 Eclipse Che 激活此插件，您可以使用 "Apache Camel based on Spring Boot" 堆栈或编辑工作区配置。

4.4. FUSE 7.12 的 BOM 文件

要将 Maven 项目配置为使用受支持的 Fuse 7.12 工件，请使用本节中记录的 BOM 版本。

4.4.1. Fuse 7.12 的 BOM 文件

要将 Fuse 独立应用程序升级到使用 7.12 依赖项，请编辑 Maven pom.xml 并更改下表中列出的 BOM 和 Maven 插件的版本：

表 4.1. 使用 BOM 的 7.12 Maven BOM 和插件版本

容器类型	Maven BOM 或 Plugin Artifact groupId/artifactId	Fuse 7.12 的版本
Spring Boot 2	**org.jboss.redhat-fuse/fuse-springboot-bom**	**7.12.0.fuse-7_12_0-00016-redhat-00001**
	org.jboss.redhat-fuse/spring-boot-maven-plugin	**7.12.0.fuse-7_12_0-00016-redhat-00001**
Apache Karaf	**org.jboss.redhat-fuse/fuse-karaf-bom**	**7.12.0.fuse-7_12_0-00016-redhat-00001**
	org.jboss.redhat-fuse/karaf-maven-plugin	**7.12.0.fuse-7_12_0-00016-redhat-00001**
JBoss EAP	**org.jboss.redhat-fuse/fuse-eap-bom**	**7.12.0.fuse-7_12_0-00016-redhat-00001**

有关使用 **BOM** 的详情，请参阅 迁移指南。

4.4.2. Fuse 7.12.1 的 BOM 文件

要将 **Maven** 项目配置为使用受支持的 **Fuse 7.12.1** 工件，请使用本节中记录的 **BOM** 版本。

表 4.2. 使用 BOM 的 7.12.1 Maven BOM 和插件版本

容器类型	Maven BOM 或 Plugin Artifact groupId/artifactId	Fuse 7.12.1 版本
Spring Boot 2	**org.jboss.redhat-fuse/fuse-springboot-bom**	**7.12.1.fuse-sb2-7_12_1-00009-redhat-00001**
	org.jboss.redhat-fuse/spring-boot-maven-plugin	**7.12.1.fuse-sb2-7_12_1-00009-redhat-00001**
Apache Karaf	**org.jboss.redhat-fuse/fuse-karaf-bom**	**7.12.1.fuse-sb2-7_12_1-00009-redhat-00001**
	org.jboss.redhat-fuse/karaf-maven-plugin	**7.12.1.fuse-sb2-7_12_1-00009-redhat-00001**
JBoss EAP	**org.jboss.redhat-fuse/fuse-eap-bom**	**7.12.1.fuse-sb2-7_12_1-00009-redhat-00001**

有关使用 **BOM** 的详情，请参阅 迁移指南。

4.5. 重要备注

Fuse standalone distribution 的 **Fuse 7.12** 发行版本的重要备注：

支持 Java 17

Fuse 7.12 发行版本支持 **Java 17**、**Java 11** 和 **Java 8**。

对 Karaf 运行时和 JBoss EAP 的支持已弃用

对 **Karaf** 运行时和 **JBoss EAP** 的支持已被弃用，因为 **Fuse 7** 将随着 **Fuse 7.12** 的发布而获得支持。

使用 MongoClients 工厂创建到 MongoDB 的连接

在 **Fuse 7.10** 及更高版本中，使用 **com.mongodb.client.MongoClient** 而不是 **com.mongodb.MongoClient** 来创建与 **MongoDB** 的连接（请注意完整路径中的额外的 **.client** 子软件包）。

这会影响使用 **camel-mongodb** 的任何用户应用程序，现在需要创建一个连接 **bean** 作为 **com.mongodb.client.MongoClient** 实例。此外，此类公开的方法与旧类完全相同，这需要重构用户代码。

例如，创建一个到 **MongoDB** 的连接，如下所示：

```
import com.mongodb.client.MongoClient;
```

然后您可以创建 **MongoClient bean**，如下例所示：

```
return MongoClients.create("mongodb://admin:password@192.168.99.102:32553");
```

第 5 章 弃用和删除的功能

如果您需要任何帮助，或者对 Fuse 7 中即将推出的更改有任何疑问，请联系 support@redhat.com。

5.1. 已弃用

Fuse 7.12 中已弃用以下功能，并可能在以后的版本中删除：

对 Fuse Online 的支持已弃用

对 Fuse Online 的支持现已弃用，因为 Fuse 7 现在处于维护支持中。Fuse 7 结束支持时，不会有任何用于 Fuse Online 的开发。

对 iPXE 运行时和 JBoss Enterprise Application Platform (EAP)的支持已弃用

当 Fuse 7 于 2024 年 6 月 30 日结束支持时，支持将停止支持，以及对 JBoss Enterprise Application Platform (EAP)的支持。当 Fuse 7 结束支持时，Camel 将不再在 Karaf OSGi 或 JBoss EAP 上受到支持。

OpenWire 协议已弃用

从 Fuse 7.10 开始，使用 OpenWire 协议（可用于连接 AMQ Broker 实例）已弃用。请注意，自 AMQ Broker 版本 7.9.0 后，OpenWire 协议也被弃用。

wsdl2rest 工具已弃用

自 Fuse 7.10 起，wsdl2rest 命令行工具已被弃用。VS Code 的 WSDL 2 Camel Rest DSL 扩展也已被弃用。

Fuse Online 安装脚本，用于在 OCP 4 上安装

自 Fuse 7.8 起，Fuse Online 安装脚本在 OpenShift Container Platform (OCP) 4.x 版本上安装 Fuse Online 已被弃用。在 OCP 4.x 版本中，我们建议您使用 Fuse Online Operator。

在 Camel 应用程序中弃用了 PHP、Python 和 Ruby 脚本语言

自 Fuse 7.4 起，PHP、Python 和 Ruby 脚本语言在 Camel 应用程序中被弃用，并将在以后的版本中删除。从 Camel 2.19 开始，Camel 社区已弃用 PHP、Python 和 Ruby （请参阅 CAMEL-10973）。这适用于所有 Fuse 容器类型：Apache Karaf、JBoss EAP 和 Spring Boot。

HP-UX OS 已被弃用

HP-UX 操作系统已被弃用，因为 Fuse 7.2 和对此操作系统的支持可能会在以后的 Fuse 发行版本中删除。特别是，JBoss EAP 7.2 容器已丢弃了对 HP-UX 的支持，因此任何在 JBoss EAP 7.2 上运行的 Fuse 版本都不支持在 HP-UX 上。

Camel MQTT 组件已弃用

Camel MQTT 组件在 **Fuse 7.0** 中已弃用，并将在以后的 **Fuse** 发行版本中删除。您可以使用 **Camel Paho** 组件，它使用流行的 **Eclipse Paho** 库来支持 **MQTT** 消息传递协议。

除了 Linux 外，Camel LevelDB 组件在所有操作系统中都已弃用

自 **Fuse 6.3** 起，**Camel LevelDB (camel-leveldb)**组件在所有操作系统上已被弃用，但 **Red Hat Enterprise Linux** 除外。未来，**Camel LevelDB** 组件仅在 **Red Hat Enterprise Linux** 上被支持。

Camel SJMS 组件的 BatchMessage 类已弃用

Camel SJMS 组件的 **BatchMessage** 类在 **Fuse 7** 中被弃用（自 **Apache Camel 2.17** 起弃用），并可能从未来版本的 **Apache Camel** 和 **Fuse** 中删除。

5.2. 在 FUSE 7.11 中删除

在 OCP 3.11 上安装 Fuse Online

不支持在 **OCP 3.11** 上安装 **Fuse** 在线环境 **7.12**。在 **OCP 3.11** 上安装 **Fuse Online** 的 **Fuse Online** 已完全删除。

由 camel-ftp 和 camel-ssh 默认不支持 RSA/SHA-1 Ciphers

在 **Fuse 7.11** 中，**camel-ftp** 和 **camel-ssh** 组件将不再支持 **RSA/SHA-1** 密码的 **TLS**。依赖于 **JSch** 库的其他 **Camel** 组件也可能会受到影响。

如需更多信息，请参阅此红帽客户门户网站文章。

5.3. 在 FUSE 7.10 中删除

fabric8-maven-plugin

fabric8-maven-plugin 已从 **Fuse 7.10** 中完全删除。我们建议您使用 **openshift-maven-plugin** 在 **OpenShift** 上的 **Fuse** 中构建和部署 **Maven** 项目。该插件由 **Eclipse JKube** 维护，它为插件提供了广泛的文档。

5.4. 在 FUSE 7.8 中删除

Spring Boot 1

Fuse 7.8 不再支持 **Spring Boot 1**。建议您按照 **Spring Boot 2.0** 迁移指南中的指导将 **Spring Boot** 应用程序迁移到 **Spring Boot 2**。

Fuse Online 中的 Camel K 运行时

Fuse 7.8 不再支持 **Fuse Online** 中的 **Camel K** 运行时（技术预览功能）。

Camel XmlJson 组件已在 **7.8** 中删除

Camel XmlJson (camel-xmljson)组件已在 **Fuse 7.8** 中删除。

5.5. 在 FUSE 7.5 中删除

Fuse 7.5 中删除了以下功能：

7.5 中丢弃了对与 **MS SQL Server 2014** 集成的支持

MS SQL Server 2014 不再经过测试并支持与 **Fuse 7.5** 集成。我们建议您使用 **MS SQL Server** 最新版本，而不是 **iwl-setuptools**，例如，**MS SQL Server 2016** 或 **2017**。

Camel LinkedIn 组件已在 **7.5** 中删除

在 **Fuse 7.5** 中删除了 **camel-linkedin** 组件。

重要

虽然从 **Fuse 7.5** 中删除，但 **camel-linkedin** 组件可能会在以后的发行版本中恢复。

5.6. 在 FUSE 7.3 中删除

Fuse 7.3 中删除了以下功能：

Camel YQL 组件已在 **7.3** 中删除

Camel YQL 组件已在 **Fuse 7.3** 中删除。

7.3 中已删除了 **openjpa** 和 **OpenzFCP3 Karaf** 功能

openjpa 功能和 **openjpa3** 功能已从 **7.3** 中的 **Apache Karaf** 容器中删除。对于 **Java Persistence** 架构**(diag)**实现，请使用支持的 **hibernate** 功能。

在 **7.3** 中删除了 **camel-jetty Karaf** 功能

camel-jetty 功能已从 **7.3** 中的 **Apache Karaf** 容器中删除，因为它使用 **Jetty 8**。改为使用

camel-jetty9 功能。

在 7.3 中删除了 Pax-jms-oracleaq Karaf 功能

pax-jms-oracleaq 功能已从 7.3 中的 Apache Karaf 容器中删除，因为它需要第三方非免费 Oracle AQ 库。

在 7.3 中，camel-elasticsearch 组件已从 EAP 上的 Fuse 中删除(Wildfly Camel)

camel-elasticsearch 组件已从 7.3 中的 EAP 上的 Fuse (Wildfly Camel)中删除。改为使用较新的 camel-elasticsearch-rest 组件。

5.7. 在 FUSE 7.2 中删除

Fuse 7.2 中删除了以下功能：

Camel XMLRPC 组件已在 7.2 中删除

Camel XMLRPC 组件已在 Fuse 7.2 中删除。

Camel Netty 组件已在 7.2 中删除

Camel Netty 组件已在 Fuse 7.2 中删除。建议您改用 Camel Netty4 组件。

5.8. 在 FUSE 7.0 中删除

Fuse 7.0 中删除了以下功能：

7.0 中删除了对 Red Hat JBoss Operations Network (JON)的支持

自 Fuse 7.0 起，Flytron 上的 Fuse 不再支持 JON，不再提供用于与 JON 运行时集成的 JON 插件。

7.0 中删除了嵌入的 ActiveMQ 代理

自 Fuse 7.0 起，Fleti 上的 Fuse 不再提供嵌入式 ActiveMQ Broker。客户应直接连接到受支持的远程代理。有关我们支持的代理的更多信息，请参阅 Red Hat Fuse 支持的配置 页面中的 "支持消息传递提供程序"部分。

7.0 中删除了 Fuse 集成包

对运行规则和流程的支持由 Red Hat JBoss BPM Suite 和 Red Hat JBoss BRMS 附带的组件提供。

7.0 中已删除用于子容器管理的 Karaf 控制台命令

自 **Fuse 7.0** 起，不支持 用于子容器管理的 **Karaf** 控制台命令。也就是说，不支持以 **instance: (Karaf 4.x** 语法)和前缀为 **admin: (Karaf 2.x** 语法)的控制台命令。

注意

在 **Fuse 7.0 GA** 版本中，**instance:** 命令不会被删除。这是个已知问题。

7.0 中已删除了 SwitchYard

自 **Fuse 7.0** 起，**drad** 已被删除，您应该直接使用 **Apache Camel**。如需更多信息，请参阅 **Swoning Support Plan after Releasing Fuse 7**。

7.0 中删除了对 Fabric8 1.x 的支持

自 **Fuse 7.0** 起，**Fabra8 v1** 已被 **OpenShift** 上的 **Fuse**（以前为 **Fuse** 集成服务）替代，其中包括 **Fabric8 v2** 技术的组件。**OpenShift** 上的 **Fuse** 提供了一组工具和 **Docker** 格式镜像，支持 **OpenShift** 中集成微服务的开发、部署和管理。

虽然 **OpenShift** 上的 **Fuse** 具有不同的架构，但它满足 **Fabric8 v1** 提供的相同调配、自动化、中央配置和管理要求。如需更多信息，请参阅 **OpenShift** 上的 **Fuse** 指南。

7.0 中删除了 Google App Engine 的 Camel 组件

Fuse 7.0 中删除了 **Google App Engine** 的 **Camel** 组件**(camel-gae)**。

在 7.0 中删除了 Camel jBPM 组件

Camel jBPM 组件**(camel-jbpm)**已在 **Fuse 7.0** 中删除。

7.0 中删除了将 Fuse 安装为服务的 Tanuki 的打包程序

在 **Fuse 7.0** 中删除了基于 **Tanuki** 的 **wrapper** 脚本，使用 **wrapper:install Karaf console command iwl-wagon for** 将 **Fuse** 作为服务安装。要将 **Apache Karaf** 容器安装为一个服务，建议您改为使用 **bin/contrib** 目录中的新的 **karaf-service indices.sh** 脚本。

在 7.0 中删除了 Smooks

自 **Fuse 7.0** 起，**Smooks** 组件已删除。

在 7.0 中删除了 puppetlabs

VirtIO（基于 **Riftsaw** 项目）已从 **Fuse 7.0** 中删除。如果您当前正在使用 **mvapich**，建议您考虑迁移到红帽 **JBoss BPM** 套件。

7.0 中删除了设计时间监管

Design Time Governance 组件已在 7.0 中删除。

7.0 中删除了运行时监管

自 Fuse 7.0 起，删除了 Runtime Governance (RTGov)组件。

在 7.0 中删除 s-RAMP

Fuse 7.0 中删除了 SOA Repository Artifact Model and Protocol (S-RAMP)组件。

bin/patch 脚本已在 7.0 中删除

在 Fuse 7.0 中删除了 bin/patch 脚本(bin\patch.bat on Windows O/S)。

7.0 不支持 Spring Dynamic Modules (Spring-DM)

Fuse 7.0 不支持 Spring XML 与 Apache Karaf 中的 OSGi 服务层集成，您应该改为使用 Blueprint 框架。使用 Blueprint XML 不会阻止您使用 Spring 框架中的 Java 库：最新版本的 Spring 与 Blueprint 兼容。

7.0 不支持 Apache Open JPA

Fuse7.0 不支持 Java Persistence API (JPA)的 Apache Open JPA 实现。建议您使用 Hibernate 实现。

5.9. 在 FUSE 7.0 中替换

Fuse 7.0 中替换了以下功能：

在 7.0 中已替换了 Geronimo 事务管理器

在 Fuse 7.0 中，Geronimo 容器中的 Geronimo 事务管理器已被 Narayana 替代。

jetty 容器已在 7.0 中被替换

在 Fuse 7.0 中，Jetty 容器已被 Undertow 替代。最初，此更改仅适用于 Jetty 容器的内部使用（例如，在 Karaf 容器中）。其他 Jetty 组件可能会在以后的版本中删除。

第 6 章 FUSE 7.12 中不支持的功能

Red Hat Fuse 7.12 不支持以下功能。

IBM PowerPC 和 Z 平台上的 Fuse 不支持 camel-leveldb 组件

当在 IBM PowerPC 或 IBM Z 平台上安装 Fuse 时，不支持 Camel LevelDB 组件。

OpenShift Container Platform (OCP) 3.11 不支持安装和运行 Fuse Online

OpenShift Container Platform (OCP) 3.11 不支持安装和运行 Fuse Online，因为 Fabric8 Maven 插件已弃用，而是使用 OpenShift Maven 插件。

OCP 3.11 不支持使用 Operator 安装 Fuse Console

不支持使用 Operator 安装 Fuse 控制台，且不适用于 OpenShift Container Platform (OCP) 3.11。在 OCP 3.11 上安装 Fuse Console 的建议方法是使用模板。

不支持 Apache Karaf EclipseLink 功能

Fuse 不支持 Apache Karaf EclipseLink 功能，因为此功能依赖于 JPA 2.2，而 Fuse 7.2 的 Karaf 容器与 JPA 2.1 一致。

不支持 Apache Aries Blueprint Web 模块

Fuse 不支持 Apache Aries Blueprint Web 模块。在 Apache Camel 的社区版中存在一个包含 Blueprint Web 的示例（作为单独的下载提供） 并不意味着 Fuse 中支持此功能。

Apache Camel on Apache Karaf 不支持 PHP 脚本语言

Apache Karaf 容器上的 Camel 应用程序 不支持 PHP 脚本语言，因为 PHP 没有适用于 PHP 的 OSGi 捆绑包。PHP 脚本语言在 JBoss EAP 容器和 Spring Boot 容器中的 Camel 应用程序中被弃用。

Apache Camel on Apache Karaf 不支持 Python 脚本语言

Apache Karaf 容器上的 Camel 应用程序 不支持 Python 脚本语言，因为 Python 没有适用于 Python 的 OSGi 捆绑包。Python 脚本语言在 JBoss EAP 容器和 Spring Boot 容器中的 Camel 应用程序中被弃用。

第 7 章 已知问题

以下小节描述了版本 7.12 中的已知问题。

7.1. CVE 安全漏洞

作为中间件集成平台，Fuse 可能会与大量第三方组件集成。无法始终排除 Fuse 的一些第三方依赖项可能会存在安全漏洞。本节记录了与影响 Fuse 7.12 第三方依赖项的安全性相关的已知常见漏洞和暴露 (CVE)。

CVE-2020-13936 CVE-2020-13936 velocity: 当攻击者能够修改模板时执行任意代码

可以修改 Velocity 模板的攻击者可以执行任意 Java 代码，或运行任意系统命令，其特权与运行 Servlet 容器的帐户相同。这适用于允许不受信任的用户上传/修改 velocity 模板的应用程序，这些模板运行 Apache Velocity Engine 版本（最多 2.2）。

Fuse 7.9 （及更高版本）的依赖项可确保只使用防止此漏洞的固定的 Velocity 版本(2.3)。如果您的应用程序代码对 Apache Velocity 组件有明确的依赖项，我们建议您升级这些依赖项以使用固定版本。

CVE-2018-10237 CVE-2018-10237 guava: Unbounded memory allocation in AtomicDoubleArray 和 CompoundOrdering 类允许远程攻击者拒绝服务 [fuse-7.0.0]

Google Guava 版本 11.0 到 24.1 会受到 AtomicDoubleArray 类中未绑定的内存分配（当使用 Java 序列化序列化）和 CompoundOrdering 类（当使用 research 序列化序列化）中无限的内存分配。攻击者可以利用使用 Guava 和反序列化不序列化数据的应用程序，从而导致拒绝 service iwl-osgi。如需更多信息，请参阅 CVE-2018-10237。

要避免此安全漏洞，我们建议您：

- 从未知源不会反序列化 AtomicDoubleArray 实例或 CompoundOrdering 实例。
- 避免使用 Guava 版本 24 及更早版本（虽然在某些情况下无法避免早期版本）。

为了便于避免较早版本的 Guava，Fuse 7.7 （及更高版本）版本已经为所有容器配置了 Maven Bill of Materials (BOM)文件，以默认选择 Guava 27。这意味着，如果您在 Maven 项目中将 Fuse BOM 整合到 Maven 项目中（通过将 BOM 的依赖添加到 POM 文件的 dependencyManagement 部分），然后在没有指定显式版本 的情况下 指定 Guava 工件的依赖关系，Genava 版本将默认为 BOM 中指定的版本，即 Fuse 7.7 BOM 的版本 27。

但是，至少有一个常见的用例涉及 **Apache Karaf (OSGi)**容器，在这种情况下，无法避免使用 **Guava**：如果您的 **OSGi** 应用程序使用 **Guava** 和 **Swagger**，则您很难使用 **Guava 20**，因为这是 **Swagger** 所需的版本。在这里我们解释为什么如此，以及如何配置 **POM** 文件来恢复之前 **(vulnerable) Genava 20** 库。首先，您需要了解 双 **OSGi** 链 的概念。

双 **OSGi** 链

OSGi 运行时中的捆绑包使用软件包约束（软件包名称 **+** 可选版本/范围）来连接 **together**，以及 **exports**。每个捆绑包可以有多个导入，通常那些导入一个带有多个捆绑包的捆绑包。例如：

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

其中 **BundleA** 依赖于 **BundleB** 和 **BundleCb**，而 **BundleB** 则依赖于 **BundleCa**。**BundleCa** 和 **BundleCb** 应相同捆绑包，如果导出相同的软件包，但由于版本（范围）约束，**BundleB** 使用(有线) 与 **BundleA** 不同的修订版本/版本 **BundleC**。

重写前面的图，以反映应用程序中的 **Guava** 和 **Swagger** 的依赖关系时发生的情况：

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

如果您尝试部署此捆绑包配置，您会收到错误 **org.osgi.framework.BundleException: Uses constraint violation**。

恢复到 **Guava 20**

如果您的项目同时使用 **Guava** 和 **Swagger** 库（直接或间接），您应该将 **maven-bundle-plugin** 配置为对 **Guava** 捆绑包导入使用显式版本范围（或根本没有范围），如下所示：

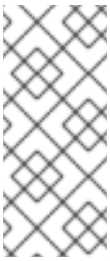
```
<Import-Package>
   com.google.common.base;version="[20.0,21.0)",
   com.google.common.collect;version="[20.0,21.0)",
```

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

此配置会强制您的 **OSGi** 应用程序恢复到**(vulnerable) Garava 20** 库。因此，在这种情况下，务必要避免反序列化 **AtomicDoubleArray** 实例。

CVE-2017-12629 Solr/Lucene -security 绕过访问敏感数据 **- CVE-2017-12629**

Apache Solr 是一个流行的开源搜索平台，它使用 **Apache Lucene** 搜索引擎。如果您的应用程序使用 **Apache Solr** 与 **Apache Lucene** （例如，使用 **Camel Solr** 组件）的 **Apache Solr** 的组合，则可能会受此安全漏洞的影响。有关此漏洞的详情以及要采取的缓解方案，请参阅链接的安全公告。



注意

Fuse 运行时 不直接 使用 **Apache Solr** 或 **Apache Lucene**。只有在集成应用程序上下文中同时使用 **Apache Solr** 和 **Apache Lucene** 时（例如，使用 **Camel Solr** 组件时），才会出现安全风险。

CVE-2021-30129 mina-sshd-core: 在 **Apache Mina SSHD** 服务器中内存泄漏拒绝服务

Apache Mina SSHD 的 **sshd-core** 中的漏洞允许攻击者溢出服务器导致 **OutOfMemory** 错误。此问题会影响 **Apache Mina SSHD** 版本 **2.0.0** 及更新版本的 **SFTP** 和端口转发功能。它在 **Apache Mina SSHD 2.7.0** 中解决

Apache Mina SSHD 中的此漏洞由 **SSHD-1004** 解决，它弃用了存在此漏洞的某些加密算法。在 **JBoss EAP** 上的 **Fuse 7.10** 和 **Fuse 7.10** 中，这些已弃用的算法仍被支持（出于向后兼容性的原因）。但是，如果您使用这些已弃用的算法之一，强烈建议您重构应用程序代码以使用不同的算法。

在 **Fuse 7.10** 中，默认的加密算法已更改，如下所示：

Fuse 7.9	Fuse 7.10	在 Fuse 7.10 中被弃用？
aes128-ctr	**aes128-ctr**	
	aes192-ctr	
	aes256-ctr	
	aes128-gcm@openssh.com	
	aes256-gcm@openssh.com	

Fuse 7.9	Fuse 7.10	在 Fuse 7.10 中被弃用？
arcfour128	**arcfour128**	**是**
aes128-cbc	**aes128-cbc**	
	aes192-cbc	
	aes256-cbc	
3des-cbc	**3des-cbc**	**是**
blowfish-cbc	**blowfish-cbc**	**是**

*在 **Fuse 7.10** 中，默认的密钥交换算法已更改，如下所示：*

Fuse 7.9	Fuse 7.10	在 7.10 中被弃用？
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**	
	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**	**是**

Fuse 7.9	Fuse 7.10	在 7.10 中被弃用？
diffie-hellman-group1-sha1	diffie-hellman-group1-sha1	是

7.2. FUSE ONLINE

Fuse Online 发行版有以下已知问题：

ENTESB-21338 Twitter API v1.1 对新应用程序的限制

由于 Twitter v1.1 API 限制，任何新的 Twitter 应用程序都无法正常工作。

ENTESB-17674 Monitoring Fuse Online with Prometheus 和 Grafana on OCP 4.9 （或更新版本）需要临时解决方案

在 OCP 4.9 （或更新版本）上，application-monitoring 项目不再有效。监控 Fuse 在线集成和基础架构组件与 Prometheus 和 Grafana 的先决条件。

要临时解决这个问题，您可以使用 内置的监控堆栈（在 openshift-monitoring 命名空间中 ）使用 openshift-user-workload-monitoring 功能，以及 grafana-operator 来使用 ops addon，如这些发行注记的 Fuse Online 部分所述。

由 Syndesis 1.11 安装的 ENTESB-14518 Jaeger operator 会影响其他命名空间

自 Fuse 7.8 起，当您在 OpenShift 集群上安装 Fuse 7.8 Online (Syndesis 1.11)时，Jaeger Operator （与 Fuse Online 一起安装）会被配置为默认管理 所有命名空间。此行为的一个副作用是，当您在集群中安装了 Fuse 7.7 Online (Syndesis 1.10)，然后在不同的命名空间中安装 Fuse 7.8 Online 时，使用 Fuse 7.8 Online 安装的 Jaeger Operator 会尝试管理 Fuse 7.7 Online 命名空间上安装的 Jaeger 实例。结果是，在 Fuse 7.7 Online 命名空间中的现有 syndesis-jaeger podcategories-jaeger podcategories-MAPPINGappears 增加了新的 syndesis-jaeger pod，新的 syndesis-jaeger pod 会进入 CrashLoopBackOff 状态。原始 Fuse 7.7 Online 实例不受影响，可以安全地忽略崩溃的复合 pod。

部署集成 API 的 ENTESB-13966 发现功能被禁用，但不真正禁用

从 Fuse 7.7 开始，在创建一个包含 API 的新集成后，集成详情页面会错误地表示这个集成禁用了 3scale 发现。另外，集成详情页面不会显示 API URL。通过单击此按钮三次（单击" 启用 "，然后单击" 禁用 "），您可以重新同步页面，以便启用 3scale 发现，并显示 API URL。

7.3. OPENSHIFT 上的 FUSE

本节列出了影响在 OpenShift 中部署 Fuse 应用程序的问题。有关影响特定容器的问题详情，请参阅 Spring Boot、Apache Karaf 上的 Fuse 部分，以及 JBoss EAP 上的 Fuse。OpenShift 发行版上的

Fuse 有以下已知问题：

ENTESB-21281 使用 **add-opens** 更新 **FoO** 镜像

在 **Open Shift** 上没有 **add-opens Fuse** 无法与 **jdk17** 正常工作。这些标志无法自动交付，因此您必须通过将标志添加到定义 附加组件的脚本来自行指定。

自 **Java 17** 起，**Java** 平台模块系统 是强制的。它实施强大的封装，以 限制访问。您可以使用 **--add-opens** 选项允许访问，提供深度反映，并允许指定的模块打开 **named** 软件包：

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

ENTESB-21281 [Fuse on Openshift] QS karaf-cxf-rest - JavaDoc 不再支持 **jdk17**

Red Hat FUSE 7.x 中的 **cxf java2wadl-plugin** 不适用于 **JDK17**。

ENTESB-17895 [Fuse Console] 升级订阅不会更新 **Hawtio**

在 **Fuse 7.10** 中，如果您通过将 **Operator** 订阅频道更改为版本 **7.10** 来更新 **Fuse** 控制台，**Fuse Console** 会保留在 **vesion 7.9** 上。即使 **Fuse Console** 容器和 **pod** 具有标签 **7.10**，它们仍然使用 **7.9** 镜像。要临时解决这个问题，请通过删除旧版本的 **Fuse** 控制台来执行升级，然后进行全新的 **Fuse Console** 版本 **7.10** 安装。

ENTESB-17861 Apicurito generator 无法生成 **Fuse Camel** 项目

在 **Fuse 7.10** 中，如果 **API Designer (Apicurito)**通过 **Apicurito Operator** 安装**(giving a Invalid Cert Error)**安装它无法正常工作。要临时解决这个问题：

1. 打开一个新标签页，进入 **https://apicurito-service-generator-apicurito.apps.cluster-name.openshift.com**

   （将 **cluster-name.openshift.com** 替换为集群名称。）

2. 接受证书。

3. 切换到应用程序，然后再次单击 **generate** 按钮。

ENTESB-17836 [Fuse Console] 在 **Camel** 树中不会显示新添加的路由

在 **Fuse 7.10** 中，部署应用程序后，**Fuse Console** 上的 **Camel** 树中不会显示路由（或路由）。您可以通过刷新页面来解决此问题，这应该会显示路由。

OCP 上的 **ENTESB-19351 FIPS - Jolokia** 代理因为不支持的安全编码而没有启动

在启用了 **OCP FIPS** 的 **Jolokia** 代理中的 **Fuse 7.11** 中，因为不支持的安全编码而不可用。

OCP 上的 **ENTESB-19352 FIPS - karaf-maven-plugin assembly** 目标无法不支持的安全供应商

在 **Fuse 7.11** 中，如果我们使用带有 **assembly** 目标的 **karaf-maven-plugin**，则二进制流部署策略在启用了 **OCP FIPS** 时失败。

7.4. APACHE KARAF 上的 FUSE

Apache Karaf 上的 **Fuse** 有以下已知问题：

ENTESB-16417 凭证存储默认使用 **PBEWithSHA1AndDESede**

OpenJDK 8u292 和 **OracleJDK 1.8.0_291** 中的安全 **API** 返回不完整的安全提供程序列表，这会导致 **Apache Karaf** 中的凭证存储失败（因为所需的安全供应商似乎不可用）。导致此问题的根本问题是 **https://bugs.openjdk.java.net/browse/JDK-8249906**。我们建议您使用早期的 **OpenJDK** 版本、**OpenJDK 8u282** 或更新的 **OpenJDK** 版本 **OpenJDK 8u302**，它们没有这个程序错误。

Windows 上的 **ENTESB-16526 fuse-karaf** 无法在补丁期间重启：**install**

在 **Windows** 平台上的 **Apache Karaf** 容器中运行 **patch:install** 时，在某些情况下，在 **patch:install** 命令尝试自动重启容器时可能会遇到以下错误：

```
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.
```

如果您遇到此错误，只需手动重新启动 **Karaf** 容器。

ENTESB-8140 Start 级别热部署捆绑包默认为 **80**

从 **Fuse 7.0 GA** 版本开始，在 **Apache Karaf** 容器中，热部署的捆绑包的开始级别默认为 **80**。这可能会导致热部署捆绑包出现问题，因为有很多系统捆绑包和功能具有相同的启动级别。要临时解决这个问题，并确保热部署的捆绑包可靠地启动，请编辑 **etc/org.apache.felix.fileinstall-deploy.cfg** 文件并更改 **felix.fileinstall.start.level** 设置，如下所示：

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

ENTESB-7664 安装框架安全特性终止 **karaf**

必须使用 **--no-auto-refresh** 选项安装 **framework-security OSGi** 功能，否则此功能将关闭 **Apache Karaf** 容器。例如：

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

7.5. JBOSS EAP 上的 FUSE

JBoss EAP 上的 **Fuse** 有以下已知问题：

ENTESB-21314 **[EAP** 上的**Fuse]** 支持 **jdk17** 模块

在 **EAP** 上没有 **add-opens Fuse** 无法与 **jdk17** 正常工作。这些标志无法自动交付，因此您必须通过将标志添加到定义 附加组件的脚本来自行指定。

自 **Java 17** 起，**Java** 平台模块系统 是强制的。它实施强大的封装，以 限制访问。您可以使用 **--add-opens** 选项允许访问，提供深度反映，并允许指定的模块打开 **named** 软件包：

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

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

java.security.acl.Group 在 **jdk14** 或更高版本中删除。

EAP 域模式上的 **ENTESB-13168** **Camel** 部署无法在 **Windows** 上工作

从 **Fuse 7.6.0** 开始，对于 **JBoss EAP** 上的 **Fuse**，在 **Windows OS** 上的域模式中无法部署 **Camel** 子系统。

7.6. SPRING BOOT 上的 FUSE

Spring Boot 上的 **Fuse** 有以下已知问题：

ENTESB-21315 [在 Spring-boot 上使用支持 jdk17 模块

如果没有 附加打开 Fuse，则无法与 jdk17 正常工作。这些标志无法自动交付，因此您必须通过将标志添加到定义 附加组件的脚本来自行指定。

自 Java 17 起，Java 平台模块系统 是强制的。它实施强大的封装，以 限制访问。您可以使用 --add-opens 选项允许访问，提供深度反映，并允许指定的模块打开 named 软件包：

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

ENTESB-21421 / ENTESB-20842 Spring Boot 2.6 不允许循环依赖项

Spring Boot 2.6 可能无法解析循环依赖项。如果您在 Spring Boot 中使用 XML DSL 来实例化 beans 文件中的自定义 HealthCheckRegistry，则构建会失败。

作为临时解决方案，您可以将属性 spring.main.allow-circular-references=true 添加到 application.properties。

7.7. FUSE 工具

Fuse 工具有以下已知问题：

ENTESB-20965 [Hawtio] Login failed due: no LoginModules 为 hawtio-domain

Hawtio 只能使用 WildFly 的旧安全系统。如果您试图使用 Elytron 安全性登录到 Hawtio，控制台会显示以下出错信息。

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

ENTESB-19668 当客户端证书身份验证被拒绝时，Hawtio 管理控制台不会在 UI 上显示消息

在拒绝来自客户端证书的身份验证后，Hawtio 组件不会在登录页面上显示任何消息。Hawtio 仅将网页浏览器重定向到登录页面，而不显示任何消息。

ENTESB-17705 [Hawtio] Logout 按钮会消失

在 Fuse 7.10 中，登录并注销一行内多次后，不会显示 Logout 按钮。要临时解决这个问题，您可以刷新页面一次或多次，Logout 按钮应该重新应用。

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

在 Fuse 7.11 中，如果用户想要使用 AtlasMap vscode 扩展，那么他们必须使用 0.0.9 版本，因

为 Fuse 7.11 与 AtlasMap 2.3.x 使用。否则，请使用 AtlasMap standalone 2.3.x，但不使用 vscode-extension。

7.8. APACHE CAMEL

Apache Camel 有以下已知问题：

ENTESB-19361 / UNDERTOW-2206 Access logging support by cxf with embedded undertow server on karaf 不记录 URI

如果 DECODE_URL 选项为 true （这是 Fuse 7.11.1 karaf 运行时的默认值），并使用 HttpServerExchange 来解码 relativePath 和 requestPath，则 requestURI 参数保持编码。

分配方法(转发，包括,async 和 error)分配路径而不解码，对于 requestPath 和 relativeURL，这会导致分配给路径，如 /some%20thing。

ENTESB-15343 XSLT 组件无法与 IBM1.8 JDK 正常工作

在 Fuse 7.8 中，Camel XSLT 组件无法与 IBM 1.8 JDK 正常工作。出现这个问题的原因是，XSLT 的 Apache Xerces 实现不支持 javax.xml.XMLConstants#FEATURE_SECURE_PROCESSING 属性（请参阅 XERCESJ-1654）。

ENTESB-11060 [camel-linkedin] V1 API 不再被支持

自 Fuse 7.4.0 起，Camel LinkedIn 组件无法再与 LinkedIn 服务器通信，因为它使用 LinkedIn Version 1.0 API 实施，它不再受 LinkedIn 支持。Camel LinkedIn 组件将更新为在以后的 Fuse 版本中使用 Version 2 API。

ENTESB-7469 Camel Docker 组件无法在 EAP 上使用 Unix 套接字连接

自 Fuse 7.0 起，camel-docker 组件只能通过其 REST API 连接到 Docker，而不通过 UNIX 套接字连接。

ENTESB-5231 PHP 脚本语言无法正常工作

Apache Karaf 容器上的 Camel 应用程序 不支持 PHP 脚本语言，因为 PHP 没有适用于 PHP 的 OSGi 捆绑包。

ENTESB-5232 Python 语言无法正常工作

Apache Karaf 容器上的 Camel 应用程序 不支持 Python 脚本语言，因为 Python 没有适用于 Python 的 OSGi 捆绑包。

ENTESB-2443 Google Mail API - 发送消息和草案不是同步

当您发送消息或草案时，响应包含一个 ID 的 Message 对象。可能无法通过另一个调用 API 立即

获取此消息。您可能需要等待和重试调用。

ENTESB-2332 Google Drive API JSON 响应用于更改返回首页的项目的错误计数

Google Drive API JSON *响应用于更改返回首页的项目的错误计数。为列表操作设置* **maxResults** *可能无法返回第一个页面中的所有结果。您可能需要通过多个页面来获取完整的列表（即在新请求中设置* **pageToken** *）。*

第 8 章 修复了 FUSE 7.12 中的问题

以下小节列出了 **Fuse 7.12** 和 **Fuse 7.12.1** 中修复的问题：

- 第 8.1 节 “Fuse 7.12 中的增强”
- 第 8.2 节 “Fuse 7.12 中的组件升级”
- 第 8.3 节 “在 Fuse 7.12 中解决的错误”
- 第 8.4 节 “Fuse 7.12.1 中解决的错误”

8.1. FUSE 7.12 中的增强

问题	描述
ENTESB-17374	公开载入的插件以避免多个对 PluginServlet 的请求
ENTESB-20016	Fuse Console - 允许在 hawtio CR 中设置标签
ENTESB-20592	在 ELS 之前，在 OpenJDK 17 上认证 Fuse 7
ENTESB-20667	operator 元数据捆绑包的 operators.openshift.io/valid-subscription 注解
ENTESB-20714	确保通过 JDK17 传递的所有 CXF 测试
ENTESB-20830	在 RHEL 9 上认证 Fuse 7
ENTESB-20953	升级到 EAP-7.4.10.GA-redhat-00002

8.2. FUSE 7.12 中的组件升级

下表列出了 **Fuse 7.12** 中的组件升级。

表 **8.1. Fuse 7.12** 组件升级

问题	描述
ENTESB-20648	将 Spring Boot 升级到 2.7.12
ENTESB-20849	使 Camel 测试依赖项与 JDK17 兼容
ENTESB-21063	与 kafka-clients v3 一致

8.3. 在 FUSE 7.12 中解决的错误

*下表列出了 **Fuse 7.12** 中已解析的错误。*

*表 **8.2. Fuse 7.12** 解决的错误*

问题	描述
ENTESB-8337	离线存储库包含 org.jboss.fuse.fis.archetypes 组名称 artfacts
ENTESB-12949	SQS 步骤创建中的下一个按钮在更改自动填充的队列值前被禁用
ENTESB-13046	使用 Operator 二进制文件恢复无法正常工作
ENTESB-13366	Operator 指令不明确，secret 创建步骤不容易调试
ENTESB-13966	发现部署的集成 API 似乎已禁用，但并不实际
ENTESB-14552	支持多播队列
ENTESB-17394	错误感叹号不会显示错误消息
ENTESB-17404	x86 的构建 leveldb-jni
ENTESB-17888	连接到 https 端点时验证错误
ENTESB-18042	监控 Operator 日志中输出的错误失败
ENTESB-18364	Hawtio - 在 Keycloak 中使用 Hawtio 时 CSP 问题
ENTESB-19351	OCP 上的 FIPS - Jolokia 代理没有启动，因为不支持的安全编码
ENTESB-19352	OCP 上的 FIPS - karaf-maven-plugin assembly 目标无法不支持的安全供应商
ENTESB-19745	Quickstart spring-boot-camel-amq 集成测试引用旧的 AMQ Broker 版本

问题	描述
ENTESB-19757	为 apicurito 提供源容器镜像
ENTESB-19956	[Syndesis] CVE-2022-24785 Moment.js: Path traversal in moment.locale [fuse-7]
ENTESB-19986	Fuse hawtio 包括 HTTPClient 3.1 - CVE-2012-5783
ENTESB-20096	AMQ6 镜像 - V2 模式 1 清单摘要不再支持进行镜像拉取
ENTESB-20175	在运行时目录中缺少 dataformats fhir-json/fhir-xml/xml-json
ENTESB-20177	为容器构建发送正确的 UMB 消息
ENTESB-20404	Camel http4 producer 将数组数据编码为 http uri 参数，用逗号分开，而不是多值参数
ENTESB-20485	CVE-2022-42920 apache-bcel: Apache-Commons-BCEL: 通过越界写入 [fuse-7] 提供的任意字节代码
ENTESB-20595	将 ENTMQCL-2977 的请求反向移植到 Fuse 7.11.x
ENTESB-20596	CVE-2022-41940 engine.io：特别设计的 HTTP 请求可触发异常 [fuse-7]
ENTESB-20598	CVE-2020-13956 的不完整修复
ENTESB-20618	CVE-2022-41881 codec-haproxy: HAProxyMessageDecoder Stack Exhaustion DoS [fuse-7]
ENTESB-20619	CVE-2022-41854 dev-java-snakeyaml: dev-java/snakeyaml: DoS via stack overflow [fuse-7]
ENTESB-20626	CVE-2022-40146 batik: Server-Side Request Forgery (SSRF)安全漏洞 [fuse-7]
ENTESB-20627	CVE-2022-38398 batik: Server-Side Request Forgery [fuse-7]
ENTESB-20628	CVE-2022-38648 batik: Server-Side Request Forgery [fuse-7]
ENTESB-20630	CVE-2022-46364 CXF: Apache CXF: SSRF Vulnerability [fuse-7]
ENTESB-20632	CVE-2022-46363 CXF: Apache CXF: 目录列出 / 代码 exfiltration [fuse-7]
ENTESB-20637	CVE-2022-4492 undertow: https 连接中的服务器身份不是由 undertow 客户端 [fuse-7] 检查

问题	描述
ENTESB-20641	CVE-2022-41946 jdbc-postgresql: postgresql-jdbc: Information leak of prepared 语句数据因为不安全的临时文件权限 [fuse-7]
ENTESB-20663	带有 jdk17 启动期间的错误
ENTESB-20664	使用 jdk17 在 EAP 启动过程中出现错误
ENTESB-20672	CVE-2022-45143 tomcat: JsonErrorReportValve injection [fuse-7]
ENTESB-20690	CVE-2022-36437 hazelcast: Hazelcast 连接缓存 [fuse-7]
ENTESB-20693	查看 patch-maven-plugin → karaf-maven-plugin 通信
ENTESB-20696	自定义 fuse 控制台路由无法正常工作。
ENTESB-20697	从 RabbitMQ Connection Factory 自动恢复始终创建新连接
ENTESB-20701	fuse-patch 可能会错误地报告已应用了补丁
ENTESB-20702	netty4-http 转发一个错误的响应(exception + http code 200)
ENTESB-20710	升级到 Karaf 4.4 和 Pax Web 8 后的 CXF 测试错误
ENTESB-20711	在 Fuse 7.11 中带有 TLS 1.3 的 camel-aws 2.23 组件出现任何问题？
ENTESB-20712	升级到 Karaf 4.4 和 Pax Web 8 后 Camel 测试错误
ENTESB-20720	多播不会返回聚合
ENTESB-20726	Hazelcast 升级似乎破坏 JCache 集成
ENTESB-20741	fuse 项目中使用的 javax/mail/mail 版本错误。
ENTESB-20742	log4j-slf4j18-impl 版本使用了 fuse 项目。
ENTESB-20754	[Hawtio] 在 Karaf 中无法登录
ENTESB-20826	CVE-2022-41966 xstream: Denial of Service （基于元素的哈希值提升一个堆栈溢出 [fuse-7]）注入递归集合或映射
ENTESB-20828	CXF - 服务器传输不正确
ENTESB-20829	[Karaf] JCE 无法验证供应商 BC
ENTESB-20831	在 json 文件中使用组化的 API 版本

问题	描述
ENTESB-20835	Karaf pax web - OPTIONS 方法没有公开
ENTESB-20836	Hibernate fuse 版本与 spring boot 冲突
ENTESB-20839	[Karaf] JMX ACL MBean 验证问题
ENTESB-20840	[Karaf] 10 功能无法安装
ENTESB-20841	SB1 格式的 Fuse archetype Spring Boot 属性
ENTESB-20842	camel-master 组件无法加载集群服务
ENTESB-20845	CVE-2023-1108 undertow: 在关闭 [fuse-7]期间 SslConduit 中的 Infinite 循环
ENTESB-20847	[Karaf] Jasypt 加密问题 JDK 17 和 RHEL8-FIPS
ENTESB-20850	[standalone] No response messages via fuse client
ENTESB-20851	[standalone] Colorised 命令在历史记录中
ENTESB-20853	[Fuse on Openshift] - Quickstarts 中的 Wrong Docker image reference
ENTESB-20854	[Fuse on Openshift] - Application templates - No tag "1.12" with image stream in fis-image-streams.json
ENTESB-20855	[Fuse on Openshift] - 在 EAP 镜像 JDK8/11 中的 Wrong WILDFLY 版本
ENTESB-20857	[Fuse on Openshift] - 应用程序模板 - 带有旧的 7.11 参考的模板
ENTESB-20859	[修补] Unable to patch 7.11 to 7.12
ENTESB-20862	[Karaf FoO] 无法使用客户端到 POD
ENTESB-20869	CVE-2023-20860 springframework: Security Bypass with Un-Prefixed Double Wildcard Pattern [fuse-7]
ENTESB-20870	CVE-2023-20861 springframework: Spring Expression DoS Vulnerability [fuse-7]
ENTESB-20871	Camel 2.23 测试不支持 jdk17
ENTESB-20872	WildFly Camel 5.10 测试不支持 jdk17
ENTESB-20873	CXF 3.3.6 测试不支持 jdk17

问题	描述
ENTESB-20950	[Karaf] Doesn't install features
ENTESB-20951	Camel Mail 组件不使用会话 URI 参数中的主机/端口信息
ENTESB-20956	CVE-2022-4492，确保 Syndesis 使用固定的 undertow
ENTESB-20957	CVE-2023-1108 undertow: 在关闭期间 SslConduit (fuse 在线)中的 Infinite 循环
ENTESB-20958	CVE-2022-41704 batik: Apache XML Graphics Batik 通过 SVG [fuse-7] 对代码执行受到攻击。
ENTESB-20959	CVE-2022-42890 batik: 在 Apache XML Graphics Batik [fuse-7] 中执行不受信任的代码
ENTESB-20960	CVE-2023-22602 shiro-core: shiro: 身份验证通过特殊的精心设计的 HTTP 请求 [fuse-7] 绕过。
ENTESB-20961	[Fuse On Openshift] QS spring-boot-camel-amq 包含一个已删除的镜像
ENTESB-20963	[Fuse On Openshift] QS Spring-Boot Camel Rest SQL 在 README 中报告错误的部署步骤
ENTESB-20964	[Fuse On Openshift] Adjust Pod metering label rht.prod_ver format
ENTESB-20967	[因为 SB 升级，在 Spring Cloud 上 [Fuse on Openshift] QS Spring-Boot Camel Config 会失败
ENTESB-20966	无法单独安装 karaf 功能
ENTESB-20968	[Fuse On Openshift] QS Spring-Boot Camel Rest SQL throws bad SQL grammar 异常
ENTESB-20969	[Fuse On Openshift] QS Spring-Boot Camel XA 会在 PostGresSQL 连接上抛出错误的 SQL grammar 异常
ENTESB-20971	Hawtio 控制台指标显示可用内存而不是使用
ENTESB-21045	无法安装 Pax-web-jetty 功能
ENTESB-21046	[Fuse standalone] Exception in log jdk11 and jdk17
ENTESB-21047	CVE-2023-20860，确保 Syndesis 使用固定的 springframework
ENTESB-21048	无法在 7.12 之上安装 CVE 补丁

问题	描述
ENTESB-21049	CVE-2022-41854，确保 Syndesis 使用固定 snakeyaml
ENTESB-21050	从 cxf-spring-boot-starter-jaxrs 中删除 org.apache.tomcat.embed 依赖项
ENTESB-21051	[Fuse On Openshift] QS Spring-Boot Camel-Drools, unable to create Kie Server
ENTESB-21053	[Fuse on Openshift] QS Spring Boot Camel Singleton，应用程序不会启动
ENTESB-21052	[Fuse on Openshift] - Karaf - Unable to resolve missing rquirement in acxf-jaxrs application
ENTESB-21056	CVE-2023-20861，确保 Syndesis 使用固定的 springframework
ENTESB-21057	CVE-2022-41946，确保 Syndesis 使用固定 jdbc-postgresql
ENTESB-21058	Karaf，一些捆绑包版本不是使用 karaf-bom 中指定的版本内联
ENTESB-21059	pax-url-aether 中的内存泄漏
ENTESB-21061	cxf 3.3.6 downstream 失败
ENTESB-21704	CVE-2023-20863 springframework: Spring Expression DoS Vulnerability [fuse-7]
ENTESB-21158	unattended Jolokia Queries Not working when Keycloak is Integrated for Access Control
ENTESB-21161	[Offliner] 文件无法使用 offliner 清单文件下载
ENTESB-21162	[Offliner] Missing artifacts
ENTESB-21163	Apicurito pod 包含带有不正确的值的 metering 标签
ENTESB-21168	CVE-2023-1370 json-smart: Un control Resource Consumption vulnerability in json-smart (Resource Exhaustion)[fuse-7]
ENTESB-21272	[Fuse on Openshift] Wrong version in Quickstart BOM
ENTESB-21273	删除或重构非工作快速入门 spring-boot-camel-soap-rest-bridge
ENTESB-21274	WildFly Camel 5.10.0 下游失败
ENTESB-21304	[Fuse on Openshift] - 使用 Karaf、jaxws 和 JDK17 对 java.xml 模块的 Illegal 访问，因为 xerces 软件包没有被公开

问题	描述
ENTESB-21309	[Fuse on Openshift] - 在 camel-jdbc on Karaf 中，无法从正文交换检索列
ENTESB-21310	camel-Velocity: Deprecation 警告
ENTESB-21311	springframework 缓存丢失的 TypeConverter，用户无法清理它
ENTESB-21316	[Fuse On Openshift] - Dismiss/Remove RHOSAK Quickstarts
ENTESB-21319	CVE-2022-31692 spring-security: Authorization 规则可以通过 forward 或在 Spring Security [fuse-7] 中包含分配程序类型来绕过。
ENTESB-21322	Karaf 捆绑包的无效限定符
ENTESB-21332	CVE-2023-20883 spring-boot: Spring Boot Welcome Page DoS Vulnerability [fuse-7]
ENTESB-21335	patch-maven-plugin 无法用于 Maven 3.9
ENTESB-21412	GitHub 上缺少 refs/tags
ENTESB-21415	[Fuse Standalone] Camel-chunk 功能缺少依赖项
ENTESB-21417	cxf 3.3.6 downstream 失败
ENTESB-21418	CVE-2023-1370，确保 Syndesis 使用固定的 json-smart
ENTESB-21419	[Karaf] Jasypt 加密问题 JDK 17 和 RHEL8-FIPS
ENTESB-21421	Camel 健康检查在 Spring Boot 运行时中有所变化

8.4. FUSE 7.12.1 中解决的错误

*下表列出了 **Fuse 7.12.1** 中已解析的错误。*

*表 **8.3. Fuse 7.12.1** 解决的错误*

问题	描述
ENTESB-21742	新的 Fuse 控制台部署在每年"openshift-service-serving-signer"证书轮转后无法正常工作。
ENTESB-21757	[JDG-4351][JBMAR-235] camel-infinispan 需要从 2.0.9.Final 到 2.0.11.Final 的 jboss-marshalling 更新。

问题	描述
ENTESB-21776	Openshift 镜像上的 Fuse 使用非常旧的 jmx_prometheus_javaagent.jar
ENTESB-21858	使用 JDK 11.0.20 时将不开始
ENTESB-21878	当日志记录处于 WARN 级别时，NullPointerException
ENTESB-21881	使用 -Dpatch 用于 Maven 3.9 的 patch-maven-plugin 的问题
ENTESB-22087	无法在 7.12 之上安装补丁 7.12.1
ENTESB-21763	带有 toD 的 camel-http4 无法在 Karaf 上工作
ENTESB-21865	6.3 和 7.11 之间的 pollEnrich 文件组件行为变化
CVE-2023-46604	CVE-2023-46604 activemq-openwire: OpenWire Module: Unbounded deserialization 会导致 ActiveMQ 受到远程代码执行(RCE)攻击 [fuse-7] 的影响。
CVE-2023-40167	CVE-2023-40167 jetty-http: jetty: Improper validation of HTTP/1 content-length [fuse-7]
CVE-2023-3223	CVE-2023-3223 undertow: OutOfMemoryError due due due to @MultipartConfig 处理 [fuse-7]
CVE-2023-36479	CVE-2023-36479 jetty-servlets: jetty: Improper added of quotation marks to user inputs in CgiServlet [fuse-7]
CVE-2023-39410	CVE-2023-39410 avro: apache-avro: Apache Avro Java SDK: Memory when deserialing untrusted data in Avro Java SDK [fuse-7]
CVE-2023-34034	CVE-2023-34034 spring-security: spring-security-webflux: 路径通配符会导致安全绕过 [fuse-7]
CVE-2023-44487	CVE-2023-44487 undertow: HTTP/2: 启用多个 HTTP/2 的 Web 服务器会受到 DDoS 攻击(Rapid Reset Attack)[fuse-7]
CVE-2023-36478	CVE-2023-36478 http2-hpack: jetty: hpack header 值会导致在 http/2 [fuse-7] 中拒绝服务
CVE-2023-41900	CVE-2023-41900 jetty-openid: jetty: OpenId Revoked 身份验证允许一个请求 [fuse-7]