Red Hat Fuse 7.12

Red Hat Fuse 7.12 のリリースノート

Red Hat Fuse の新機能

Last Updated: 2023-12-11

Red Hat Fuse 7.12 Red Hat Fuse 7.12 のリリースノート

Red Hat Fuse の新機能

法律上の通知

概要

本リリースノートは、Red Hat Fuse のリリース間で変更になった内容の概要を取り上げます。

目次

多様性を受け入れるオープンソースの強化

Red Hat では、コード、ドキュメント、Web プロパティーにおける配慮に欠ける用語の置き換えに取り組んでいます。まずは、マスター (master)、スレーブ (slave)、ブラックリスト (blacklist)、ホワイトリスト (whitelist) の 4 つの用語の置き換えから始めます。この取り組みは膨大な作業を要するため、今後の複数のリリースで段階的に用語の置き換えを実施して参ります。詳細は、Red Hat CTO である Chris Wright のメッセージ をご覧ください。

第1章 FUSE 7.12 の製品概要

1.1. FUSE のディストリビューション

Fuse 7.12 は、以下の 3 つのディストリビューションで提供されます。

Fuse スタンドアロン

複数のオペレーティングシステム上でサポートされる従来の Fuse ディストリビューションです。このディストリビューションは以下のコンテナータイプでサポートされます。

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

Fuse on OpenShift

OpenShift でインテグレーションアプリケーションを実行するための Fuse ディストリビューションです (Red Hat Enterprise Linux オペレーティングシステムでサポートされます)。このディストリビューションでは、サポートされるコンテナータイプは docker 形式のコンテナーイメージで提供されます。

- Java イメージ (Spring Boot 用)
- Apache Karaf イメージ
- JBoss EAP イメージ

Fuse Online

ブラウザーベースの UI を使用して簡単なワークフローにアクセスできる、インテグレーション初心者向けの Fuse ディストリビューションです。このディストリビューションは以下のようなデプロイメントで使用できます。

- OpenShift Dedicated (OSD) クラスター上
- オンプレミス Openshift クラスターのインストール

1.2. 重要事項

JUnit 4 から JUnit5 へのアップグレード

Red Hat Fuse 7.12 は、JUnit 4 を JUnit 5 にアップグレードする Spring Boot 2.7.x を使用します。Fuse Spring Boot BOM 7.12 を使用するすべてのプロジェクトは JUnit 5 に依存します。Fuse 7.x から Fuse 7.12 に移行する場合、Fuse on Spring Boot で実行されているユニットテストが Maven ビルドの一部として実行されなくなる可能性があります。これを解決するには、以下に示すように、関連する依存関係を **maven-surefire-plugin** 設定に追加します。

```
<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>
```

JUnit4 からの移行の詳細は、Migrating from JUnit 4 を参照してください。

CVE-2020-8908 guava

30.0 より前のバージョンの Guava には、一時ディレクトリー作成の脆弱性が存在します。Guava をバージョン 30.0 以降に更新するか、Java 7 以降に更新するか、どちらも不可能な場合は、ディレクトリーの作成後にパーミッションを明示的に変更することを推奨します。

Red Hat CodeReady Studio 廃止予定

Red Hat CodeReady Studio は廃止が予定されています。JBoss Tools (コミュニティー) が後続のツールキットです。

1.3. サポートされる構成

重要

Apache Karaf で Fuse を実行する場合は、OpenJDK 8u282 または OpenJDK 8u302 が推奨されます。クレデンシャルストアに影響を及ぼす既知の問題がある OpenJDK 8u292 は使用しないでください (ENTESB-16417 を参照)。OracleJDK 1.8.0_291 もこの問題の影響を受けます。

バージョン 7.12 でサポートされる設定、標準仕様、およびコンポーネントに関する詳細は、以下のカスタマーポータルの記事を参照してください。

- Red Hat Fuse でサポートされる設定
- Red Hat Fuse でサポートされる標準
- Red Hat Fuse コンポーネントの詳細

第2章 FUSE ONLINE

Fuse Online は、コードを作成せずに複数の異なるアプリケーションやサービスの統合を可能にする Web ブラウザーインターフェイスを提供します。また、複雑なユースケースで必要な場合にコードを追加できる機能も提供します。

Fuse Online では、OpenShift のインテグレーションは Apache Camel を使用する Spring Boot として実行されます。

2.1. FUSE ONLINE ディストリビューション

Fuse Online は Red Hat の Web ベースのインテグレーションプラットフォームです。Syndesis は Fuse Online のオープンソースプロジェクトです。Fuse Online は以下のような OpenShift 環境で実行されます。

ホスト環境	インストール
OpenShift Dedicated	Red Hat が Red Hat インフラストラクチャーに Fuse Online をインストールし、提供します。
OpenShift Container Platform	お客様がインストールし、管理します。

2.2. FUSE ONLINE 7.11.X から 7.12.1 へのアップグレードには手動のアップグレード手順が必要です。

Fuse Online 7.11.x をインストールし、Fuse Online 7.12.x.x にアップグレードする場合、Fuse Online 7.12.x.0 に手動でアップグレードする必要があります。

1. OpenShift Container Platform Web コンソールの **Administrator** パースペクティブで、**Operators** > **Installed Operators** に移動します。
2. **Red Hat Integration Fuse Online 7.11.2** Operator をクリックします。
3. **Subscription** タブをクリックします。
4. **Update approval** が **Manual** に設定されていることを確認します。
   - **Update approval** が **Manual** に設定されている場合には、次の手順に進みます。
   - **Update approval** が **Automatic** に設定されている場合は、以下を実行します。
     a. **Automatic** をクリックします。
     b. **Change Update Approval Strategy** ダイアログで **Manual** を選択し、**Save** をクリックします。
5. **Update channel** で **7.11.2** をクリックします。
6. **Change subscription update channel** で **7.12.x** を選択します。
   注記: latest、**candidate**、および **stable** チャネルは、テクノロジープレビュー機能です。
7. **Upgrade status** で **Upgrade available** をクリックします。

8. **Preview InstallPlan** をクリックしてから、**Approve** をクリックします。
9. Operator が Fuse Online 7.12.0 へのアップグレードを完全に完了していることを確認します。
    a. **Operators** > **Installed Operators** ページに移動し、**Red Hat Integration Fuse Online** をクリックします。**Operator Details** ページが開きます。
    b. **Syndesis** タブを選択します。Fuse Online インスタンスのステータス (デフォルト名は **app**) は、最初に **Installed** を表示します (Fuse Online 7.12.0 がインストールされていることを示すため)。続いて、いくつかのフェーズ (**Installing**、**Starting**、および **Installed**) に進みます。**Installed** フェーズ に再び到達すると、7.12.0 へのアップグレードが完了します。
10. **Operators** > **Installed Operators** ページに戻り、**Red Hat Integration Fuse Online** Operator の **Upgrade available** をクリックします。
11. **Preview InstallPlan** をクリックしてから、**Approve** をクリックします。
12. Operator が Fuse Online 7.12.x へのアップグレードを完全に完了していることを確認します。
    a. **Networking** > **Routes** に移動してから、**syndesis** の場所リンクをクリックして、Fuse Online Web コンソールを開きます。
    b. Fuse Online コンソールの右上隅にある **?** アイコンをクリックしてから **About** を選択します。
    c. **About** ページのバージョン番号に **7_12_x** が含まれていることを確認します。

2.3. FUSE ONLINE インテグレーションのアップグレード

オンサイトの OCP で稼働している Fuse Online 環境をアップグレードするには、OCP での Fuse Online のアップグレード の説明どおりに、Operator を使用して、稼働中のインテグレーションを再パブリッシュすることで Fuse Online を更新する必要があります。

OCP 4.9 以降では、Operator を使用して 7.11 にアップグレードすると、Fuse Online Operator のアップグレードプロセス中に以下の警告が表示されます。

W1219 18:38:58.064578 1 warnings.go:70] extensions/v1beta1 Ingress is deprecated in v1.14+, unavailable in v1.22+; use networking.k8s.io/v1 Ingress

この警告は、クライアント (Fuse Online が Kubernetes/OpenShift API 初期化コードに使用する) が非推奨の Ingress バージョンにアクセスするために表示されます。この警告は、非推奨の API が完全に使用されていることを示すものでは **なく**、Fuse Online7.11 へアップグレードすることに問題はありません。

2.4. FUSE ONLINE での重要事項

Fuse Online ディストリビューションの Fuse 7.12 リリースにおける重要事項

- Fuse 7 が現在メンテナンスサポート中であるため、Fuse Online のサポートは非推奨になりました。Fuse 7 のサポートが終了すると、Fuse Online の今後の開発は行われません。
- Fuse Online のインストールは、OCP 3.11 ではサポート対象外となります。
- Fuse Online は Camel K ランタイムまたは KNative コネクターをサポートしなくなりました。

- Fuse Online が Red Hat インフラストラクチャーにインストールされ、プロビジョニングされる場合、アカウントは同時に実行可能な特定数のインテグレーションに制限されます。詳細は、価格プランを参照してください。

- Fuse Online にアップロードする OpenAPI スキーマに出入力タイプが定義されていないことがあります。Fuse Online が出入力タイプを指定しない OpenAPI からカスタム API クライアントを作成した場合、API クライアントが処理できるフィールドにインテグレーションデータをマップするインテグレーションや、API クライアントが処理したフィールドから統合データをマップするインテグレーションを作成できません。インテグレーションにカスタム API をマップ先またはマップ元とするマッピングが必要な場合、OpenAPI スキーマをアップロードするときに **Review/Edit** をクリックして API 編集ツールの API Designer を開き、出入力タイプの指定を追加します。

- Fuse 7.8 以降、カスタム API クライアントコネクターまたは API プロバイダーインテグレーションに使用する OpenAPI ドキュメントは、循環スキーマ参照を持つことができません。たとえば、リクエストまたは応答ボディーを指定する JSON スキーマは、そのスキーマ自体を全体的に参照することはできず、任意数の中間スキーマを介してそれ自体を部分的に参照することもできません。

- OCP 4.9 (またはそれ以降) では、**application-monitoring** プロジェクトは機能しなくなりました。これは、Prometheus および Grafana で Fuse Online インテグレーションおよびインフラストラクチャーコンポーネントを監視するための前提条件です。
この問題を回避するには、(**openshift-monitoring** namespace で) ビルトインのモニタリングスタック を使用して **openshift-user-workload-monitoring** 機能および **grafana-operator** を使用し、以下の **OCP 4.9 (またはそれ以降) に Fuse Online 監視リソース (Prometheus および Grafana) を追加する** の手順の説明にあるように、**ops addon** を使用します。

2.4.1. OCP 4.9 (またはそれ以降) に Fuse Online 監視リソース (Prometheus および Grafana) を追加する

前提条件

- Fuse Online は、オンサイトで OCP 4.9 (またはそれ以降) にインストールされ、実行されている。

- **oc** クライアントツールがインストール済みであり、Fuse Online がインストールされている OCP クラスターに接続されている。

- OCP クラスターへの **admin** アクセスがある。

- Fuse Online インストールが **ops addon** が有効になっている状態で設定されている。必要に応じて、以下のコマンドで有効にすることができます。

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

手順

1. 既存の **openshift-monitoring** 設定がある場合は、手順 2 に進みます。
それ以外の場合には、ユーザーワークロードモニタリングオプションを **true** に設定する **openshift-monitoring** 設定を作成し、手順 3 に進みます。

```
oc apply -f - <<EOF
apiVersion: v1
kind: ConfigMap
metadata:
```

```
  name: cluster-monitoring-config
  namespace: openshift-monitoring
data:
  config.yaml:
   enableUserWorkload: true
EOF
```

2. 既存の **openshift-monitoring** 設定がある場合:

   a. 既存の **openshift-monitoring** 設定をチェックして、**ユーザーワークロードモニタリング** オプションが **true** に設定されるかどうかを判別します。

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

   結果が **enableUserWorkload: true** の場合、**ユーザーワークロードモニタリング** オプションは **true** に設定されます。ステップ 3 に進みます。

   結果に他の設定が表示される場合には、次の手順に進み、ConfigMap を編集してユーザーワークロードの監視を有効にします。

   b. 以下のようにエディターで ConfigMap ファイルを開きます。

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

   c. **enableUserWorkload** を **true** に設定します。以下に例を示します。

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

   d. ConfigMap ファイルを保存します。

3. 以下のコマンドを使用して、**openshift-user-workload-monitoring** namespace の Pod のステータスを確認します。

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

   Pod のステータスが Running になるまで待機します。以下に例を示します。

   ```
   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. Prometheus で Fuse Online のアラートルールが有効になっていることを確認します。

   a. 内部 prometheus インスタンスにアクセスします。

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

b. ブラウザーを開いて **localhost:9090** にアクセスします。

c. **Status**> **Targets** の順に選択します。3 つの **syndesis** エンドポイントが表示されるはずです。

d. **CTRL-C** を押して、**port-forward** プロセスを終了します。

5. OperatorHub から、Grafana Operator 4.1.0 を選択した namespace(例:**grafana-middleware** namespace) にインストールします。

6. クラスターロールとクラスターロールのバインディングを追加して、**grafana-operator** がノードおよび namespace をリスト表示できるようにします。

a. **grafana-operator** Web サイトからクラスターロール YAML ファイルをダウンロードします。

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

b. **grafana-operator** のクラスターパーミッションを追加して、他の namespace およびノードを読み取ります。

```
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. **DASHBOARD_NAMESPACES_ALL** 環境変数を使用して namespace を制限することで、**grafana-operator** が他の namespace から Grafana ダッシュボードを読み取れるようにします。

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

8. **grafana** Pod が再作成されていることを確認します。

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

9. 必要に応じて、**grafana-operator** ログを表示します。

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

10. Grafana カスタムリソース を追加して、以下のように Grafana サーバー Pod を起動します。

```
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. **grafana-operator** がモニタリング情報を読み取ることを許可します。

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

12. **GrafanaDatasource** を追加して、**thanos-querier** をクエリーします。

```
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. grafana サーバーログを表示します。

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

14. grafana URL にアクセスし、Fuse Online ダッシュボードを表示します。

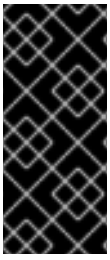
```
echo "https://"$(oc -n grafana-middleware get route/grafana-route -ojsonpath='{.spec.host}')
```

2.5. FUSE ONLINE のテクニカルサポートの利用

テクニカルサポートを利用するには、Fuse Online コンソールの左ナビゲーションパネルで **Support** をクリックします。**Support** ページを使用して、すべてのインテグレーションに関する診断情報や、選択した 1 つまたは複数のインテグレーションに関する診断情報をダウンロードします。このページには、サポートチケットを作成するためのリンクや、ダウンロードした診断情報を提供するためのリンクもあります。

2.6. FUSE ONLINE のテクノロジープレビュー機能

本リリースには、以下に示すテクノロジープレビュー機能が含まれています。



重要

テクノロジープレビューの機能は、Red Hat の本番環境のサービスレベルアグリーメント (SLA) ではサポートされず、機能的に完全ではないことがあるため、Red Hat は本番環境での使用は推奨しません。テクノロジープレビューの機能は、最新の技術をいち早く提供して、開発段階で機能のテストやフィードバックの収集を可能にするために提供されます。詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

- **Fuse Online の監査**
  Fuse Online は、ユーザーが以下の Fuse Online コンポーネントに対して加えた変更の基本監査をサポートします。

  - **コネクション** - **Name** および Fuse Online Web コンソールのコネクターの **Details** ページに表示されるその他のフィールド。
  - **コネクター** - **Name** フィールド。
  - **インテグレーション** - **Name** フィールド。

- データフィールドをマッピングするための条件式
  データマッパーでは、条件式を指定し、データマッピングに適用することができます。たとえば、条件式はソースフィールドの評価や、ソースフィールドが空の場合にターゲットフィールドに入力する方法を指定できます。指定できる式の限定セットは、Microsoft Excel の式に似ています。

- **データマッパーのユーザー定義プロパティーのドキュメント範囲**
  データマッパーでは、ソースとターゲットのマッピングに定義されたプロパティーの範囲を指定できます。**Mapping Details** パネルで、**Properties** の横にある **Add** (+) をクリックします。新しい **Scope** オプションの**Create Property** ダイアログで、現在のメッセージヘッダー、前のステップからのメッセージヘッダー、または Camel 固有のプロパティーの **Camel Exchange Property** を選択できます。

- **OAuth を使用する REST API クライアントでは**、API クライアントコネクターの作成時に、そのコネクターから作成するコネクションのデフォルト OAuth2 の動作を変更することができます。OpenAPI 仕様への Fuse Online ベンダーエクステンションは以下をサポートします。

  - クライアントクレデンシャルをパラメーターとして提供。
  - HTTP レスポンスステータスコードを基にした新しいアクセストークンの取得。

第3章 FUSE ON OPENSHIFT

Fuse on OpenShift は、OpenShift Container Platform での Fuse アプリケーションのデプロイを可能にします。

3.1. OPENSHIFT のサポート対象バージョン

Fuse on OpenShift と使用する OpenShift Container Platform のサポート対象バージョンについては Red Hat Fuse でサポートされる設定 を参照してください。

3.2. サポートされるイメージ

Fuse on OpenShift は以下の Docker 形式のイメージを提供します。

Image	プラットフォーム	サポート対象のアーキテクチャー
fuse7/fuse-java-openshift-rhel8	Spring Boot	AMD64 および Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk11-rhel8	Spring Boot	AMD64 および Intel 64 (x86_64)
fuse7/fuse-java-openshift-jdk17-rhel8	Spring Boot	AMD64 および Intel 64 (x86_64)
fuse7/fuse-java-openshift-openj9-11-rhel8	Spring Boot	IBM Z および LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-karaf-openshift-rhel8	Apache Karaf	AMD64 および Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk11-rhel8	Apache Karaf	AMD64 および Intel 64 (x86_64)
fuse7/fuse-karaf-openshift-jdk17-rhel8	Apache Karaf	AMD64 および Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk8-rhel7	Red Hat JBoss Enterprise Application Platform	AMD64 および Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk11-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 および Intel 64 (x86_64)
fuse7/fuse-eap-openshift-jdk17-rhel8	Red Hat JBoss Enterprise Application Platform	AMD64 および Intel 64 (x86_64)
fuse7/fuse-console-rhel8	Fuse console	AMD64 および Intel 64 (x86_64) IBM Z および LinuxONE (s390x) IBM Power Systems (ppc64le)

Image	プラットフォーム	サポート対象のアーキテクチャー
fuse7/fuse-console—rhel8-operator	Fuse console operator	AMD64 および Intel 64 (x86_64) IBM Z および LinuxONE (s390x) IBM Power Systems (ppc64le)
fuse7/fuse-apicurito-generator-rhel8	Apicurito REST アプリケーションジェネレーター	AMD64 および Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8	Apicurito REST API エディター	AMD64 および Intel 64 (x86_64)
fuse7/fuse-apicurito-rhel8-operator	API Designer Operator	AMD64 および Intel 64 (x86_64)

3.3. FUSE 7.12 ON OPENSHIFT の新機能

Fuse on OpenShift のバージョン 7.12 では、以下の新機能が提供されます。

- JDK 17 のサポート
  Fuse 7.12 は、JDK17 を使用して Fuse on OpenShift クイックスタートを構築するためのサポートを提供します。

- **openshift-maven-plugin** を使用したクイックスタートの実行
  Fuse 7.12 は、Maven アーキタイプで Fuse on OpenShift クイックスタートをビルドして実行する際に、新しい **openshift-maven-plugin** を使用します。

- IBM Power Systems、IBM Z、および LinuxONE へのサポート
  Fuse 7.12 は、Red Hat OpenShift Container Platform 4.10 以降で、IBM Power Systems(ppc64le)、IBM Z、および LinuxONE (s390x) のサポートを追加します。

注記

Fuse 7.12 では、Fuse on OpenShift イメージストリームおよびテンプレートを IBM Power Systems、IBM Z、および LinuxONE へインストールすることは、**サポートされていません**。Fuse on OpenShift Operator でインストールできるコンポーネントのみが IBM Power Systems、IBM Z、および LinuxONE でサポートされます。

3.4. 重要事項

Fuse on OpenShift ディストリビューションの Fuse 7.12 リリースにおける重要事項

OpenShift Container Platform (OCP) 4.11 以降での Fuse 7.12 のサポート

Fuse 7.12 には、OpenShift Container Platform (OCP) 4.11 以降と連携できるようにする更新が含まれています。OCP 4.11 にアップグレードする場合は、OCP をバージョン 4.11 にアップグレードする **前** に、Fuse をバージョン 7.12 にアップグレードする必要があります。以前のバージョンの Fuse (7.10 より前) は OCP 4.9 以降をサポートしません。

Data Virtualization の削除

Data Virtualization は Fuse 7.7 で非推奨となり、Fuse 7.8 から削除されました。

Spring Boot 1 の削除

Spring Boot 1 は Fuse 7.7 で非推奨となり、Fuse 7.8 から削除されました。Spring Boot 2.0 Migration Guide の説明にしたがって、Spring Boot アプリケーションを Spring Boot 2 に移行することが推奨されます。

Fabric8 Maven プラグインの削除

Fabric8 Maven プラグインは Fuse 7.10 から完全に削除され、Fuse 7.10 以降は OpenShift Maven プラグイン に置き換えられています。OpenShift Maven プラグインを使用してアプリケーションをビルドおよびデプロイします。

JDK11 を使用したクイックスタートの実行

ランタイム時に JDK11 ベースのイメージを使用する場合は、コンパイル時に正しい JDK11 プロファイルを使用します。JDK11 を使用してクイックスタートをビルドおよびデプロイする場合は、ビルドマシンに JDK11 をインストールし、正しい JDK11 プロファイルを使用してクイックスタートをビルドするようにしてください。

Spring Boot アーティファクト ID の変更

Fuse 7.12 では、Spring Boot が 2.7.12 にアップグレードされています。

Spring -Boot RHOSAK のクイックスタートが spring -boot のアップグレードが原因で失敗する

eap-camel-jpa クイックスタートの削除

依存関係の問題により、**eap-camel-jpa** クイックスタートが Fuse 7.8 から削除されました。

Fuse7.8 以降、外部から Jolokia にアクセスできない

Fuse 7.8 より、Jolokia のデフォルトプロトコルは HTTP から HTTPS に変更されました。

FIPS 対応の Jolokia エージェントは使用不可になる

OCP FIPS 対応 Jolokia エージェントは、セキュリティーエンコーディングがサポートされていないため、使用できなくなります。

第4章 FUSE スタンドアロン

4.1. サポートされるコンテナー

Fuse スタンドアロン 7.12 は以下のランタイムコンテナーでサポートされます。

- Spring Boot 2 (スタンドアロン)
- Apache Karaf
- Red Hat JBoss Enterprise Application Platform (JBoss EAP)

4.2. FUSE 7.12 の新機能

Fuse スタンドアロンのバージョン 7.12 の主な新機能は次のとおりです。

Java 17 のサポート

Fuse 7.12 リリースは、Java 17、Java 11、および Java 8 をサポートします。

4.3. テクノロジープレビューの機能

以下の Fuse スタンドアロンの機能は **テクノロジープレビュー** であるため、Fuse 7.12 ではサポートされません。

Saga EIP

Saga EIP (Enterprise Integration Pattern) はテクノロジープレビューの機能で、実稼働環境に適していない **インメモリー** Saga サービスのみが対象になります。LRA Saga サービスはサポート **されません**。詳細は Apache Camel Development Guide の Saga EIP を参照してください。

4.3.1. Apache Camel の Fuse Tooling サポート

Fuse Tooling は、Apache Camel 言語サポートエクステンションや、Visual Studio Code、Eclipse IDE、および Eclipse Che のプラグインを使用して、Camel アプリケーションの開発でクロスプラットフォームおよびクロス IDE を提供します。

Visual Studio Code の機能

注記

VS Code Apache Camel エクステンションはコミュニティー機能です。これらは Red Hat ではサポートされません。

Language Support for Apache Camel エクステンションは、以下のような Camel URI の機能を提供します。

XML DSL および Java DSL の場合:

- VS Code の **Outline** パネルおよび **Go > Go to Symbol in File**ナビゲーションパネルで、エンドポイントに移動できます。
- エディターは入力時に Camel コンポーネント、属性、および属性値のリストでコード補完を提供します。

- Camel コンポーネントにマウスオーバーすると、エディターにコンポーネントの簡単な説明が表示されます (Apache Camel component reference から)。
- ファイルを編集すると、エディターは Camel コードで Apache Camel 検証チェックを実行します。
- **File → Preferences → Settings → Apache Camel Tooling → Camel catalog version**と選択すると、特定の Camel Catalog 指定できます。
- Quick fix(クリック修正) 機能を使用して、無効な列挙値や未知の Camel URI コンポーネントプロパティーに対応できます。

XML DSL の場合のみ:

- VS Code の **Outline** パネルおよび **Go > Go to Symbol in File**ナビゲーションパネルで、Camel コンテキストおよびルートに移動できます。
- エディターは入力時に **direct**、**direct VM**、**VM**、および **SEDA** コンポーネントの参照された ID に対し、コード補完を提供します。
- 開いているすべての Camel ファイルで **direct** および **direct VM** コンポーネントの参照を見つけることができます。

プロパティーの場合:

- Camel コンポーネントプロパティーの完了
- 診断

Language Support for Apache Camel機能にアクセスするには、エクステンションを 1 つ以上追加します。

Apache Camel Extension Pack によって以下の VS Code エクステンションがインストールされます。

- 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

エクステンションを個別にインストールすることもできます。

詳細は、以下の README ファイルを参照してください。

- Apache Camel Extension Pack の README ファイル。

- Apache Camel Language Server Protocol for Visual Studio Code の README ファイル。
- AtlasMap Data Transformation エディター の README

Eclipse IDE 機能

Language Support for Apache Camel Eclipse プラグインは Camel URI に以下の機能を提供します。

XML DSL および Java DSL 両方の汎用 Eclipse テキストエディターの場合:

- エディターは入力時に Camel コンポーネント、属性、および属性値のリストでコード補完を提供します。
- Camel コンポーネントにマウスオーバーすると、エディターにコンポーネントの簡単な説明が表示されます (Apache Camel component reference から)。

Language Support for Apache Camel機能にアクセスするには、Eclipse Marketplace から Eclipse プラグインをインストールします。詳細は、Apache Camel Language Server Protocol for Eclipse IDE の README file を参照してください。

Eclipse Che の機能

Eclipse Che 7 の **Language Support for Apache Camel**プラグインは、XML DSL および Java DSL で Camel URI の機能を提供します。

- エディターは入力時に Camel コンポーネント、属性、および属性値のリストでコード補完を提供します。
- Camel コンポーネントにマウスオーバーすると、エディターにコンポーネントの簡単な説明が表示されます (Apache Camel component reference から)。
- ファイルを保存すると、エディターによって Camel コードで Apache Camel 検証チェックが実行されます。

Eclipse Che に対してこのプラグインをアクティベートするには、Apache Camel based on Spring Boot スタックまたはワークスペース設定を使用します。

4.4. FUSE 7.12 の BOM ファイル

サポートされる Fuse 7.12 アーティファクトを使用するために Maven プロジェクトを設定するには、本セクションで説明する BOM バージョンを使用してください。

4.4.1. Fuse 7.12 の BOM ファイル

Fuse スタンドアロンアプリケーションをアップグレードして 7.12 の依存関係を使用するには、Maven の **pom.xml** を編集し、下表にある BOM と Maven プラグインのバージョンを変更します。

表4.1 Maven BOM および BOM を使用した 7.12 のプラグインバージョン

コンテナータイプ	Maven BOM またはプラグインアーティファクト groupId/artifactId	Fuse 7.12 向けのバージョン
Spring Boot 2	**org.jboss.redhat-fuse/fuse-springboot-bom**	**7.12.0.fuse-7_12_0-00016-redhat-00001**

コンテナータイプ	Maven BOM またはプラグインアーティファクト groupId/artifactId	Fuse 7.12 向けのバージョン
	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**

BOM の使用に関する詳細は Migration Guide を参照してください。

4.4.2. Fuse 7.12.1 の BOM ファイル

サポートされる Fuse 7.12.1アーティファクトを使用するために Maven プロジェクトを設定するには、このセクションで説明する BOM バージョンを使用してください。

表4.2 Maven BOM および BOM を使用した 7.12.1 のプラグインバージョン

コンテナータイプ	Maven BOM またはプラグインアーティファクト groupId/artifactId	Fuse 7.12.1 向けのバージョン
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**

BOM の使用に関する詳細は Migration Guide を参照してください。

4.5. 重要事項

Fuse スタンドアロンディストリビューションの Fuse 7.12 リリースにおける重要事項

Java 17 のサポート

Fuse 7.12 リリースは、Java 17、Java 11、および Java 8 をサポートします。

Karaf ランタイムと JBoss EAP のサポートは非推奨になる

Fuse7.12 のリリースに伴い Fuse7 のサポートが終了するため、Karaf ランタイムと JBoss EAP のサポートは非推奨になりました。

MongoClients ファクトリーを使用した MongoDB への接続の作成

Fuse 7.10 以降、**com.mongodb.MongoClient** の代わりに **com.mongodb.client.MongoClient** を使用して、MongoDB への接続を作成します (フルパスの追加の **.client** サブパッケージに注意してください)。
これは、**camel-mongodb** を使用するすべてのユーザーアプリケーションに影響します。この場合、接続 Bean を **com.mongodb.client.MongoClient** インスタンスとして作成する必要があります。さらに、このクラスで公開されるメソッドは古いクラスとまったく同じではありません。そのため、ユーザーコードのリファクタリングがより多く必要になる場合があります。

たとえば、以下のように MongoDB へのコネクションを作成します。

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

以下の例のように MongoClient Bean を作成できます。

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

第5章 非推奨となった機能および削除された機能

Fuse 7 の今後の変更に関するご質問やヘルプは、support@redhat.com にお問い合わせください。

5.1. 非推奨

以下の機能は Fuse 7.12 で非推奨となったため、今後のリリースで削除される可能性があります。

Fuse Online のサポートは非推奨です

Fuse 7 が現在メンテナンスサポート中であるため、Fuse Online のサポートは非推奨になりました。Fuse 7 のサポートが終了すると、Fuse Online の今後の開発は行われません。

Karaf OSGi ランタイムと JBoss Enterprise Application Platform (EAP) のサポートが非推奨になる

2024 年 6 月 30 日に Fuse7 のサポートが終了するのに伴い、Karaf OSGi ランタイムと JBoss Enterprise Application Platform (EAP) のサポートは終了します。Fuse 7 のサポートが終了すると、Karaf OSGi または JBoss EAP で Camel はサポート対象外になります。

OpenWire プロトコルが非推奨となる

Fuse 7.10 以降、OpenWire プロトコル (AMQ ブローカーインスタンスの接続に使用可能) の使用は非推奨になりました。OpenWire プロトコルは、AMQ Broker バージョン 7.9.0 以降 AMQ Broker でも非推奨になることに注意してください。

wsdl2rest ツールが非推奨となる

Fuse 7.10 以降、**wsdl2rest** コマンドラインツールは非推奨となりました。VS Code の WSDL 2 Camel Rest DSL エクステンションも非推奨となりました。

OCP 4 インストールの Fuse Online インストールスクリプト

Fuse 7.8 より OpenShift Container Platform (OCP) 4.x バージョン上に Fuse Online をインストールする場合に Fuse Online のインストールスクリプトは非推奨となりました。OCP 4.x バージョンでは、Fuse Online Operator の使用が推奨されます。

Camel アプリケーションで非推奨となった PHP、Python、および Ruby スクリプト言語

PHP、Python、および Ruby スクリプト言語は、Fuse 7.4 より Camel アプリケーションで非推奨となり、今後のリリースで削除される予定です。Camel コミュニティーでは、Camel 2.19 より PHP、Python、および Ruby が非推奨になりました (CAMEL-10973 を参照)。これは、Apache Karaf、JBoss EAP、および Spring Boot のすべての Fuse コンテナータイプに適用されます。

非推奨となった HP-UX OS

HP-UX オペレーティングシステムは Fuse 7.2 より非推奨となり、このオペレーティングシステムのサポートは Fuse の今後のリリースで除外される可能性があります。JBoss EAP 7.2 コンテナーではすでに HP-UX のサポートが除外されたため、JBoss EAP 7.2 で実行される Fuse on JBoss EAP の今後のバージョンは HP-UX ではサポート**されません**。

非推奨となった Camel MQTT コンポーネント

Camel MQTT コンポーネントは Fuse 7.0 で非推奨となり、Fuse の今後のリリースでは削除されます。このコンポーネントの代わりに、Eclipse Paho ライブラリーを使用して MQTT メッセージングプロトコルをサポートする Camel Paho コンポーネントを使用できます。

Linux 以外のオペレーティングシステムで非推奨となった Camel LevelDB コンポーネント

Camel LevelDB (**camel-leveldb**) コンポーネントは、Fuse 6.3 より Red Hat Enterprise Linux 以外のすべてのオペレーティングシステムで非推奨となりました。今後、Camel LevelDB コンポーネントは Red Hat Enterprise Linux でのみサポートされます。

非推奨となった Camel SJMS コンポーネントからの BatchMessage クラス

Camel SJMS コンポーネントからの BatchMessage クラスは Fuse 7 で非推奨となり (Apache Camel ではバージョン 2.17 より非推奨)、Apache Camel および Fuse の今後のバージョンで削除される可能性があります。

5.2. FUSE 7.11 で削除された機能

OCP 3.11 での Fuse Online のインストール

OCP 3.11 への Fuse Online 環境 7.12 のインストールはサポートされていません。OCP 3.11 への Fuse Online のインストールに関して、Fuse Online のインストールスクリプトは完全に削除されます。

RSA/SHA-1 暗号は camel-ftp および camel-ssh によってデフォルトでサポートされない

Fuse 7.11 から、**camel-ftp** および **camel-ssh** コンポーネントは、デフォルトで RSA/SHA-1 暗号を使用した TLS をサポートしなくなりました。JSch ライブラリーに依存する他の Camel コンポーネントも影響を受ける可能性があります。
詳細は、Red Hat カスタマーポータルの記事 を参照してください。

5.3. FUSE 7.10 で削除された機能

fabric8-maven-plugin

fabric8-maven-plugin は Fuse 7.10 から完全に削除されました。Fuse on OpenShift で Maven プロジェクトをビルドおよびデプロイに代わりに **openshift-maven-plugin** を使用することが推奨されます。プラグインは Eclipse JKube によって維持され、プラグインに関する幅広い ドキュメント が提供されます。

5.4. FUSE 7.8 で削除された機能

Spring Boot 1

Spring Boot 1 は Fuse 7.8 ではサポート対象外になりました。Spring Boot 2.0 Migration Guide の説明にしたがって、Spring Boot アプリケーションを Spring Boot 2 に移行することが推奨されます。

Fuse Online の Camel K ランタイム

Fuse Online の Camel K ランタイム (テクノロジープレビュー機能) は Fuse 7.8 ではサポート対象外になりました。

7.8 で削除された Camel XmlJson コンポーネント

Camel XmlJson(**camel-xmljson**) コンポーネントは Fuse 7.8 で削除されました。

5.5. FUSE 7.5 で削除された機能

以下の機能は Fuse 7.5 で削除されました。

7.5 で廃止された MS SQL Server 2014 とのインテグレーションに対するサポート

MS SQL Server 2014 の Fuse 7.5 とのインテグレーションはテストおよびサポート対象外になりました。代わりに、MS SQL Server 2016 や 2017 などのより最近のバージョンの MS SQL Server を使用することが推奨されます。

7.5 で削除された Camel LinkedIn コンポーネント

camel-linkedin コンポーネントは Fuse 7.5 で削除されました。

重要

Fuse 7.5 で削除された **cam el-linkedin** コンポーネントは、今後のリリースで復元される可能性があります。

5.6. FUSE 7.3 で削除された機能

以下の機能は Fuse 7.3 で削除されました。

7.3 で削除された Camel YQL コンポーネント

Camel YQL コンポーネントは Fuse 7.3 で削除されました。

7.3 で削除された OpenJPA および OpenJPA3 Karaf 機能

openjpa 機能および **openjpa3** 機能は、7.3 の Apache Karaf コンテナーから削除されました。Java Persistence Architecture (JPA) 実装では、代わりにサポートされる **hibernate** 機能を使用してください。

7.3 で削除された camel-jetty Karaf 機能

camel-jetty 機能は Jetty 8 を使用するため、7.3 の Apache Karaf コンテナーから削除されました。この代わりに **camel-jetty9** 機能を使用してください。

7.3 で削除された pax-jms-oracleaq Karaf 機能

サードパーティーの無償ではない Oracle AQ ライブラリーが必要なため、**pax-jms-oracleaq** 機能は 7.3 の Apache Karaf コンテナーから削除されました。

7.3 の Fuse on EAP (Wildfly Camel) から削除された camel-elasticsearch コンポーネント

camel-elasticsearch コンポーネントは 7.3 の Fuse on EAP (Wildfly Camel) から削除されました。代わりに新しい **camel-elasticsearch-rest** コンポーネントを使用してください。

5.7. FUSE 7.2 で削除された機能

以下の機能は Fuse 7.2 で削除されました。

7.2 で削除された Camel XMLRPC コンポーネント

Camel XMLRPC コンポーネントは Fuse 7.2 で削除されました。

7.2 で削除された Camel Netty コンポーネント

Camel Netty コンポーネントは Fuse 7.2 で削除されました。この代わりに Camel Netty4 コンポーネントを使用することが推奨されます。

5.8. FUSE 7.0 で削除された機能

以下の機能は Fuse 7.0 で削除されました。

7.0 でサポートが除外された Red Hat JBoss Operations Network (JON)

Fuse 7.0 より Fuse on Karaf は JON をサポートしなくなり、JON ランタイムと統合するための JON プラグインの提供を停止しました。

7.0 で削除された組み込み ActiveMQ ブローカー

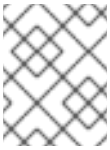
Fuse 7.0 より Fuse on Karaf は組み込み ActiveMQ ブローカーの提供を停止しました。そのため、サポートされるリモートブローカーへ直接接続するようにしてください。サポートされるブローカーの詳細は Red Hat Fuse でサポートされる設定 のサポートされるメッセージングプロバイダーを参照してください。

7.0 で削除された Fuse インテグレーションパック

ルールやプロセスの実行に対するサポートは、Red Hat JBoss BPM Suite および Red Hat JBoss BRMS に含まれるコンポーネントによって提供されます。

7.0 で削除された子コンテナー管理用の Karaf コンソールコマンド

Fuse 7.0 より、子コンテナー管理用の Karaf コンソールコマンドはサポートされて **いません**。対象となる **instance:** (Karaf 4.x 構文) で始まるコンソールコマンドと、 **admin:** (Karaf 2.x 構文) で始まるコンソールコマンドはサポートされません。



注記

Fuse 7.0 GA リリースでは、**instance:** コマンドは削除されていません。これは既知の問題です。

7.0 で削除された Switch Yard

Switch Yard は Fuse 7.0 で削除され、代わりに Apache Camel を直接使用する必要があります。詳細は、ナレッジベースの SwitchYard Support Plan After Releasing Fuse 7 を参照してください。

7.0 で除外された Fabric8 1.x のサポート

Fuse 7.0 で Fabric8 v1 は Fabric8 v2 のコンポーネントが含まれる Fuse on OpenShift (旧名称 Fuse Integration Services) に置き換えられました。Fuse on OpenShift は、OpenShift 内でインテグレーションマイクロサービスの開発、デプロイメント、および管理を可能にするツールのセットと Docker 形式のイメージを提供します。

Fuse on OpenShift のアーキテクチャーは異なりますが、Fabric 8 v1 が提供する同じプロビジョニング、自動化、中央設定、管理要件に対応します。詳細は Fuse on OpenShift ガイド を参照してください。

7.0 で削除された Google App Engine の Camel コンポーネント

Google App Engine の Camel コンポーネント (**camel-gae**) は Fuse 7.0 で削除されました。

7.0 で削除された Camel jBPM コンポーネント

Camel jBPM コンポーネント (**camel-jbpm**) は Fuse 7.0 で削除されました。

7.0 で削除された Fuse をサービスとしてインストールするための Tanuki ベースのラッパー

Fuse をサービスとしてインストールするための Tanuki ベースのラッパースクリプト (**wrapper:install** Karaf コンソールコマンドを使用して生成) は Fuse 7.0 で削除されました。Apache Karaf コンテナーをサービスとしてインストールする場合、この代わりに **bin/contrib** ディレクトリーから新しい **karaf-service-*.sh** スクリプトを使用することが推奨されます。

7.0 で削除された Smooks

Switch Yard の Smooks コンポーネントは Fuse 7.0 で削除されました。

7.0 で削除された BPEL

Riftsaw プロジェクトをベースとする BPEL は Fuse 7.0 で削除されました。BPEL を現在使用している場合は、Red Hat JBoss BPM Suite への移行を考慮することが推奨されます。

7.0 で削除された Design Time Governance

Design Time Governance コンポーネントは Fuse 7.0 で削除されました。

7.0 で削除された Runtime Governance

Runtime Governance (RTGov) コンポーネントは Fuse 7.0 で削除されました。

7.0 で削除された S-RAMP

S-RAMP (SOA Repository Artifact Model and Protocol) コンポーネントは Fuse 7.0 で削除されました。

7.0 で削除された bin/patch スクリプト

bin/patch スクリプト (Windows O/S では **bin\patch.bat**) は Fuse 7.0 で削除されました。

7.0 でサポートされない Spring-DM (Spring Dynamic Modules)

Spring XML を Apache Karaf の OSGi サービスレイヤーと統合する Spring-DM は Fuse 7.0 ではサポートされないため、代わりに Blueprint フレームワークを使用する必要があります。Blueprint

XML を使用しても、Spring フレームワークから Java ライブラリーを使用することはできます。最新バージョンの Spring は Blueprint と互換性があります。

7.0 でサポートされない Apache OpenJPA

JPA (Java Persistence API) の Apache OpenJPA 実装は Fuse 7.0 ではサポートされません。代わりに Hibernate 実装を使用することが推奨されます。

5.9. FUSE 7.0 で置き換えられた機能

以下の機能は Fuse 7.0 で置き換えられました。

7.0 で置き換えられた Geronimo トランザクションマネージャー

Fuse 7.0 では Karaf コンテナーの Geronimo トランザクションマネージャーが Narayana に置き換えられました。

7.0 で置き換えられた Jetty コンテナー

Fuse 7.0 では Jetty コンテナーが Undertow によって置き換えられました。この変更は最初に Jetty コンテナーの内部使用のみ (Karaf コンテナー内など) に適用されます。他の Jetty コンポーネントは今後のリリースで削除される可能性があります。

第6章 FUSE 7.12 でサポートされない機能

以下の機能は、Red Hat Fuse 7.12 ではサポートされません。

camel-leveldb コンポーネントは、IBM PowerPC および Z プラットフォームの Fuse ではサポートされない

Fuse が IBM PowerPC または IBM Z プラットフォームにインストールされている場合、Camel LevelDB コンポーネントはサポートされません。

Fuse Online のインストールと実行は、OpenShift Container Platform (OCP) 3.11 ではサポートされない

Fuse Online のインストールおよび実行は、OpenShift Container Platform (OCP) 3.11 ではサポートされていません。これは、Fabric8 Maven プラグインが非推奨になり、OpenShift Maven プラグインが優先されるためです。

Operator を使用した Fuse Console のインストールは OCP 3.11 ではサポートされない

OpenShift Container Platform (OCP) 3.11 では、Operator を使用した Fuse Console のインストールはサポートされておらず、機能しません。OCP 3.11 に Fuse Console をインストールする場合は、テンプレートを使用する手法が推奨されます。

サポートされない Apache Karaf EclipseLink 機能

Apache Karaf EclipseLink 機能は Fuse ではサポート**されません**。この機能は JPA 2.2 に依存しますが、Fuse 7.2 の Karaf コンテナーは JPA 2.1 と関連しているからです。

サポートされない Apache Aries Blueprint Web モジュール

Apache Aries Blueprint Web モジュールは Fuse ではサポート **されません**。Apache Camel のコミュニティー版で Blueprint Web を使用している例がありますが (個別ダウンロードとして提供)、Fuse でのサポートを意味するものでは**ありません**。

Apache Karaf の Apache Camel でサポートされない PHP スクリプト言語

PHP の OSGi バンドルがないため、PHP スクリプト言語は Apache Karaf コンテナー上の Camel アプリケーションでサポート**されません**。PHP スクリプト言語は、JBoss EAP コンテナーおよび Spring Boot コンテナー上の Camel アプリケーションでは非推奨になりました。

Apache Karaf の Apache Camel でサポートされない Python スクリプト言語

Python の OSGi バンドルがないため、Python スクリプト言語は Apache Karaf コンテナー上の Camel アプリケーションでサポート**されません**。Python スクリプト言語は、JBoss EAP コンテナーおよび Spring Boot コンテナー上の Camel アプリケーションでは非推奨になりました。

第7章 既知の問題

以下の項ではバージョン 7.12 の既知の問題について説明します。

7.1. CVE セキュリティー脆弱性

Fuse はミドルウェア統合プラットフォームであるため、多くのサードパーティーコンポーネントと統合される可能性があります。そのため、サードパーティーの依存関係の一部にセキュリティーの脆弱性がある可能性を常に排除することは困難です。ここでは、Fuse 7.12 のサードパーティー依存関係に影響するセキュリティー関連の既知の CVE (Common Vulnerabilities and Exposures) を記載します。

CVE-2020-13936 CVE-2020-13936 velocity: 攻撃者がテンプレートを変更できる場合の任意コードの実行

Velocity テンプレートを変更できる攻撃者は、Servlet コンテナーを実行しているアカウントと同じ権限で、任意の Java コードを実行したり、任意のシステムコマンドを実行したりする可能性があります。これには、バージョン 2.2 までの Apache Velocity Engine を実行する velocity テンプレートを信頼できないユーザーがアップロード/変更できるアプリケーションが該当します。
Fuse 7.9 (およびそれ以降) の依存関係は、このセキュリティー脆弱性から保護する修正された Velocity バージョン (2.3) のみを使用します。アプリケーションコードに Apache Velocity コンポーネントへの明示的な依存関係がある場合は、これらの依存関係をアップグレードして修正されたバージョンを使用することが推奨されます。

CVE-2018-10237 CVE-2018-10237 guava: AtomicDoubleArray および CompoundOrdering クラスでの無制限のメモリー割り当てにより、リモートの攻撃者がサービス拒否を引き起こす [fuse-7.0.0]

Google Guava の 11.0 から 24.1 までのバージョンは、**AtomicDoubleArray** クラス (Java のシリアライズでシリアル化される場合) および **CompoundOrdering** クラス (GWT のシリアライズでシリアル化される場合) のバインドされていないメモリー割り当てに対して脆弱です。攻撃者が Guava を使用するアプリケーションを悪用すると、信用できないデータをデシリアライズしてサービス拒否 (DoS) を発生できる可能性があります。詳細は、CVE-2018-10237 を参照してください。
このセキュリティー脆弱性を回避するため、以下を行うことが推奨されます。

- **AtomicDoubleArray** インスタンスまたは **CompoundOrdering** インスタンスを不明なソースからデシリアライズしないでください。
- 24 以前の Guava バージョンの使用しないようにします (ただし、場合によっては以前のバージョンの使用を避けられないことがあります)。

Fuse 7.7 (およびそれ以降) では、以前の (脆弱な) バージョンの Guava を簡単に使用できないようにするため、デフォルトですべてのコンテナーが Guava 27 を選択するよう、Maven BOM (Bill of Material) ファイルが設定されています。そのため、Fuse BOM を Maven プロジェクトに組み込み (BOM ファイルの依存関係を POM ファイルの **dependencyManagement** セクションに 追加)、明示的なバージョンを指定 **せずに** Guava アーティファクトの依存関係を指定すると、Guava のデフォルトのバージョンは BOM に指定されたバージョン (Fuse 7.7 の BOM ではバージョン 27) になります。

しかし、脆弱なバージョンの Guava の使用を回避できない一般的なユースケースが少なくとも 1 つあります。これは、OSGi アプリケーションが Guava と Swagger を一緒に使用する場合で、Swagger には Guava 20 が必要であるため、そのバージョンを使用する必要があります。ここでは、その理由と、以前の (脆弱な) Guava 20 ライブラリーを元に戻すために POM ファイルを設定する方法について説明します。まず、**ダブル OSGi チェーン** という概念を理解する必要があります。

ダブル OSGi チェーン

OSGi ランタイムのバンドルは、パッケージ制約 (パッケージ名 + 任意のバージョン/範囲) を使用して **ワイヤリング** されます (インポートおよびエクスポート)。各バンドルは複数のインポートを持つ

ことができ、通常これらのインポートは指定のバンドルを複数のバンドルでワイヤリングします。以下に例を示します。

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

この例では、**BundleA** は **BundleB** および **BundleCb** に依存し、**BundleB** は **BundleCa** に依存します。**BundleCa** と **BundleCb** が同じパッケージをエクスポートする場合、同じバンドルである必要があります。ただし、バージョン (範囲) の制約により、**BundleB** は **BundleA** とは異なるリビジョン/バージョンの **BundleC** を使用 (**ワイヤリング**) します。

上記の図を書き換えて、アプリケーションに Guava と Swagger の両方の依存関係を含めるとどうなるか反映させます。

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

このバンドル設定のデプロイを試みると、エラー **org.osgi.framework.BundleException: Uses constraint violation** が発生します。

Guava 20 に戻す

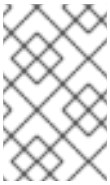
プロジェクトが直接的または間接的に Guava ライブラリーと Swagger ライブラリーの両方を使用する場合、Guava バンドルインポートに明示的なバージョン範囲を使用するよう、以下のように **maven-bundle-plugin** を設定する必要があります。

```
<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>
```

この設定により、OSGi アプリケーションは (脆弱性のある) Guava 20 ライブラリーに強制的に戻されます。そのため、この場合には **AtomicDoubleArray** インスタンスをデシリアライズしないようにすることが特に重要です。

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

Apache Solr は、Apache Lucene 検索エンジンを使用する一般的なオープンソースの検索プラットフォームです。アプリケーションが Apache Solar と Apache Lucene の組み合わせ (Camel Solr コンポーネントを使用している場合など) を使用する場合、このセキュリティー脆弱性の影響を受ける可能性があります。この脆弱性の詳細と軽減策について、リンク先のセキュリティーアドバイザリーを確認してください。



注記

Fuse ランタイムは Apache Solr や Apache Lucene を直接使用 **しません**。統合アプリケーションで Apache Solr と Apache Lucene を一緒に使用する場合のみセキュリティー上のリスクが発生します (Camel Solr コンポーネントを使用する場合など)。

CVE-2021-30129 mina-sshd-core: Apache Mina SSHD サーバーでのメモリーリークのサービス拒否

Apache Mina SSHD の sshd-core の脆弱性により、攻撃者がサーバーをオーバーフローさせ、OutOfMemory エラーが発生する可能性があります。この問題は、Apache Mina SSHD バージョン 2.0.0 以降の SFTP およびポート転送機能に影響します。これは、Apache Mina SSHD 2.7.0 で対処されました。
Apache Mina SSHD のこの脆弱性は、SSHD-1004 により対処されました。これは、この脆弱性を持つ特定の暗号化アルゴリズムを非推奨にします。Fuse 7.10 on Karaf および Fuse 7.10 on JBoss EAP では、これらの非推奨のアルゴリズムは引き続きサポートされます (後方互換性のため)。ただし、非推奨となったアルゴリズムのいずれかを使用している場合は、アプリケーションコードをリファクタリングして、代わりに別のアルゴリズムを使用することが強く推奨されます。

Fuse 7.10 では、デフォルトの暗号化アルゴリズムが以下のように変更されました。

Fuse 7.9	Fuse 7.10	Fuse 7.10 で非推奨となりましたか？
aes128-ctr	**aes128-ctr**	
	aes192-ctr	
	aes256-ctr	
	aes128-gcm@openssh.com	
	aes256-gcm@openssh.com	
arcfour128	**arcfour128**	**はい**
aes128-cbc	**aes128-cbc**	
	aes192-cbc	
	aes256-cbc	
3des-cbc	**3des-cbc**	**はい**
blowfish-cbc	**blowfish-cbc**	**はい**

Fuse 7.10 では、デフォルトの鍵交換アルゴリズムが以下のように変更されました。

Fuse 7.9	Fuse 7.10	7.10 で非推奨となりましたか？
diffie-hellman-group-exchange-sha256	**diffie-hellman-group-exchange-sha256**	
ecdh-sha2-nistp521	**ecdh-sha2-nistp521**	

Fuse 7.9	Fuse 7.10	7.10 で非推奨となりましたか？
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**	**はい**
diffie-hellman-group1-sha1	**diffie-hellman-group1-sha1**	**はい**

7.2. FUSE ONLINE

Fuse Online ディストリビューションの既知の問題は次のとおりです。

ENTESB-21338 新しいアプリケーションに対する Twitter API v1.1 の制限

Twitter v1.1 API の制限により、新しい Twitter アプリケーションは動作しません。

ENTESB-17674 OCP 4.9(またはそれ以降) で Prometheus および Grafana を使用して Fuse Online を監視するには、回避策が必要

OCP 4.9 (またはそれ以降) では、**application-monitoring** プロジェクトは機能しなくなりました。これは、Prometheus および Grafana で Fuse Online インテグレーションおよびインフラストラクチャーコンポーネントを監視するための前提条件です。
この問題を回避するには、(**openshift-monitoring** namespace で) ビルトインのモニタリングスタック を使用して **openshift-user-workload-monitoring** 機能および **grafana-operator** を使用し、このリリースノートの **Fuse Online での重要事項** セクションの説明にあるように、**ops addon** を使用します。

ENTESB-14518 Syndesis 1.11 によってインストールされた Jaeger Operator は、他の namespace に影響を与える

Fuse 7.8 以降、OpenShift クラスターに Fuse 7.8 Online (Syndesis 1.11) をインストールすると、Jaeger Operator (Fuse Online とともにインストールされる) は、デフォルトで **すべての namespace** を管理するよう設定されます。そのため、クラスターに Fuse 7.7 Online (Syndesis 1.10) がすでにインストールされている場合に、Fuse 7.8 Online を別の namespace にインストールする

と、Fuse 7.8 Online とともにインストールされた Jaeger Operator が Fuse 7.7 Online の namespace にインストールされた (以前の) Jaeger インスタンスを管理しようとします。その結果、既存の **syndesis-jaeger** Pod に加え、新しい **syndesis-jaeger** Pod が Fuse 7.7 Online namespace に表示され、新しい **syndesis-jaeger** Pod が **CrashLoopBackOff** 状態に入ります。元の Fuse 7.7 Online インスタンスは影響を受けず、クラッシュした **syndesis-jaeger** Pod は無視しても問題ありません。

ENTESB-13966 デプロイされた統合 API の検出が無効になっているようだが、実際にはそうではない

Fuse 7.7 以降、API が含まれる新しいインテグレーションの作成後に、インテグレーションの詳細ページでそのインテグレーションの 3scale 検出が無効になっていると誤って表示されます。また、インテグレーションの詳細ページには API URL が表示されません。このボタンを 3 回クリックすると (**Enable**、**Disable**、**Enable** の順にクリックします) ページが再同期され、3scale の検出が有効になり、API URL が表示されます。

7.3. FUSE ON OPENSHIFT

このセクションでは、OpenShift 上の Fuse アプリケーションのデプロイメントに影響する問題を取り上げます。特定のコンテナーに影響する問題の詳細は、Spring Boot、Fuse on Apache Karaf、および Fuse on JBoss EAP のセクションも参照にしてください。Fuse on OpenShift ディストリビューションの既知の問題を以下に示します。

ENTESB-21281 add-opens を使用した FoO イメージの更新

add-opens を使用しない場合、Fuse on Open Shift は jdk17 では正しく動作しません。これらのフラグは自動的に提供できないため、**add-opens** を定義するスクリプトにフラグを追加して、自分で指定する必要があります。

Java 17 以降、Java Platform Module System が **必須** になりました。これは、アクセスを制限 する強力なカプセル化を実装します。**--add-opens** オプションを使用してアクセスを許可することで、ディープリフレクションを提供し、指定したモジュールが名前付きパッケージを開くことができるようになります。

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

ENTESB-21281 [Fuse on Openshift] QS karaf-cxf-rest - JavaDoc が jdk17 でサポートされない

Red Hat FUSE 7.x の **cxf java2wadl-plugin** は、JDK17 では動作しません。

ENTESB-17895 [Fuse Console] アップグレードサブスクリプションは、Hawtio を更新しない

Fuse 7.10 では、Operator サブスクリプションチャネルをバージョン 7.10 に変更して Fuse Console を更新した場合、Fuse Console は vesion 7.9 のままになります。Fuse Console コンテナーと Pod にラベル 7.10 がある場合でも、これらのコンテナーは引き続き 7.9 イメージを使用しています。この問題を回避するには、以前のバージョンの Fuse Console を削除してアップグレードを実行し、Fuse Console バージョン 7.10 を新規インストールします。

ENTESB-17861 Apicurito ジェネレーターが Fuse Camel プロジェクトを生成できない

Fuse 7.10 では、API Designer(Apicurito) が Apicurito Operator 経由でインストールされている場合は適切に機能しません (Invalid Cert Error が表示されます)。この問題を回避するには、以下を実行します。

1. **https://apicurito-service-generator-apicurito.apps.cluster-name.openshift.com** への新しいタブを開きます。
   (**cluster-name.openshift.com** は、クラスター名に置き換えます。)
2. 証明書を受け入れます。
3. アプリケーションに切り替え、生成ボタンを再度クリックします。

ENTESB-17836 **[Fuse Console] 新しく追加されたルートがキャメルツリーに表示されない**

Fuse 7.10 では、アプリケーションをデプロイした後、ルート (または複数のルート) は Fuse Console の Camel ツリーに表示されません。この問題を回避するには、ルートが表示されるようにページを更新します。

ENTESB-19351FIPS on OCP - サポート対象外のセキュリティーエンコーディングが原因で Jolokia エージェントが起動しない

Fuse 7.11 では、OCP FIPS 対応 Jolokia エージェントは、セキュリティーエンコーディングがサポートされていないため使用できなくなります。

ENTESB-19352 FIPS on OCP - karaf-maven-plugin アセンブリーゴールがサポート対象外のセキュリティープロバイダーで失敗する

Fuse 7.11 では、アセンブリゴールで **karaf-maven-plugin** を使用すると、Karaf アプリケーションで OCP FIPS が有効になっている場合にバイナリーストリームデプロイストラテジーが失敗します。

7.4. FUSE ON APACHE KARAF

Fuse on Apache Karaf の既知の問題は次のとおりです。

ENTESB-16417 **認証情報ストアはデフォルトで PBEWithSHA1AndDESede を使用**

OpenJDK 8u292 および OracleJDK 1.8.0_291 のセキュリティー API は、セキュリティープロバイダーの不完全なリストを返すため、Apache Karaf のクレデンシャルストアが失敗します (必要なセキュリティープロバイダーが利用できないように見えるため)。この問題の原因となる根本的な問題は https://bugs.openjdk.java.net/browse/JDK-8249906 です。このバグがない、以前の OpenJDK バージョン (OpenJDK 8u282)、または新しいバージョンの OpenJDK (OpenJDK 8u302) を使用することを推奨します。

ENTESB-16526 **fuse-karaf on Windows は、patch:install 中に再起動できない**

Windows プラットフォームの Apache Karaf コンテナーで **patch:install** の実行中に、特定の状況では、**patch:install** コマンドがコンテナーの自動再起動を試行すると、以下のエラーが発生する可能性があります。

```
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.
```

このエラーが発生した場合は、Karaf コンテナーを手動で再起動するだけです。

ENTESB-8140 **ホットデプロイバンドルの開始レベルはデフォルトで 80**

Fuse 7.0 GA リリース以降の Apache Karaf コンテナーでは、ホットデプロイバンドルの開始レベルがデフォルトで 80 になっています。これにより、同じ開始レベルを持つシステムバンドルや機能が多く存在するため、ホットデプロイバンドルに問題が発生することがあります。この問題を回避し、ホットデプロイバンドルが確実に開始するようにするには、**etc/org.apache.felix.fileinstall-deploy.cfg** ファイルを編集し、**felix.fileinstall.start.level** 設定を以下のように変更します。

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

ENTESB-7664 framework-security 機能をインストールすると、karaf を終了する

--no-auto-refresh オプションを使用して **framework-security** OSGi 機能をインストールしないと、Apache Karaf コンテナーがシャットダウンします。以下に例を示します。

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

7.5. FUSE ON JBOSS EAP

Fuse on JBoss EAP の既知の問題は次のとおりです。

ENTESB-21314 [Fuse on EAP] jdk17 モジュール性のサポート

add-opens を使用しない場合、Fuse on EAP は jdk17 では正しく動作しません。これらのフラグは自動的に提供できないため、**add-opens** を定義するスクリプトにフラグを追加して、自分で指定する必要があります。
Java 17 以降、Java Platform Module System が **必須** になりました。これは、アクセスを制限 する強力なカプセル化を実装します。**--add-opens** オプションを使用してアクセスを許可することで、ディープリフレクションを提供し、指定したモジュールが名前付きパッケージを開くことができるようになります。

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

ENTESB-20833 jdk17 の java.security.acl.Group の削除

java.security.acl.Group は、バージョン jdk14 以降では削除されます。

ENTESB-13168 EAP ドメインモードでの Camel デプロイメントは Windows で機能しない

Fuse 7.6.0 以降では、Fuse on JBoss EAP で Camel サブシステムを Windows OS 上の ドメインモードの JBoss EAP にデプロイできません。

7.6. FUSE ON SPRING BOOT

Fuse on Spring Boot の既知の問題は次のとおりです。

ENTESB-21315 [Fuse on Spring-boot] jdk17 モジュール性のサポート

add-opens を使用しない場合、Fuse は jdk17 では正しく動作しません。これらのフラグは自動的に提供できないため、**add-opens** を定義するスクリプトにフラグを追加して、自分で指定する必要があります。
Java 17 以降、Java Platform Module System が **必須** になりました。これは、アクセスを制限 する強力なカプセル化を実装します。**--add-opens** オプションを使用してアクセスを許可することで、ディープリフレクションを提供し、指定したモジュールが名前付きパッケージを開くことができるようになります。

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

ENTESB-21421 / ENTESB-20842 Spring Boot 2.6 では循環依存関係が許可されない

Spring Boot 2.6 は循環依存関係を解決できない可能性があります。Spring Boot で XML DSL を使用して、Bean ファイル内でカスタマイズされた **HealthCheckRegistry** をインスタンス化すると、ビルドが失敗します。
回避策として、プロパティー **spring.main.allow-circular-references=true** を **application.properties** に追加できます。

7.7. FUSE TOOLING

Fuse Tooling の既知の問題は次のとおりです。

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

Hawtio は、WildFly を使用した古いセキュリティーシステムでのみ動作します。Elytron セキュリティーを使用して Hawtio にログインしようとすると、コンソールに次のエラーメッセージが表示されます。

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

ENTESB-19668 **クライアント証明書の認証が拒否された場合、Hawtio 管理コンソールの UI にメッセージが表示されない**

Hawtio コンポーネントが、クライアント証明書からの認証を拒否した後、ログインページにメッセージを表示しません。Hawtio は、Web ブラウザーをログインページにリダイレクトするだけで、メッセージを表示しません。

ENTESB-17705 **[Hawtio] ログアウトボタンが消える**

Fuse 7.10 では、数回連続してログインおよびログアウトすると、**Logout** ボタンが表示されなくなります。この問題を回避するには、ページを 1 回以上更新すると、**Logout** ボタンが再度表示されます。

ENTESB-17839**Fuse + AtlasMap: dataSourceType フィールドが認識されない**

Fuse 7.11 では、ユーザーが AtlasMap vscode エクステンションを使用する場合、Fuse7.11 は AtlasMap 2.3.x であるため、バージョン 0.0.9 を使用する必要があります。それ以外の場合は AtlasMap スタンドアロン 2.3.x を使用しますが、vscode-extension は使用しません。

7.8. APACHE CAMEL

Apache Camel の既知の問題は次のとおりです。

ENTESB-19361 / UNDERTOW-2206 **karaf の埋め込み undertow サーバーを使用する cxf でのアクセスロギングサポートでは、URI がロギングされない**

DECODE_URL オプションが **true** (Fuse 7.11.1 karaf ランタイムのデフォルト値)
で、**HttpServerExchange** を使用して **relativePath** および **requestPath** をデコードする場合、**requestURI** パラメーターはエンコードされたままになります。
dispatch メソッド (**forward**、**include**、**async**、および **error**) は、パスをデコードせずに **requestPath** および **relativeURL** に割り当てるので、**/some%20thing** などのパスにディスパッチされます。

ENTESB-15343 **XSLT コンポーネントが IBM1.8JDK で正しく機能しない**

Fuse 7.8 では、Camel XSLT コンポーネントは IBM 1.8 JDK と正しく動作しません。この問題は、XSLT の基礎となる Apache Xerces 実装が **javax.xml.XMLConstants#FEATURE_SECURE_PROCESSING** プロパティーをサポートしないために発生します (XERCESJ-1654 を参照)。

ENTESB-11060 **[camel-linkedin] V1 API は今後はサポートされない**

Fuse 7.4.0 以降、Camel LinkedIn コンポーネントが LinkedIn サーバーと通信できなくなりました。これは、LinkedIn でサポートされなくなった LinkedIn Version 1.0 API を使用して実装されているためです。Fuse の今後のリリースで Camel LinkedIn コンポーネントが更新され、Version 2 API を使用するようになる予定です。

ENTESB-7469 **Camel Docker コンポーネントは EAP で Unix ソケット接続を使用できない**

Fuse 7.0 より、**camel-docker** コンポーネントは UNIX ソケットではなく REST API のみを介して Docker に接続できます。

ENTESB-5231 **PHP スクリプト言語は機能しない**

PHP の OSGi バンドルがないため、PHP スクリプト言語は Apache Karaf コンテナー上の Camel アプリケーションでサポート**されません**。

ENTESB-5232 **Python 言語は機能しない**

Python の OSGi バンドルがないため、Python スクリプト言語は Apache Karaf コンテナー上の Camel アプリケーションでサポート**されません**。

ENTESB-2443 **Google Mail API - メッセージの送信と下書きが同期されていない**

メッセージまたは下書きを送信すると、応答には ID を持つ Message オブジェクトが含まれます。API への別の呼び出しを介してこのメッセージを即座に取得できない可能性があります。このような場合、待機して呼び出しを再試行する必要があります。

ENTESB-2332 **Google Drive API JSON の変更への応答は、最初のページのアイテムの不正な数を返す**

変更に対する Google Drive API JSON 応答によって返される最初のページのアイテム数は適切でありません。リスト操作の **maxResults** を設定すると、最初のページにすべての結果が返されないことがあります。この場合、複数のページを確認して完全リストを取得する必要があります (新しいリクエストに **pageToken** を設定して行います)。

第8章 FUSE 7.12 で修正された問題

以下のセクションには、Fuse 7.12 および Fuse 7.12.1 で修正された問題が記載されています。

- 「Fuse 7.12 で改良された機能」
- 「Fuse 7.12 のコンポーネントアップグレード」
- 「Fuse 7.12 で解決されたバグ」
- 「Fuse 7.12.1 で解決されたバグ」

8.1. FUSE 7.12 で改良された機能

問題	説明
ENTESB-17374	ロードされたプラグインを公開して、PluginServlet への複数のリクエストを回避する
ENTESB-20016	Fuse コンソール - hawtio CR でラベルを設定できるようにする
ENTESB-20592	ELS の前に OpenJDK 17 で Fuse 7 を証明する
ENTESB-20667	Operator メタデータバンドルの operators.openshift.io/valid-subscription アノテーション
ENTESB-20714	すべての CXF テストが JDK17 で合格したことを確認する
ENTESB-20830	RHEL 9 で Fuse 7 を証明する
ENTESB-20953	EAP-7.4.10.GA-redhat-00002 へのアップグレード

8.2. FUSE 7.12 のコンポーネントアップグレード

以下の表に Fuse 7.12 のコンポーネントのアップグレードを示します。

表8.1 Fuse 7.12 コンポーネントのアップグレード

問題	説明
ENTESB-20648	Spring Boot を 2.7.12 にアップグレードする
ENTESB-20849	Camel テストの依存関係を調整して JDK17 と互換性を持たせる
ENTESB-21063	Kafka-clients v3 との整合性を確保する

8.3. FUSE 7.12 で解決されたバグ

以下の表に、Fuse 7.12 で解決されたバグを示します。

表8.2 Fuse 7.12 で解決されたバグ

問題	説明
ENTESB-8337	オフラインリポジトリーに org.jboss.fuse.fis.archetypes グループ名アーティファクトが含まれている
ENTESB-12949	SQS ステップの作成で、自動入力されたキューの値を変更するまで、次に進むボタンが無効なままである
ENTESB-13046	Operator バイナリーを使用した復元が期待どおりに機能しない
ENTESB-13366	Operator の指示が不明瞭で、シークレット作成手順のデバッグが容易ではない
ENTESB-13966	デプロイされた統合 API の検出が無効になっているようだが、実際にはそうではない
ENTESB-14552	マルチキャストキューのサポート
ENTESB-17394	エラーの感嘆符にエラーメッセージが表示されない
ENTESB-17404	x86 用の leveldb-jni をビルドする
ENTESB-17888	https エンドポイントに接続するときに検証エラーが発生する
ENTESB-18042	Failed to watch エラーが Operator ログに出力される
ENTESB-18364	Hawtio - Keycloak で Hawtio を使用する場合の CSP の問題
ENTESB-19351	FIPS on OCP - サポート対象外のセキュリティーエンコーディングが原因で Jolokia エージェントが起動しない
ENTESB-19352	FIPS on OCP - karaf-maven-plugin アセンブリーゴールがサポート対象外のセキュリティープロバイダーで失敗する
ENTESB-19745	クイックスタート spring-boot-camel-amq 統合テストが古い AMQ ブローカーバージョンを参照する
ENTESB-19757	apicurito のソースコンテナーイメージを提供する
ENTESB-19956	[Syndesis] CVE-2022-24785 Moment.js: moment.locale でのパストラバーサル [fuse-7]
ENTESB-19986	Fuse hawtio に HTTPClient 3.1 が含まれている - CVE-2012-5783

問題	説明
ENTESB-20096	AMQ6 イメージ - V2 スキーマ 1 マニフェストダイジェストがイメージプルでサポートされていない
ENTESB-20175	ランタイム固有のカタログにデータ形式 fhir-json/fhir-xml/xml-json がない
ENTESB-20177	コンテナービルド用の正しい UMB メッセージを送信する
ENTESB-20404	Camel http4 プロデューサーが、配列データを複数値パラメーターではなくコンマ区切り形式で http uri パラメーターにエンコードする
ENTESB-20485	CVE-2022-42920 apache-bcel: Apache-Commons-BCEL: 範囲外の書き込みによって生成された任意のバイトコード [fuse-7]
ENTESB-20595	ENTMQCL-2977 の Fuse 7.11.x へのバックポートリクエスト
ENTESB-20596	CVE-2022-41940 engine.io: 悪用目的で作成された HTTP リクエストにより、キャッチされない例外がトリガーされる可能性がある [fuse-7]
ENTESB-20598	CVE-2020-13956 の不完全な修正
ENTESB-20618	CVE-2022-41881 codec-haproxy: HAProxyMessageDecoder スタック枯渇 DoS [fuse-7]
ENTESB-20619	CVE-2022-41854 dev-java-snakeyaml: dev-java/snakeyaml: スタックオーバーフローによる DoS [fuse-7]
ENTESB-20626	CVE-2022-40146 batik: サーバーサイドリクエストフォージェリー (SSRF) の脆弱性 [fuse-7]
ENTESB-20627	CVE-2022-38398 batik: サーバーサイドリクエストフォージェリー [fuse-7]
ENTESB-20628	CVE-2022-38648 batik: サーバーサイドリクエストフォージェリー [fuse-7]
ENTESB-20630	CVE-2022-46364 CXF: Apache CXF: SSRF の脆弱性 [fuse-7]
ENTESB-20632	CVE-2022-46363 CXF: Apache CXF: ディレクトリーリスティング/コードの流出 [fuse-7]
ENTESB-20637	CVE-2022-4492 undertow: https 接続のサーバー ID が undertow クライアントによってチェックされない [fuse-7]
ENTESB-20641	CVE-2022-41946 jdbc-postgresql: postgresql-jdbc: セキュアでない一時ファイルパーミッションによる準備済みステートメントデータの情報漏洩 [fuse-7]

問題	説明
ENTESB-20663	jdk17 での Karaf 起動時のエラー
ENTESB-20664	jdk17 での EAP 起動時のエラー
ENTESB-20672	CVE-2022-45143 tomcat: JsonErrorReportValve インジェクション [fuse-7]
ENTESB-20690	CVE-2022-36437 hazelcast: Hazelcast 接続キャッシュ [fuse-7]
ENTESB-20693	patch-maven-plugin → karaf-maven-plugin 接続の見直し
ENTESB-20696	カスタム Fuse Console ルートが機能しない
ENTESB-20697	RabbitMQ 接続ファクトリーからの AutomaticRecovery で 常に新しい接続が作成される
ENTESB-20701	fuse-patch が、パッチがすでに適用されていると誤って報告する場合がある
ENTESB-20702	netty4-http が不正な応答を転送する (例外 + http コード 200)
ENTESB-20710	Karaf 4.4 および Pax Web 8 にアップグレードした後の CXF テストエラー
ENTESB-20711	Fuse 7.11 で TLS 1.3 を使用する camel-aws 2.23 コンポーネントの問題
ENTESB-20712	Karaf 4.4 および Pax Web 8 にアップグレードした後の Camel テストエラー
ENTESB-20720	マルチキャストが集約を返さない
ENTESB-20726	Hazelcast のアップグレードにより JCache 統合が中断される
ENTESB-20741	Fuse プロジェクトで使用される javax/mail/mail のバージョンが間違っている
ENTESB-20742	Fuse プロジェクトで間違った log4j-slf4j18-impl バージョンが使用される
ENTESB-20754	[Hawtio] Karaf にログインできない
ENTESB-20826	CVE-2022-41966 xstream: 要素のハッシュ値に基づいて再帰的なコレクションまたはマップを挿入することによるサービス拒否により、スタックオーバーフローが発生する [fuse-7]
ENTESB-20828	cxf - サーバートランスポートが正しく起動しない
ENTESB-20829	[Karaf] JCE がプロバイダー BC を認証できない

問題	説明
ENTESB-20831	json ファイルでグループ化された API バージョンを使用する
ENTESB-20835	Karaf pax Web - OPTIONS メソッドが公開されない
ENTESB-20836	Hibernate Fuse のバージョンが Spring Boot と競合する
ENTESB-20839	[Karaf] JMX ACL MBean 認証の問題
ENTESB-20840	[Karaf] 10 個の機能をインストールできない
ENTESB-20841	SB1 形式の Fuse アーキタイプの Spring Boot プロパティー
ENTESB-20842	camel-master コンポーネントがクラスターサービスをロードできない
ENTESB-20845	CVE-2023-1108 undertow: クローズ時の SslConduit での無限ループ [fuse-7]
ENTESB-20847	[Karaf] Jasypt 暗号化の問題 (JDK 17 および RHEL8-FIPS)
ENTESB-20850	[Standalone] Fuse クライアント経由で応答メッセージを得られない
ENTESB-20851	[Standalone] 履歴内の色分けされたコマンド
ENTESB-20853	[Fuse on Openshift] - クイックスタートの Docker イメージ参照が間違っている
ENTESB-20854	[Fuse on Openshift] - アプリケーションテンプレート - fis-image-streams.json のイメージストリームに "1.12" のタグがない
ENTESB-20855	[Fuse on Openshift] - EAP イメージの WILDFLY バージョンが間違っている (JDK8/11)
ENTESB-20857	[Fuse on Openshift] - アプリケーションテンプレート - 古い 7.11 参照が含まれたテンプレート
ENTESB-20859	[Patching] 7.11 から 7.12 にパッチを適用できない
ENTESB-20862	[karaf FoO] クライアントを POD に使用できない
ENTESB-20869	CVE-2023-20860 springframework: 接頭辞のないダブルワイルドカードパターンによるセキュリティーバイパス [fuse-7]
ENTESB-20870	CVE-2023-20861 springframework: Spring 式の DoS 脆弱性 [fuse-7]
ENTESB-20871	Camel 2.23 テストが jdk17 をサポートしていない

問題	説明
ENTESB-20872	Wildfly Camel 5.10 テストが jdk17 をサポートしていない
ENTESB-20873	CXF 3.3.6 テストが jdk17 をサポートしていない
ENTESB-20950	[Karaf] 機能がインストールされない
ENTESB-20951	Camel Mail コンポーネントがセッション URI パラメーターからのホスト/ポート情報を使用しない
ENTESB-20956	CVE-2022-4492、Syndesis が修正された undertow を使用していることを確認する
ENTESB-20957	CVE-2023-1108 undertow: クローズ時の SslConduit での無限ループ (Fuse Online)
ENTESB-20958	CVE-2022-41704 batik: Apache XML Graphics Batik が SVG 経由のコード実行に脆弱 [fuse-7]
ENTESB-20959	CVE-2022-42890 batik: Apache XML Graphics Batik で信頼できないコードが実行される [fuse-7]
ENTESB-20960	CVE-2023-22602 shiro-core: shiro: 悪用目的で作成された HTTP リクエストによる認証バイパス [fuse-7]
ENTESB-20961	[Fuse On Openshift] QS spring-boot-camel-amq に削除されたイメージが含まれている
ENTESB-20963	[Fuse On Openshift] QS Spring-Boot Camel Rest SQL が README で間違ったデプロイメントステップを報告する
ENTESB-20964	[Fuse On Openshift] メータリングラベル rht.prod_ver のフォーマットを調整する
ENTESB-20967	[Fuse on Openshift] SB のアップグレードにより、Spring Cloud で QS Spring-Boot Camel Config が失敗する
ENTESB-20966	karaf 機能を個別にインストールできない
ENTESB-20968	[Fuse on Openshift] QS Spring-Boot Camel Rest SQL が不正な SQL 文法例外を出力する
ENTESB-20969	[Fuse on Openshift] QS Spring-Boot Camel XA が PostGresSQL 接続で不正な SQL 文法例外を出力する
ENTESB-20971	Hawtio コンソールのメトリックに、使用済みメモリーではなく空きメモリーが表示される

問題	説明
ENTESB-21045	Pax-web-jetty 機能をインストールできない
ENTESB-21046	[Fuse standalone] ログの例外 (jdk11 および jdk17)
ENTESB-21047	CVE-2023-20860、Syndesis が修正された springframework を使用していることを確認する
ENTESB-21048	7.12 上に CVE パッチをインストールできない
ENTESB-21049	CVE-2022-41854、Syndesis が修正された Snakeyaml を使用していることを確認する
ENTESB-21050	cxf-spring-boot-starter-jaxrs から org.apache.tomcat.embed 依存関係を削除する
ENTESB-21051	[Fuse on Openshift] QS Spring-Boot Camel-Drools、Kie Server を作成できない
ENTESB-21053	[Fuse on Openshift] QS Spring Boot Camel Singleton、アプリケーションが起動しない
ENTESB-21052	[Fuse on Openshift] - Karaf - cxf-jaxrs アプリケーションで不足している要件を解決できない
ENTESB-21056	CVE-2023-20861、Syndesis が修正された springframework を使用していることを確認する
ENTESB-21057	CVE-2022-41946、Syndesis が修正された jdbc-postgresql を使用していることを確認する
ENTESB-21058	Karaf、一部のバンドルバージョンが karaf-bom で指定されたバージョンと一致していない
ENTESB-21059	pax-url-aether でのメモリーリーク
ENTESB-21061	CXF 3.3.6 ダウンストリームの障害
ENTESB-21704	CVE-2023-20863 springframework: Spring 式の DoS 脆弱性 [fuse-7]
ENTESB-21158	Keycloak がアクセス制御用に統合されている場合、無人 Jolokia クエリーが機能しない
ENTESB-21161	[Offliner] offliner マニフェストファイルを使用してファイルをダウンロードできない

問題	説明
ENTESB-21162	[Offliner] 不足しているアーティファクト
ENTESB-21163	Apicurito Pod に誤った値のメータリングラベルが含まれている
ENTESB-21168	CVE-2023-1370 json-smart: json-smart の制御できないリソース消費の脆弱性 (リソース枯渇) [fuse-7]
ENTESB-21272	[Fuse on Openshift] クイックスタート BOM のバージョンが間違っている
ENTESB-21273	機能しないクイックスタート spring-boot-camel-soap-rest-bridge を削除またはリファクタリングする
ENTESB-21274	Wildfly Camel 5.10.0 ダウンストリームの障害
ENTESB-21304	[Fuse on Openshift] - xerces パッケージが公開されていないため、Karaf、jaxws、JDK17 を使用した java.xml モジュールへの不正アクセスが発生する
ENTESB-21309	[Fuse on Openshift] - Karaf の Camel-jdbc で、body exchange から列を取得できない
ENTESB-21310	Camel-Velocity: 非推奨の警告
ENTESB-21311	SpringFramework が失敗した TypeConverter をキャッシュし、ユーザーがそれを消去できない
ENTESB-21316	[Fuse on Openshift] - RHOSAK クイックスタートを消去/削除する
ENTESB-21319	CVE-2022-31692 spring-security: Spring Security に転送またはディスパッチャータイプを含めることで、認可ルールをバイパスできる [fuse-7]
ENTESB-21322	Karaf バンドルの修飾子が無効である
ENTESB-21332	CVE-2023-20883 spring-boot: Spring Boot ウェルカムページの DoS 脆弱性 [fuse-7]
ENTESB-21335	patch-maven-plugin が Maven 3.9 で動作しない
ENTESB-21412	GitHub で参照/タグが欠落している
ENTESB-21415	[Fuse standalone] Camel-chunk 機能の依存関係が欠落している
ENTESB-21417	CXF 3.3.6 ダウンストリームの障害
ENTESB-21418	CVE-2023-1370、Syndesis が修正された json-smart を使用していることを確認する

問題	説明
ENTESB-21419	[Karaf] Jasypt 暗号化の問題 (JDK 17 および RHEL8-FIPS)
ENTESB-21421	Spring Boot ランタイムでの Camel ヘルスチェックの動作の変更

8.4. FUSE 7.12.1 で解決されたバグ

以下の表に、Fuse 7.12.1 で解決されたバグを示します。

表8.3 Fuse 7.12.1 で解決されたバグ

問題	説明
ENTESB-21742	新しい Fuse Console デプロイメントが、毎年の "openshift-service-serving-signer" 証明書のローテーション後に機能しない
ENTESB-21757	[JDG-4351][JBMAR-235] camel-infinispan が、2.0.9.Final から 2.0.11.Final 以降への jboss-marshalling の更新を必要とする
ENTESB-21776	Fuse on Openshift イメージが非常に古い jmx_prometheus_javaagent.jar を使用する
ENTESB-21858	JDK 11.0.20 を使用すると Karaf が起動しない
ENTESB-21878	ロギングが WARN レベルの場合の NullPointerException
ENTESB-21881	Maven 3.9 で patch-maven-plugin に -Dpatch を使用する際の問題
ENTESB-22087	パッチ 7.12.1 を 7.12 上にインストールできない
ENTESB-21763	toD を使用した camel-http4 が Karaf で動作しない
ENTESB-21865	pollEnrich ファイルコンポーネントの動作が 6.3 と 7.11 の間で変化する
CVE-2023-46604	CVE-2023-46604 activemq-openwire: OpenWire モジュール: 無制限の逆シリアル化により、ActiveMQ がリモートコード実行 (RCE) 攻撃に対して脆弱化する [fuse-7]
CVE-2023-40167	CVE-2023-40167 jetty-http: jetty: HTTP/1 コンテンツ長の不適切な検証 [fuse-7]
CVE-2023-3223	CVE-2023-3223 undertow: @MultipartConfig 処理による OutOfMemoryError [fuse-7]
CVE-2023-36479	CVE-2023-36479 jetty-servlets: jetty: CgiServlet でユーザー入力に不適切な引用符が追加される [fuse-7]

問題	説明
CVE-2023-39410	CVE-2023-39410 avro: apache-avro: Apache Avro Java SDK: Avro Java SDK で信頼できないデータを逆シリアル化するときのメモリー [fuse-7]
CVE-2023-34034	CVE-2023-34034 spring-security: spring-security-webflux: パスのワイルドカードによるセキュリティーバイパス [fuse-7]
CVE-2023-44487	CVE-2023-44487 undertow: HTTP/2: 複数の HTTP/2 対応 Web サーバーが DDoS 攻撃 (ラピッドリセット攻撃) からの影響を受ける [fuse-7]
CVE-2023-36478	CVE-2023-36478 http2-hpack: jetty: hpack ヘッダー値により http/2 でサービス妨害が発生する [fuse-7]
CVE-2023-41900	CVE-2023-41900 jetty-openid: jetty: OpenId の取り消された認証で 1 つのリクエストが許可される [fuse-7]