



Red Hat Decision Manager 7.4

Red Hat OpenShift Container Platform への Red Hat Decision Manager イミュータブルサー バー環境のデプロイメント

ガイド

Red Hat Decision Manager 7.4 Red Hat OpenShift Container Platform への Red Hat Decision Manager イミュータブルサーバー環境のデプロイメント

ガイド

Enter your first name here. Enter your surname here.

Enter your organisation's name here. Enter your organisational division here.

Enter your email address here.

法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Deploying_a_Red_Hat_Decision_Manager_immutable_server_environment_on_Red_Hat_OpenS file |.

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.

概要

本書は、Red Hat OpenShift Container Platform に Red Hat Decision Manager 7.4 イミュータブルサーバー環境をデプロイする方法を説明します。

目次

はじめに	4
第1章 RED HAT OPENSIFT CONTAINER PLATFORM における RED HAT DECISION MANAGER の概要	5
第2章 OPENSIFT 環境に RED HAT DECISION MANAGER をデプロイする準備	7
2.1. イメージストリームとイメージレジストリーの可用性確認	7
2.2. DECISION SERVER にシークレットの作成	8
2.3. S2I ビルドに使用する BUSINESS CENTRAL からのソースコードの展開	9
2.4. オフラインで使用する MAVEN ミラーリポジトリの用意	9
第3章 イミュータブルサーバーを使用した環境	12
3.1. S2I ビルドの使用によるイミュータブル DECISION SERVER のデプロイ	12
3.1.1. S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始	12
3.1.2. S2I の使用によるイミュータブル Decision Server に必要なパラメーターの設定	13
3.1.3. S2I の使用によるイミュータブル Decision Server のイメージストリーム namespace の設定	15
3.1.4. S2I の使用によるイミュータブル Decision Server 用の Business Central インスタンスについての情報の設定	15
3.1.5. S2I の使用によるイミュータブル Decision Server のオプションの Maven リポジトリの設定	16
3.1.6. S2I の使用によるイミュータブル Decision Server の公開インターネットへの接続のない環境での Maven ミラーへのアクセスの設定	16
3.1.7. S2I の使用によるイミュータブル Decision Server 用の AMQ サーバーとの通信の設定	17
3.1.8. S2I の使用によるイミュータブル Decision Server の RH-SSO 認証パラメーターの設定	18
3.1.9. S2I の使用によるイミュータブル Decision Server の LDAP 認証パラメーターの設定	19
3.1.10. S2I の使用によるイミュータブル Decision Server の Prometheus メトリクス収集の有効化	21
3.1.11. S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始	21
3.2. KJAR サービスからのイミュータブル DECISION SERVER のデプロイ	21
3.2.1. KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始	22
3.2.2. KJAR サービスからのイミュータブル Decision Server のパラメーターの設定	22
3.2.3. イミュータブル Decision Server のイメージストリーム namespace の設定	24
3.2.4. KJAR サービスを使用したイミュータブル Decision Server 用の Business Central インスタンスについての情報の設定	24
3.2.5. KJAR サービスを使用したイミュータブル Decision Server の公開インターネットへの接続のない環境での Maven ミラーへのアクセスの設定	25
3.2.6. KJAR サービスの使用によるイミュータブル Decision Server の RH-SSO 認証パラメーターの設定	26
3.2.7. KJAR サービスの使用によるイミュータブル Decision Server の LDAP 認証パラメーターの設定	27
3.2.8. KJAR サービスの使用によるイミュータブル Decision Server からの Prometheus メトリクス収集の有効化	28
3.2.9. KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行	29
3.3. (任意) LDAP ロールマッピングファイルの指定	29
第4章 RED HAT DECISION MANAGER ロールおよびユーザー	31
第5章 OPENSIFT テンプレートの参考資料	32
5.1. RHDM74-PROD-IMMUTABLE-KIESERVER.YAML テンプレート	32
5.1.1. パラメーター	32
5.1.2. オブジェクト	45
5.1.2.1. サービス	45
5.1.2.2. ルート	46
5.1.2.3. ビルド設定	46
5.1.2.4. デプロイメント設定	46
5.1.2.4.1. トリガー	46
5.1.2.4.2. レプリカ	46
5.1.2.4.3. Pod テンプレート	47

5.1.2.5. 外部の依存関係	57
5.1.2.5.1. シークレット	57
5.2. RHDM74-PROD-IMMUTABLE-KIESERVER-AMQ.YAML テンプレート	57
5.2.1. パラメーター	57
5.2.2. オブジェクト	72
5.2.2.1. サービス	72
5.2.2.2. ルート	73
5.2.2.3. ビルド設定	73
5.2.2.4. デプロイメント設定	74
5.2.2.4.1. トリガー	74
5.2.2.4.2. レプリカ	74
5.2.2.4.3. Pod テンプレート	74
5.2.2.5. 外部の依存関係	88
5.2.2.5.1. シークレット	88
5.3. OPENSIFT の使用に関するクイックリファレンス	88
付録A バージョン情報	90

はじめに

システムエンジニアは、Red Hat OpenShift Container Platform に Red Hat Decision Manager イミュータブルサーバー環境をデプロイして、サービスおよびその他のビジネスアセットを実行するインフラストラクチャーを提供します。イミュータブル Decision Server イメージを管理する標準統合ツールを使用できます。新しいサーバーイメージを作成して、ビジネスアセットを追加および更新できます。

前提条件

- OpenShift クラスター/namespace で 2 ギガバイト以上のメモリーが利用可能である。
- デプロイメントに使用する OpenShift プロジェクトが作成されている。
- **oc** コマンドを使用してプロジェクトにログインしている。**oc** コマンドランツールに関する詳細は、OpenShift の [CLI リファレンス](#) を参照してください。OpenShift Web コンソールを使用してテンプレートをデプロイするには、Web コンソールを使用してログインしている必要もあります。

第1章 RED HAT OPENSIFT CONTAINER PLATFORM における RED HAT DECISION MANAGER の概要

Red Hat Decision Manager は、Red Hat OpenShift Container Platform 環境にデプロイすることができます。

この場合、Red Hat Decision Manager のコンポーネントは、別の OpenShift Pod としてデプロイされます。各 Pod のスケールアップおよびスケールダウンを個別に行い、特定のコンポーネントに必要な数だけコンテナを提供できます。標準の OpenShift の手法を使用して Pod を管理し、負荷を分散できます。

以下の Red Hat Decision Manager の主要コンポーネントが OpenShift で利用できます。

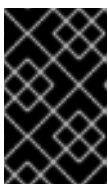
- **Decision Server (実行サーバー (Execution Server) または KIE Server と呼ばれる)** は、インフラストラクチャーの要素でデシジョンサービスやその他のデプロイ可能なアセットを実行します (これらすべてで総称で **サービス** と呼ぶ)。サービスのすべてのロジックは実行サーバーで実行されます。

Decision Server Pod をスケールアップして、同一または異なるホストで実行するコピーを必要な数だけ提供できます。Pod のスケールアップまたはスケールダウンを行うと、そのコピーはすべて同じサービスを実行します。OpenShift は負荷分散を提供しているため、要求はどの Pod でも処理できます。

個別の Decision Server Pod をデプロイして、異なるサービスグループを実行することができます。この Pod もスケールアップやスケールダウンが可能です。複製された個別の Decision Server Pod を必要な数だけ設定することができます。

- **Business Central** は、オーサリングサービスに対する Web ベースのインタラクティブ環境です。Business Central は管理コンソールも提供します。Business Central を使用してサービスを開発し、それらを Decision Server にデプロイできます。Business Central は一元化アプリケーションです。複数の Pod を実行し、同じデータを共有する高可用性用に設定できます。

Business Central には開発するサービスのソースを保管する Git リポジトリが含まれます。また、ビルトインの Maven リポジトリも含まれます。設定に応じて、Business Central はコンパイルしたサービス (KJAR ファイル) をビルドイン Maven リポジトリに配置できます (設定した場合は外部 Maven リポジトリにも可能)。



重要

現在のバージョンでは、高可用性の Business Central 機能はテクノロジープレビュー機能となっています。Red Hat のテクノロジープレビュー機能のサポートの詳細は、[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。

OpenShift 内でさまざまな環境設定にこのコンポーネントおよびその他のコンポーネントを配置できます。

以下の環境タイプが一般的です。

- **オーサリングまたは管理対象の環境:** Business Central 経由でサービスの作成や変更、Decision Server でのサービスの実行に使用可能な環境のアーキテクチャー。この環境は、オーサリング作業用の Business Central を提供する Pod と、サービス実行用の Decision Server 1 つまたは複数を提供する Pod で設定されます。Decision Server それぞれが 1 つの Pod となっており、必要に応じてスケールアップやスケールダウンすることで複製が可能です。Business Central を使用して、各 Decision Server にサービスをデプロイしたり、デプロイ解除したりすることがで

きます。この環境をデプロイする方法については、[Red Hat OpenShift Container Platform への Red Hat Decision Manager オーサリングまたは管理サーバー環境のデプロイ](#) を参照してください。

- **イミュータブルサーバーを使用するデプロイメント:** ステージングおよび実稼働目的で既存のサービスを実行するための代替の環境です。この環境では、Process Server の Pod のデプロイ時に、サービスまたはサービスグループをロードおよび起動するイメージをビルドします。この Pod でサービスを停止したり、新しいサービスを追加したりすることはできません。サービスの別のバージョンを使用したり、別の方法で設定を変更する必要がある場合は、新規のサーバーイメージをデプロイして、古いサーバーと入れ替えます。このシステムでは、Decision Server は OpenShift 環境の他の Pod のように実行されるので、コンテナベースの統合ワークフローはどれでも使用でき、別のツールを使用して Pod を管理する必要はありません。このような環境のデプロイメント手順は、[Red Hat OpenShift Container Platform への Red Hat Decision Manager イミュータブルサーバー環境のデプロイメント](#) を参照してください。

試用 または評価環境をデプロイすることも可能です。この環境には、Business Central と Decision Server が含まれます。この環境はすばやく設定でき、これを使用して、アセットの開発や実行を評価し、体験できます。ただし、この環境では永続ストレージを使用せず、この環境でのいずれの作業も保存されません。この環境のデプロイ方法については、[Red Hat OpenShift Container Platform への Red Hat Decision Manager 試用環境のデプロイ](#) を参照してください。

OpenShift に Red Hat Decision Manager 環境をデプロイするには、Red Hat Decision Manager で用意した OpenShift テンプレートを使用します。

第2章 OPENSIFT 環境に RED HAT DECISION MANAGER をデプロイする準備

OpenShift 環境に Red Hat Decision Manager をデプロイする前に、準備タスクをいくつか完了する必要があります。追加イメージ (たとえば、デシジョンサービスの新しいバージョン、または別のデシジョンサービス) をデプロイする場合は、このタスクを繰り返す必要はありません。

2.1. イメージストリームとイメージレジストリーの可用性確認

Red Hat OpenShift Container Platform で Red Hat Decision Manager コンポーネントをデプロイするには、OpenShift が Red Hat レジストリーから正しいイメージをダウンロードできるようにする必要があります。これらのイメージをダウンロードするために、OpenShift ではイメージの場所情報が含まれる **イメージストリーム** が必要になります。また、OpenShift は、お使いのサービスアカウントのユーザー名とパスワードを使用して Red Hat レジストリーへの認証が行われるように設定する必要があります。

OpenShift 環境のバージョンによっては、必要なイメージストリームが含まれている場合があります。イメージストリームが提供されているかどうかを確認する必要があります。デフォルトでイメージストリームが OpenShift に含まれている場合は、OpenShift インフラストラクチャーがレジストリー認証サーバー用に設定されているのであれば、使用できます。管理者は、OpenShift 環境のインストール時に、レジストリーの認証設定を完了する必要があります。

それ以外の方法として、レジストリー認証を独自のプロジェクトで設定し、イメージストリームをそのプロジェクトにインストールすることができます。

手順

1. Red Hat OpenShift Container Platform が Red Hat レジストリーへのアクセス用に、ユーザー名とパスワードで設定されているかを判断します。必須の設定に関する詳細は、[レジストリーの場所の設定](#) を参照してください。OpenShift オンラインサブスクリプションを使用する場合は、Red Hat レジストリー用のアクセスはすでに設定されています。
2. Red Hat OpenShift Container Platform が Red Hat レジストリーへのアクセス用のユーザー名とパスワードで設定されている場合は、以下のコマンドを実行します。

```
$ oc get imagestreamtag -n openshift | grep rhdm74-decisioncentral-openshift
$ oc get imagestreamtag -n openshift | grep rhdm74-kieserver-openshift
```

両コマンドの出力が空でない場合は、必要なイメージストリームが **openshift** namespace にあるため、これ以外の操作は必要ありません。

3. コマンドの1つまたは複数の出力が空白の場合や、Red Hat レジストリーにアクセスするために、OpenShift をユーザー名およびパスワードで設定していない場合は、以下の手順を実行してください。
 - a. **oc** コマンドで OpenShift にログインして、プロジェクトがアクティブであることを確認します。
 - b. [Registry Service Accounts for Shared Environments](#) で説明されている手順を実行します。Red Hat カスタマーポータルにログインし、このドキュメントにアクセスし、レジストリーサービスアカウントを作成する手順を実行する必要があります。
 - c. **OpenShift Secret** タブを選択し、**Download secret** のリンクをクリックして、YAML シークレットファイルをダウンロードします。
 - d. ダウンロードしたファイルを確認して、**name:** エントリーに記載の名前をメモします。

- e. 以下のコマンドを実行します。

```
oc create -f <file_name>.yaml
oc secrets link default <secret_name> --for=pull
oc secrets link builder <secret_name> --for=pull
```

<file_name> はダウンロードしたファイルに、<secret_name> はファイルの **name:** のエントリに記載されている名前に置き換えてください。

- f. [Software Downloads](#) ページから **rhdm-7.4.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードし、**rhdm74-image-streams.yaml** ファイルを展開します。

- g. 以下のアクションの1つを完了します。

- 以下のコマンドを入力します。

```
$ oc create -f rhdm74-image-streams.yaml
```

- OpenShift Web UI で、**Add to Project** → **Import YAML / JSON**を選択してからファイルを選択するか、またはその内容を貼り付けます。



注記

上記の手順を完了したら、イメージストリームを独自のプロジェクトの名前空間にインストールします。今回の例では、テンプレートのデプロイ時に **IMAGE_STREAM_NAMESPACE** パラメーターをこのプロジェクトの名前に設定する必要があります。

2.2. DECISION SERVER にシークレットの作成

OpenShift は **シークレット** と呼ばれるオブジェクトを使用してパスワードやキーストアなどの機密情報を保持します。OpenShift のシークレットに関する詳細は、OpenShift ドキュメントの [シークレット](#) の章を参照してください。

Decision Server への HTTP アクセス用に SSL 証明書を作成し、これをシークレットとして OpenShift 環境に指定する必要があります。

手順

1. Decision Server の SSL 暗号化の秘密鍵および公開鍵を使用して SSL キーストアを生成します。自己署名または購入した SSL 証明書でキーストアを作成する方法は、[SSL 暗号化キーおよび証明書](#) を参照してください。



注記

実稼働環境で、想定されている Decision Server の URL と一致する、有効な署名済み証明書を生成します。

2. キーストアを **keystore.jks** ファイルに保存します。
3. 証明書の名前をメモします。Red Hat Decision Manager 設定におけるこのデフォルト名は **jboss** です。

4. キーストアファイルのパスワードをメモします。Red Hat Decision Manager 設定におけるこのデフォルト名は **mykeystorepass** です。
5. **oc** コマンドを使用して、新しいキーストアファイルからシークレット **kieserver-app-secret** を生成します。

```
$ oc create secret generic kieserver-app-secret --from-file=keystore.jks
```

2.3. S2I ビルドに使用する BUSINESS CENTRAL からのソースコードの展開

オーサリングサービスに Business Central を使用する場合は、サービスのソースコードを展開して、S2I ビルドを使用する別の Git リポジトリ (GitHub や GitLab のオンプレミスインストールなど) に配置できます。

手順

1. 以下のコマンドを使用してソースコードを展開します。

```
git clone ssh://<adminUser>@<decision-central-host>:8001/<MySpace>/<MyProject>
```

このコマンドでは、以下の変数を置き換えてください。

- **<adminUser>**: Business Central の管理ユーザー
 - **<decision-central-host>**: Business Central を実行しているホスト
 - **<MySpace>**: プロジェクトが配置された Business Central 領域の名前
 - **<MyProject>**: プロジェクトの名前
2. S2I ビルドの別の Git リポジトリ (GitHub または GitLab など) へのソースコードのアップロード

2.4. オフラインで使用する MAVEN ミラーリポジトリの用意

Red Hat OpenShift Container Platform 環境に公開インターネットへの送信アクセスが設定されていない場合には、必要なアーティファクトすべてのミラーが含まれる Maven リポジトリを用意して、このリポジトリを使用できるようにする必要があります。



注記

Red Hat OpenShift Container Platform 環境がインターネットに接続されている場合は、この手順を飛ばして次に進むことができます。

前提条件

- 公開インターネットへの送信アクセスが設定されているコンピューターが利用できる。

手順

1. 書き込み可能な Maven リリースリポジトリを準備します。このリポジトリは、認証なしに読み込みアクセスを許可する必要があります。OpenShift 環境は、このリポジトリへのアク

セスが必要です。OpenShift 環境に、Nexus リポジトリマネージャーをデプロイできます。OpenShift への Nexus の設定方法は、[Nexus の設定](#)を参照してください。このリポジトリをミラーリポジトリとして使用します。また、KJAR サービスからイミュータブルサーバーを作成する予定の場合は、サービスをこのリポジトリに配置します。このリポジトリを外部 Maven リポジトリとして設定する必要があります。イミュータブル環境に別個のミラーリポジトリを設定することはできません。

2. 公開インターネットに送信アクセスができるコンピューターで、以下のアクションを実行します。

- a. 最新版の [Offliner tool](#) をダウンロードします。
- b. Red Hat カスタマーポータル [の Software Downloads](#) ページから利用可能な **rhdm-7.4.0-offliner.txt** の製品配信可能ファイルをダウンロードします。
- c. 以下のコマンドを入力して、Offliner ツールを使用し、必要なアーティファクトをダウンロードします。

```
java -jar offliner-<version>.jar -r https://maven.repository.redhat.com/ga/ -r
https://repo1.maven.org/maven2/ -d /home/user/temp rhdm-7.4.0-offliner.txt
```

/home/user/temp は空の一時ディレクトリーに、**<version>** はダウンロードした Offliner ツールのバージョンに置き換えます。ダウンロードにはかなり時間がかかる可能性があります。

- d. このツールにより、ダウンロードの失敗が報告された場合には、以下のコマンドを入力して初回にダウンロードに失敗したアーティファクトをダウンロードします。

```
grep Path: errors.log | sed -n -e 's/^.*/Path: //p' > failed-downloads.txt
java -jar offliner-<version>.jar -r https://maven.repository.redhat.com/ga/ -r
https://repo1.maven.org/maven2/ -d /home/user/temp failed-downloads.txt
```

もう一度ダウンロードの失敗が報告され、失敗数が初回のダウンロード合計数と比較して少しの場合には、続行してください。

- e. 一時ディレクトリーから作成した Maven リポジトリにすべてのアーティファクトをアップロードします。アーティファクトのアップロードには、[Maven リポジトリプロビジョナーユーティリティー](#)を使用できます。
3. Business Central 外でサービスを開発し、追加の依存関係がある場合は、ミラーリポジトリにその依存関係を追加します。サービスを Maven プロジェクトとして開発した場合は、以下の手順を使用し、これらの依存関係を自動的に用意します。公開インターネットへに送信接続できるコンピューターで、この手順を実行します。
 - a. ローカルの Maven キャッシュディレクトリー (**~/m2/repository**) のバックアップを作成して、ディレクトリーを削除します。
 - b. **mvn clean install** コマンドを使用してプロジェクトのソースをビルドします。
 - c. すべてのプロジェクトで以下のコマンドを入力し、Maven を使用してプロジェクトで生成したすべてのアーティファクトのランタイムの依存関係をすべてダウンロードするようにします。

```
mvn -e -DskipTests dependency:go-offline -f /path/to/project/pom.xml --batch-mode -
Djava.net.preferIPv4Stack=true
```

`/path/to/project/pom.xml` は、プロジェクトの `pom.xml` ファイルへの正しいパスに置き換えます。

- d. ローカルの Maven キャッシュディレクトリー (`~/.m2/repository`) から作成した Maven ミラーリポジトリーにすべてのアーティファクトをアップロードします。アーティファクトのアップロードには、[Maven リポジトリープロビジョナー ユーティリティー](#)を使用できます。

第3章 イミュータブルサーバーを使用した環境

事前に読み込んだサービスで **イミュータブル Decision Server** を実行する 1 つ以上の Pod を含む環境をデプロイできます。必要に応じて、Decision Server Pod ごとに個別にスケーリング可能です。

イメージの作成時に、イミュータブル Decision Server ですべてのサービスをサーバーに読み込む必要があります。実行中のイミュータブル Decision Server でサービスのデプロイまたはデプロイ解除を行うことはできません。このアプローチの利点は、サービスが含まれる Decision Server は他のコンテナ化されたサービスのように実行され、特別な管理が必要ない点です。Decision Server は、OpenShift 環境で他の Pod のように実行され、必要に応じて、コンテナベースの統合ワークフローを使用できます。

Decision Server イメージを作成する場合は、S2I (Source to Image) を使用してサービスをビルドする必要があります。サービスのソースおよびその他のビジネスアセットを使用して Git リポジトリを提供します。Business Central でサービスまたはアセットを開発する場合は、S2I ビルドの個別のリポジトリにソースをコピーします。Business Central でサービスまたはアセットを開発する場合は、S2I ビルドの個別のリポジトリにソースをコピーします。OpenShift は自動的にソースをビルドし、Decision Server イメージにサービスをインストールして、このサービスでコンテナを起動します。

オーサリングサービスに Business Central を使用する場合は、プロセスのソースを展開して、S2I ビルドで使用する別の Git リポジトリ (GitHub や、GitLab のオンプレミスインストールなど) に配置できます。

または、KJAR ファイルとしてすでにビルドされているサービスを使用して同様の Decision Server デプロイメントを作成できます。この場合、サービスを Maven リポジトリに指定する必要があります。Business Central のビルトインリポジトリまたは独自のリポジトリを使用できます (例: Nexus デプロイメント)。サーバー Pod が起動すると、これは KJAR サービスを Maven リポジトリから取得します。Pod 上のサービスが更新したり、変更することはありません。Pod の毎回の再起動またはスケーリング時に、サーバーはリポジトリからファイルを取得するため、デプロイメントをイミュータブルに保つには、それらのファイルが Maven リポジトリで変更されないようにする必要があります。

イミュータブルのイメージを作成する方法はいずれも、イメージの管理が必要ありません。サービスの新規バージョンを使用する場合は、新規イメージをビルドできます。

3.1. S2I ビルドの使用によるイミュータブル DECISION SERVER のデプロイ

S2I ビルドを使用してイミュータブル Decision Server をデプロイできます。サーバーをデプロイする際、デプロイメント手順ではこのサーバーで実行される必要のあるすべてのサービスのソースコードを取得し、サービスをビルドし、それらをサービスイメージに組み込みます。

実行中のイミュータブル Decision Server でサービスのデプロイまたはデプロイ解除を行うことはできません。Business Central を使用すると、モニター情報を表示できます。Decision Server は、OpenShift 環境で他の Pod のように実行され、必要に応じて、コンテナベースの統合ワークフローを使用できます。

イミュータブル Decision Server の JMS 機能を有効にできます。JMS 機能を使用すると、外部 AMQ メッセージブローカーを使用し、JMS API 経由でサーバーと対話できます。

Business Central が同じ namespace にデプロイされる場合、これはイミュータブル Decision Server を自動的に検出します。Business Central を使用してイミュータブル Decision Server でサービスを起動および停止を実行でき (ただしデプロイはできません)、モニターデータを表示できます。

3.1.1. S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始

S2I ビルドを使用してイミュータブル Decision Server をデプロイするには、JMS 機能を有効にする必要がある場合には `rhdm74-prod-immutable-kieserver-amq.yaml` テンプレートファイルを使用します。そうでない場合には、`rhdm74-prod-immutable-kieserver.yaml` テンプレートファイルを使用します。

手順

1. Red Hat カスタマーポータルでの [Software Downloads](#) ページから製品配信可能ファイル `rhdm-7.4.0-openshift-templates.zip` をダウンロードします。
2. 必要なテンプレートファイルを展開します。
3. 以下のいずれかの方法を使用してテンプレートのデプロイを開始します。
 - OpenShift Web UI を使用するには、OpenShift アプリケーションコンソールで **Add to Project → Import YAML / JSON** を選択してから `<template-file-name>.yaml` ファイルを選択または貼り付けます。Add Template ウィンドウで、**Process the template** が選択されていることを確認し、**Continue** をクリックします。
 - OpenShift コマンドラインコンソールを使用するには、以下のコマンドラインを準備します。

```
oc new-app -f <template-path>/&lt;template-file-name&gt;.yaml -p
KIE_SERVER_HTTPS_SECRET=kieserver-app-secret -p PARAMETER=value
```

このコマンドラインで、以下のように変更します。

- `<template-path>` を、ダウンロードしたテンプレートファイルのパスに置き換えます。
- `<template-file-name>` は、テンプレート名に置き換えます。
- 必要なパラメーターに設定するために必要な数だけ `-p PARAMETER=value` ペアを使用します。

次のステップ

テンプレートのパラメーターを設定します。「[S2I の使用によるイミュータブル Decision Server に必要なパラメーターの設定](#)」の手順に従い、共通のパラメーターを設定します。テンプレートファイルを表示して、すべてのパラメーターの説明を確認します。

3.1.2. S2I の使用によるイミュータブル Decision Server に必要なパラメーターの設定

テンプレートをイミュータブル Decision Server を S2I ビルドを使用してデプロイするように設定する際、いずれの場合でも以下のパラメーターを設定する必要があります。

前提条件

- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

1. 以下のパラメーターを設定します。
 - KIE Server キーストアのシークレット名 (`KIE_SERVER_HTTPS_SECRET`): 「[Decision Server にシークレットの作成](#)」で作成した Decision Server のシークレットの名前。

- **KIE Server Certificate Name (KIE_SERVER_HTTPS_NAME):** 「[Decision Server にシークレットの作成](#)」 で作成したキーストアの証明書名。
 - **KIE Server Keystore Password (KIE_SERVER_HTTPS_PASSWORD):** 「[Decision Server にシークレットの作成](#)」 で作成したキーストアのパスワード。
 - **アプリケーション名 (APPLICATION_NAME):** OpenShift アプリケーションの名前。これは Business Central Monitoring および Decision Server のデフォルト URL で使用されます。OpenShift はアプリケーション名を使用して、デプロイメント設定、サービス、ルート、ラベル、およびアーティファクトの個別のセットを作成します。同じテンプレートを同じプロジェクトで使用して複数のアプリケーションをデプロイすることもできますが、その場合はアプリケーション名を同じにすることはできません。また、アプリケーション名は、Decision Server が Business Central で参加するサーバーの設定 (サーバーテンプレート) の名前を決定するものとなります。複数の Decision Server をデプロイする場合には、サーバーごとに異なるアプリケーション名を指定する必要があります。
 - **KIE Server コンテナのデプロイメント (KIE_SERVER_CONTAINER_DEPLOYMENT):** ソースのビルド後にデプロイメントでローカルまたは外部リポジトリからプルする必要のあるデシジョンサービス (KJAR ファイル) の ID 情報。形式は `<containerId>=<groupId>:<artifactId>:<version>` になります。以下の例に示されるように、区切り文字 | を使用して 2 つ以上の KJAR ファイルを指定できます。


```
containerId=groupId:artifactId:version|c2=g2:a2:v2
```

KIE_SERVER_CONTAINER_DEPLOYMENT 値が定義されていない場合、サーバーはプロジェクトの `pom.xml` ファイルを検査してグループ IP、アーティファクト ID およびアーティファクトのバージョンを検出し、アーティファクト ID をコンテナ ID として使用します。コンテナ ID の重複を防ぐには、アーティファクトビルドごとに、またはプロジェクト内で、一意のアーティファクト ID を指定する必要があります。
 - **Git リポジトリ URL (SOURCE_REPOSITORY_URL):** サービスのソースを含む Git リポジトリの URL。
 - **Git 参照 (SOURCE_REPOSITORY_REF):** Git リポジトリのブランチ。
 - **コンテキストディレクトリ (CONTEXT_DIR):** Git リポジトリからダウンロードしたプロジェクト内のソースへのパス。
 - **アーティファクトディレクトリ (ARTIFACT_DIR):** Maven のビルドに成功したあとに必要なバイナリファイル (KJAR ファイル、およびその他の必要なファイル) を含むプロジェクトのパス。通常、このディレクトリはビルドのターゲットディレクトリです。ただし、Git リポジトリのこのディレクトリにビルド済みのバイナリを提供できます。
 - **ImageStream 名前空間 (IMAGE_STREAM_NAMESPACE):** イメージストリームが利用可能な名前空間。OpenShift 環境でイメージストリームが利用可能な場合 (「[イメージストリームとイメージレジストリーの可用性確認](#)」を参照) は、namespace が `openshift` になります。イメージストリームファイルをインストールしている場合は、名前空間が OpenShift プロジェクトの名前になります。
2. 以下のユーザー名とパスワードを設定できます。デフォルトでは、デプロイすると、パスワードが自動生成されます。
- **KIE Server User (KIE_SERVER_USER) および KIE Server Password (KIE_SERVER_PWD):** Decision Server に接続するためにクライアントアプリケーションが使用できるユーザー名およびパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」の手順に従います。

3.1.3. S2I の使用によるイミュータブル Decision Server のイメージストリーム namespace の設定

openshift ではない名前空間でイメージストリームを作成した場合は、テンプレートで名前空間を設定する必要があります。

すべてのイメージストリームが Red Hat OpenShift Container Platform 環境ですでに利用可能な場合は、この手順を省略できます。

前提条件

- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

「[イメージストリームとイメージレジストリーの可用性確認](#)」の説明に従ってイメージストリームファイルをインストールした場合は、**ImageStream Namespace (IMAGE_STREAM_NAMESPACE)** パラメーターを OpenShift プロジェクトの名前に設定します。

3.1.4. S2I の使用によるイミュータブル Decision Server 用の Business Central インスタンスについての情報の設定

同じ namespace で Business Central インスタンスから Decision Server への接続を有効にする必要がある場合は、Business Central インスタンスについての情報を設定する必要があります。

前提条件

- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

1. 以下のパラメーターを設定します。

- **KIE Admin User (KIE_ADMIN_USER)** および **KIE Admin Password (KIE_ADMIN_PWD)**: 管理者ユーザーのユーザー名およびパスワード。これらの値は Business Central の **KIE_ADMIN_USER** および **KIE_ADMIN_PWD** 設定と同じである必要があります。Business Central で RH-SSO または LDAP 認証を使用する場合には、これらのユーザー名とパスワードの値は、Business Central の管理者ロールを使用して認証システムに設定したユーザー名およびパスワードである必要があります。
- **Business Central サービスの名前 (DECISION_CENTRAL_SERVICE)**: Business Central の OpenShift サービス名。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」の手順に従います。

3.1.5. S2I の使用によるイミュータブル Decision Server のオプションの Maven リポジトリの設定

S2I ビルドを使用してテンプレートをイミュータブル Decision Server をデプロイするように設定する際に、ソースビルドに公開 Maven ツリーで利用可能ではない依存関係が含まれ、別個のカスタム Maven リポジトリが必要な場合、リポジトリにアクセスできるようにパラメーターを設定する必要があります。

前提条件

- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

カスタム Maven リポジトリへのアクセスを設定するには、以下のパラメーターを設定します。

- **Maven リポジトリの URL (MAVEN_REPO_URL):** Maven リポジトリの URL。
- **Maven リポジトリの ID (MAVEN_REPO_ID):** Maven リポジトリの ID。デフォルト値は **repo-custom** です。
- **Maven repository username (MAVEN_REPO_USERNAME):** Maven リポジトリのユーザー名。
- **Maven リポジトリのパスワード (MAVEN_REPO_PASSWORD):** Maven リポジトリのパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」の手順に従います。

3.1.6. S2I の使用によるイミュータブル Decision Server の公開インターネットへの接続のない環境での Maven ミラーへのアクセスの設定

S2I ビルドを使用してテンプレートをイミュータブル Decision Server をデプロイするように設定する際に、OpenShift 環境に公開インターネットへの接続がない場合は、「[オフラインで使用する Maven ミラーリポジトリの用意](#)」に従って設定した Maven ミラーへのアクセスを設定する必要があります。

前提条件

- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

Maven ミラーへのアクセスを設定するには、以下のパラメーターを設定します。

- **Maven ミラー URL (MAVEN_MIRROR_URL)**: 「[オフラインで使用する Maven ミラーリポジトリの用意](#)」 で設定した Maven ミラーリポジトリの URL。この URL は、OpenShift 環境の Pod からアクセスできるようにする必要があります。
- **Maven mirror of (MAVEN_MIRROR_OF)**: ミラーから取得されるアーティファクトを定める値。**mirrorOf** 値の設定方法は、Apache Maven ドキュメントの [Mirror Settings](#) を参照してください。デフォルト値は **external:*** です。この値の場合、Maven はミラーから必要なアーティファクトをすべて取得し、他のリポジトリにクエリーを送信しません。
 - 外部の Maven リポジトリ (**MAVEN_REPO_URL**) を設定する場合は、ミラーからこのリポジトリ内のアーティファクトを除外するように **MAVEN_MIRROR_OF** を変更します (例: **external:*;!repo-custom**)。 **repo-custom** は、 **MAVEN_REPO_ID** で設定した ID に置き換えます。
 - 組み込みの Business Central Maven リポジトリ (**BUSINESS_CENTRAL_MAVEN_SERVICE**) を設定した場合には、ミラーからこのリポジトリのアーティファクトを除外するように **MAVEN_MIRROR_OF** を変更します (例: **external:*;!repo-rhdmcentr**)。
 - 両リポジトリを設定した場合は、ミラーから両リポジトリのアーティファクトを除外するように **MAVEN_MIRROR_OF** を変更します (例: **external:*;!repo-rhdmcentr;!repo-custom**)。 **repo-custom** は、 **MAVEN_REPO_ID** で設定した ID に置き換えます。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」 の手順に従います。

3.1.7. S2I の使用によるイミュータブル Decision Server 用の AMQ サーバーとの通信の設定

rhdm74-prod-immutable-kieserver-amq.yaml テンプレートファイルを使用する場合、Decision Server の JMS 機能が有効にされます。外部の AMQ メッセージブローカーを使用して、JMS API 経由でサーバーと対話できます。

環境に必要な場合は、JMS 設定を変更できます。

前提条件

- **rhdm74-prod-immutable-kieserver-amq.yaml** テンプレートファイルを使用して「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」 に説明されているテンプレートの設定を開始していること。

手順

必要に応じて、お使いの環境に以下のパラメーターのいずれかを設定します。

- **AMQ ユーザー名 (AMQ_USERNAME)** および **AMQ パスワード (AMQ_PASSWORD)**: ブローカーのユーザー認証が環境で必要な場合の標準ブローカーユーザーのユーザー名およびパスワード。
- **AMQ ロール (AMQ_ROLE)**: 標準ブローカーユーザーのユーザーロール。デフォルトロールは **admin** です。
- **AMQ キュー (AMQ_QUEUES)**: コンマで区切られた AMQ キュー名。これらのキューはブロー

カーの起動時に自動的に作成され、JBoss EAP サーバーの JNDI リソースとしてアクセスできます。カスタムのキュー名を使用する場合は、同じキュー名を **KIE_SERVER_JMS_QUEUE_RESPONSE** パラメーター、**KIE_SERVER_JMS_QUEUE_REQUEST** パラメーター、**KIE_SERVER_JMS_QUEUE_SIGNAL** パラメーター、**KIE_SERVER_JMS_QUEUE_AUDIT** パラメーター、および **KIE_SERVER_JMS_QUEUE_EXECUTOR** パラメーターに設定する必要があります。

- **AMQ グローバル最大サイズ (AMQ_GLOBAL_MAX_SIZE)**: メッセージデータが消費できるメモリの最大量。値が指定されない場合は、Pod で利用可能なメモリの半分が割り当てられます。
- **AMQ Protocols (AMQ_PROTOCOL)**: コンマで区切られた、Decision Server が AMQ サーバーとの通信に使用できるブローカーのプロトコル。許可される値は、**openwire**、**amqp**、**stomp**、および **mqtt** です。**openwire** のみが JBoss EAP でサポートされます。デフォルト値は **openwire** です。
- **AMQ ブローカーイメージ (AMQ_BROKER_IMAGESTREAM_NAME)**: AMQ ブローカーイメージのイメージストリーム名。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」の手順に従います。

3.1.8. S2I の使用によるイミュータブル Decision Server の RH-SSO 認証パラメーターの設定

RH-SSO 認証を使用する必要がある場合は、テンプレートを S2I ビルドを使用してイミュータブル Decision Server をデプロイするように設定する際に追加の設定を実行します。



重要

LDAP 認証および RH-SSO 認証を同じデプロイメントに設定しないようにしてください。

前提条件

- Red Hat Decision Manager のレلمムが RH-SSO 認証システムに作成されている。
- Red Hat Decision Manager のユーザー名およびパスワードが RH-SSO 認証システムに作成されている。利用可能なロールの一覧については、[4章 Red Hat Decision Manager ロールおよびユーザー](#)を参照してください。環境のパラメーターを設定するには、**kie-server,rest-all,admin** ロールを持つ管理者ユーザーが必要です。このユーザーのデフォルトユーザー名は **adminUser** です。このユーザーは環境を管理し、これを使用できます。
- デプロイしている Red Hat Decision Manager 環境の全コンポーネントに対して、クライアントが RH-SSO 認証システムに作成されている。クライアントのセットアップには、コンポーネントの URL が含まれます。環境のデプロイ後に URL を確認し、編集できます。または、Red Hat Decision Manager のデプロイメントでクライアントを作成できます。ただし、このオプションの環境に対する制御の詳細度合はより低くなります。
- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

1. テンプレートの **KIE_ADMIN_USER** および **KIE_ADMIN_PASSWORD** パラメーターを、RH-SSO 認証システムで作成したユーザー名およびパスワードに設定します。
2. 以下のパラメーターを設定します。
 - **RH-SSO URL (SSO_URL)**: RH-SSO の URL。
 - **RH-SSO レルム名 (SSO_REALM)**: Red Hat Decision Manager の RH-SSO レルム。
 - **RH-SSO が無効な SSL 証明書の検証 (SSO_DISABLE_SSL_CERTIFICATE_VALIDATION)**: RH-SSO インストールで有効な HTTPS 証明書を使用していない場合は **true** に設定します。
3. 以下の手順のいずれかを実行します。
 - a. RH-SSO で Red Hat Decision Manager のクライアントを作成した場合は、テンプレートで以下のパラメーターを設定します。
 - **Business Central RH-SSO クライアント名 (DECISION_CENTRAL_SSO_CLIENT)**: Business Central の RH-SSO クライアント名。
 - **KIE Server の RH-SSO クライアント名 (KIE_SERVER_SSO_CLIENT)**: Decision Server の RH-SSO クライアント名。
 - **KIE Server の RH-SSO クライアントのシークレット (KIE_SERVER_SSO_SECRET)**: Decision Server のクライアントに対して RH-SSO に設定するシークレットの文字列。
 - b. RH-SSO に Red Hat Decision Manager のクライアントを作成する場合は、テンプレートで以下のパラメーターを設定します。
 - **KIE Server の RH-SSO クライアント名 (KIE_SERVER_SSO_CLIENT)**: Decision Server 向けに RH-SSO に作成するクライアント名。
 - **KIE Server の RH-SSO クライアントのシークレット (KIE_SERVER_SSO_SECRET)**: Decision Server のクライアントに対して RH-SSO に設定するシークレットの文字列。
 - **RH-SSO レルムの管理者のユーザー名 (SSO_USERNAME)** および **RH-SSO レルムの管理者のパスワード (SSO_PASSWORD)**: Red Hat Decision Manager の RH-SSO レルムの管理者ユーザーに指定するユーザー名とパスワード必要なクライアントを作成するためにこのユーザー名およびパスワードを指定する必要があります。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」の手順に従います。

デプロイの完了後に、RH-SSO 認証システムで Red Hat Decision Manager のコンポーネントの URL が正しいことを確認してください。

3.1.9. S2I の使用によるイミュータブル Decision Server の LDAP 認証パラメーターの設定

LDAP 認証を使用する必要がある場合は、テンプレートを S2I ビルドを使用してイミュータブル Decision Server をデプロイするように設定する際に追加の設定を実行します。



重要

LDAP 認証および RH-SSO 認証を同じデプロイメントに設定しないようにしてください。

前提条件

- LDAP システムに Red Hat Decision Manager のユーザー名およびパスワードを作成している。利用可能なロールの一覧については、[4章 Red Hat Decision Manager ロールおよびユーザー](#) を参照してください。この環境のパラメーターを設定するために、少なくとも以下のユーザーを作成する必要があります。
 - **kie-server,rest-all,admin** ロールを持つ管理者ユーザー。このユーザーは環境を管理し、これを使用できます。
 - **kie-server,rest-all,user** ロールを持つサーバーユーザー。このユーザーは、Decision Server に対する REST API 呼び出しを実行できます。
- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」 に説明されているようにテンプレートの設定を開始している。

手順

1. LDAP サービスでは、デプロイメントパラメーターですべてのユーザー名を作成します。パラメーターを設定しない場合には、デフォルトのユーザー名を使用してユーザーを作成します。作成したユーザーにはロールに割り当てる必要もあります。
 - **KIE_ADMIN_USER**: デフォルトのユーザー名 **adminUser**、ロール: **kie-server,rest-all,admin**
 - **KIE_SERVER_USER**: デフォルトのユーザー名 **executionUser**、ロール **kie-server,rest-all,guest**
LDAP で設定可能なユーザーロールについては、[ロールおよびユーザー](#) を参照してください。
2. テンプレートの **AUTH_LDAP*** パラメーターを設定します。これらのパラメーターは、Red Hat JBoss EAP の **LdapExtended** ログインモジュールの設定に対応します。これらの設定に関する説明は、[LdapExtended ログインモジュール](#) を参照してください。
LDAP サーバーがデプロイメントに必要な全ロールを定義していない場合は、LDAP グループを Red Hat Decision Manager ロールにマッピングしてください。LDAP のロールマッピングを有効にするには、以下のパラメーターを設定します。
 - **RoleMapping rolesProperties** ファイルパス (**AUTH_ROLE_MAPPER_ROLES_PROPERTIES**):
/opt/eap/standalone/configuration/rolemapping/rolemapping.properties など、ロールのマッピングを定義するファイルの完全修飾パス名。このファイルを指定して、該当するすべてのデプロイメント設定でこのパスにマウントする必要があります。これを実行する方法については、「[\(任意\) LDAP ロールマッピングファイルの指定](#)」を参照してください。
 - **RoleMapping replaceRole** プロパティ (**AUTH_ROLE_MAPPER_REPLACE_ROLE**):
true に設定した場合、マッピングしたロールは、LDAP サーバーに定義したロールに置き換えられます。**false** に設定した場合は、LDAP サーバーに定義したロールと、マッピングしたロールの両方がユーザーアプリケーションロールとして設定されます。デフォルトの設定は **false** です。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」の手順に従います。

3.1.10. S2I の使用によるイミュータブル Decision Server の Prometheus メトリクス収集の有効化

Decision Server デプロイメントを Prometheus を使用してメトリクスを収集し、保存するように設定する必要がある場合、デプロイ時に Decision Server でこの機能のサポートを有効にします。

前提条件

- 「[S2I の使用によるイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

Prometheus メトリクス収集のサポートを有効にするには、**Prometheus Server 拡張無効 (PROMETHEUS_SERVER_EXT_DISABLED)** パラメーターを **false** に設定します。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始](#)」の手順に従います。

Prometheus メトリクス収集の方法については、[Decision Server の管理および監視](#)を参照してください。

3.1.11. S2I の使用によるイミュータブル Decision Server テンプレートのデプロイの開始

OpenShift Web UI またはコマンドラインに必要なすべてのパラメーターを設定した後に、テンプレートのデプロイを実行します。

手順

使用している方法に応じて、以下の手順を実行します。

- OpenShift Web UI の場合は **Create** をクリックします。
 - **This will create resources that may have security or project behavior implications** メッセージが表示された場合は、**Create Anyway** をクリックします。
- コマンドラインに入力して、Enter キーを押します。

3.2. KJAR サービスからのイミュータブル DECISION SERVER のデプロイ

KJAR ファイルとしてすでにビルドされているサービスを使用して、イミュータブル Decision Server をデプロイできます。

サービスを Maven リポジトリに指定する必要があります。Business Central のビルトインリポジトリまたは独自のリポジトリを使用できます (例: Nexus デプロイメント)。サーバー Pod が起動すると、これは KJAR サービスを Maven リポジトリから取得します。Pod 上のサービスが更新したり、

変更することはありません。Pod の毎回の再起動またはスケーリング時に、サーバーはリポジトリからファイルを取得するため、デプロイメントをイミュータブルに保つには、それらのファイルが Maven リポジトリで変更されないようにする必要があります。

実行中のイミュータブル Decision Server でサービスのデプロイまたはデプロイ解除を行うことはできません。Business Central を使用すると、モニター情報を表示できます。Decision Server は、OpenShift 環境で他の Pod のように実行され、必要に応じて、コンテナベースの統合ワークフローを使用できます。

Business Central が同じ namespace にデプロイされる場合、これはイミュータブル Decision Server を自動的に検出します。Business Central を使用してイミュータブル Decision Server でサービスを起動および停止を実行でき（ただしデプロイはできません）、モニターデータを表示できます。

3.2.1. KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始

KJAR サービスからイミュータブル Decision Server をデプロイするには、`rhdm74-kieserver.yaml` テンプレートファイルを使用します。このファイルは、

手順

1. Red Hat カスタマーポータル [の Software Downloads](#) ページから製品配信可能ファイル `rhdm-7.4.0-openshift-templates.zip` をダウンロードします。
2. `rhdm74-kieserver.yaml` テンプレートファイルを展開します。
3. 以下のいずれかの方法を使用してテンプレートのデプロイを開始します。
 - OpenShift Web UI を使用するには、OpenShift アプリケーションコンソールで **Add to Project → Import YAML / JSON** を選択してから、`rhdm74-kieserver.yaml` ファイルを選択するか、またはこれを貼り付けます。Add Template ウィンドウで、**Process the template** が選択されていることを確認し、**Continue** をクリックします。
 - OpenShift コマンドラインコンソールを使用するには、以下のコマンドラインを準備します。

```
oc new-app -f <template-path>/rhdm74-kieserver.yaml -p
KIE_SERVER_HTTPS_SECRET=kieserver-app-secret -p PARAMETER=value
```

このコマンドラインで、以下のように変更します。

- `<template-path>` を、ダウンロードしたテンプレートファイルのパスに置き換えます。
- 必要なパラメーターに設定するために必要な数だけ `-p PARAMETER=value` ペアを使用します。

次のステップ

テンプレートのパラメーターを設定します。「[KJAR サービスからのイミュータブル Decision Server のパラメーターの設定](#)」の手順に従い、共通のパラメーターを設定します。テンプレートファイルを表示して、すべてのパラメーターの説明を確認します。

3.2.2. KJAR サービスからのイミュータブル Decision Server のパラメーターの設定

テンプレートをイミュータブル Decision Server を KJAR サービスからデプロイするように設定する際、いずれの場合でも以下のパラメーターを設定する必要があります。

前提条件

- 「KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始」 に説明されているようにテンプレートの設定を開始している。

手順

1. 以下のパラメーターを設定します。

- KIE Server キーストアのシークレット名(KIE_SERVER_HTTPS_SECRET): 「Decision Server にシークレットの作成」 で作成した Decision Server のシークレットの名前。
- KIE Server Certificate Name(KIE_SERVER_HTTPS_NAME): 「Decision Server にシークレットの作成」 で作成したキーストアの証明書名。
- KIE Server Keystore Password(KIE_SERVER_HTTPS_PASSWORD): 「Decision Server にシークレットの作成」 で作成したキーストアのパスワード。
- アプリケーション名 (APPLICATION_NAME): OpenShift アプリケーションの名前。これは Business Central Monitoring および Decision Server のデフォルト URL で使用されます。OpenShift はアプリケーション名を使用して、デプロイメント設定、サービス、ルート、ラベル、およびアーティファクトの個別のセットを作成します。同じテンプレートを同じプロジェクトで使用して複数のアプリケーションをデプロイすることもできますが、その場合はアプリケーション名を同じにすることはできません。また、アプリケーション名は、Decision Server が Business Central で参加するサーバーの設定 (サーバーテンプレート) の名前を決定するものとなります。複数の Decision Server をデプロイする場合には、サーバーごとに異なるアプリケーション名を指定する必要があります。
- Maven repository URL(MAVEN_REPO_URL): Maven リポジトリーの URL。Decision Server にデプロイするすべてのプロセス (KJAR ファイル) をこのリポジトリーにアップロードする必要があります。
- Maven リポジトリーの ID(MAVEN_REPO_ID): Maven リポジトリーの ID。デフォルト値は **repo-custom** です。
- Maven repository username(MAVEN_REPO_USERNAME): Maven リポジトリーのユーザー名。
- Maven リポジトリーのパスワード (MAVEN_REPO_PASSWORD): Maven リポジトリーのパスワード。
- KIE Server コンテナのデプロイメント (KIE_SERVER_CONTAINER_DEPLOYMENT): デプロイメントが Maven リポジトリーからプルする必要のあるデシジョンサービス (KJAR ファイル) の識別情報。形式は `<containerId>=<groupId>:<artifactId>:<version>` になります。以下の例に示されるように、区切り文字 | を使用して 2 つ以上の KJAR ファイルを指定できます。

```
containerId=groupId:artifactId:version|c2=g2:a2:v2
```

- KIE Server Mode(KIE_SERVER_MODE): rhdm74-kieserver-*.yaml テンプレートで、デフォルト値は **PRODUCTION** です。PRODUCTION モードでは、**SNAPSHOT** バージョンの KJAR アーティファクトは Decision Server にデプロイできず、既存のコンテナでアーティファクトのバージョンを変更することはできません。PRODUCTION モードで新規バージョンをデプロイするには、同じ Decision Server で新規コンテナを作成します。SNAPSHOT バージョンをデプロイするか、または既存コンテナのアーティファクトのバージョンを変更するには、このパラメーターを **DEVELOPMENT** に設定します。

- **ImageStream 名前空間 (IMAGE_STREAM_NAMESPACE)**: イメージストリームが利用可能な名前空間。OpenShift 環境でイメージストリームが利用可能な場合 ([「イメージストリームとイメージレジストリーの可用性確認」](#) を参照) は、namespace が **openshift** になります。イメージストリームファイルをインストールしている場合は、名前空間が OpenShift プロジェクトの名前になります。
2. 以下のユーザー名とパスワードを設定できます。デフォルトでは、デプロイすると、パスワードが自動生成されます。
 - **KIE Server User (KIE_SERVER_USER)** および **KIE Server Password (KIE_SERVER_PWD)**: Decision Server に接続するためにクライアントアプリケーションが使用できるユーザー名およびパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、[「KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行」](#) の手順に従います。

3.2.3. イミュータブル Decision Server のイメージストリーム namespace の設定

openshift ではない名前空間でイメージストリームを作成した場合は、テンプレートで名前空間を設定する必要があります。

すべてのイメージストリームが Red Hat OpenShift Container Platform 環境ですでに利用可能な場合は、この手順を省略できます。

前提条件

- [「KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始」](#) に説明されているようにテンプレートの設定を開始している。

手順

[「イメージストリームとイメージレジストリーの可用性確認」](#) の説明に従ってイメージストリームファイルをインストールした場合は、**ImageStream Namespace (IMAGE_STREAM_NAMESPACE)** パラメーターを OpenShift プロジェクトの名前に設定します。

3.2.4. KJAR サービスを使用したイミュータブル Decision Server 用の Business Central インスタンスについての情報の設定

同じ namespace で Business Central インスタンスから Decision Server への接続を有効にする必要がある場合は、Business Central インスタンスについての情報を設定する必要があります。

前提条件

- [「KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始」](#) に説明されているようにテンプレートの設定を開始している。

手順

1. 以下のパラメーターを設定します。

- **KIE Admin User (KIE_ADMIN_USER)** および **KIE Admin Password (KIE_ADMIN_PWD)**: 管理者ユーザーのユーザー名およびパスワード。これらの値は Business Central の

KIE_ADMIN_USER および **KIE_ADMIN_PWD** 設定と同じである必要があります。
Business Central で RH-SSO または LDAP 認証を使用する場合には、これらのユーザー名とパスワードの値は、Business Central の管理者ロールを使用して認証システムに設定したユーザー名およびパスワードである必要があります。

- **Business Central サービスの名前 (DECISION_CENTRAL_SERVICE)**: Business Central の OpenShift サービス名。
2. 以下の設定が Business Central の同じ設定と同じ値に設定されていることを確認します。
- **Maven repository URL (MAVEN_REPO_URL)**: サービスのデプロイに使用する必要のある外部 Maven リポジトリーの URL。
 - **Maven repository username (MAVEN_REPO_USERNAME)**: Maven リポジトリーのユーザー名。
 - **Maven リポジトリーのパスワード (MAVEN_REPO_PASSWORD)**: Maven リポジトリーのパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行](#)」の手順に従います。

3.2.5. KJAR サービスを使用したイミュータブル Decision Server の公開インターネットへの接続のない環境での Maven ミラーへのアクセスの設定

KJAR サービスを使用してテンプレートをイミュータブル Decision Server をデプロイするように設定する際に、OpenShift 環境に公開インターネットへの接続がない場合は、「[オフラインで使用する Maven ミラーリポジトリーの用意](#)」に従って設定した Maven ミラーへのアクセスを設定する必要があります。

前提条件

- 「[KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

Maven ミラーへのアクセスを設定するには、以下のパラメーターを設定します。

- **Maven ミラー URL (MAVEN_MIRROR_URL)**: 「[オフラインで使用する Maven ミラーリポジトリーの用意](#)」で設定した Maven ミラーリポジトリーの URL。この URL は、OpenShift 環境の Pod からアクセスできるようにする必要があります。
- **Maven mirror of (MAVEN_MIRROR_OF)**: ミラーから取得されるアーティファクトを定める値。**mirrorOf** 値の設定方法は、Apache Maven ドキュメントの [Mirror Settings](#) を参照してください。デフォルト値は **external:*** です。この値の場合、Maven はミラーから必要なアーティファクトをすべて取得し、他のリポジトリーにクエリーを送信しません。
 - 外部の Maven リポジトリー (**MAVEN_REPO_URL**) を設定する場合は、ミラーからこのリポジトリー内のアーティファクトを除外するように **MAVEN_MIRROR_OF** を変更します (例: **external:*;!repo-custom**)。repo-custom は、**MAVEN_REPO_ID** で設定した ID に置き換えます。

- 組み込みの Business Central Maven リポジトリ (**BUSINESS_CENTRAL_MAVEN_SERVICE**) を設定した場合には、ミラーからこのリポジトリのアーティファクトを除外するように **MAVEN_MIRROR_OF** を変更します (例: `external:*;!repo-rhdmcentr`)。
- 両リポジトリを設定した場合は、ミラーから両リポジトリのアーティファクトを除外するように **MAVEN_MIRROR_OF** を変更します (例: `external:*;!repo-rhdmcentr;!repo-custom`)。 **repo-custom** は、**MAVEN_REPO_ID** で設定した ID に置き換えます。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行](#)」の手順に従います。

3.2.6. KJAR サービスの使用によるイミュータブル Decision Server の RH-SSO 認証パラメーターの設定

RH-SSO 認証を使用する必要がある場合は、テンプレートを KJAR サービスを使用してイミュータブル Decision Server をデプロイするように設定する際に追加の設定を実行します。



重要

LDAP 認証および RH-SSO 認証を同じデプロイメントに設定しないようにしてください。

前提条件

- Red Hat Decision Manager のレルムが RH-SSO 認証システムに作成されている。
- Red Hat Decision Manager のユーザー名およびパスワードが RH-SSO 認証システムに作成されている。利用可能なロールの一覧については、[4章 Red Hat Decision Manager ロールおよびユーザー](#) を参照してください。環境のパラメーターを設定するには、**kie-server,rest-all,admin** ロールを持つ管理者ユーザーが必要です。このユーザーのデフォルトユーザー名は **adminUser** です。このユーザーは環境を管理し、これを使用できます。
- デプロイしている Red Hat Decision Manager 環境の全コンポーネントに対して、クライアントが RH-SSO 認証システムに作成されている。クライアントのセットアップには、コンポーネントの URL が含まれます。環境のデプロイ後に URL を確認し、編集できます。または、Red Hat Decision Manager のデプロイメントでクライアントを作成できます。ただし、このオプションの環境に対する制御の詳細度合はより低くなります。
- 「[KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

1. テンプレートの **KIE_ADMIN_USER** および **KIE_ADMIN_PASSWORD** パラメーターを、RH-SSO 認証システムで作成したユーザー名およびパスワードに設定します。
2. 以下のパラメーターを設定します。
 - **RH-SSO URL (SSO_URL)**: RH-SSO の URL。
 - **RH-SSO レルム名 (SSO_REALM)**: Red Hat Decision Manager の RH-SSO レルム。

- **RH-SSO が無効な SSL 証明書の検証 (SSO_DISABLE_SSL_CERTIFICATE_VALIDATION):** RH-SSO インストールで有効な HTTPS 証明書を使用していない場合は **true** に設定します。

3. 以下の手順のいずれかを実行します。

- a. RH-SSO で Red Hat Decision Manager のクライアントを作成した場合は、テンプレートで以下のパラメーターを設定します。
 - **Business Central RH-SSO クライアント名 (DECISION_CENTRAL_SSO_CLIENT):** Business Central の RH-SSO クライアント名。
 - **KIE Server の RH-SSO クライアント名 (KIE_SERVER_SSO_CLIENT):** Decision Server の RH-SSO クライアント名。
 - **KIE Server の RH-SSO クライアントのシークレット (KIE_SERVER_SSO_SECRET):** Decision Server のクライアントに対して RH-SSO に設定するシークレットの文字列。
- b. RH-SSO に Red Hat Decision Manager のクライアントを作成する場合は、テンプレートで以下のパラメーターを設定します。
 - **KIE Server の RH-SSO クライアント名 (KIE_SERVER_SSO_CLIENT):** Decision Server 向けに RH-SSO に作成するクライアント名。
 - **KIE Server の RH-SSO クライアントのシークレット (KIE_SERVER_SSO_SECRET):** Decision Server のクライアントに対して RH-SSO に設定するシークレットの文字列。
 - **RH-SSO レルムの管理者のユーザー名 (SSO_USERNAME) および RH-SSO レルムの管理者のパスワード (SSO_PASSWORD):** Red Hat Decision Manager の RH-SSO レルムの管理者ユーザーに指定するユーザー名とパスワード必要なクライアントを作成するためにこのユーザー名およびパスワードを指定する必要があります。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行](#)」の手順に従います。

デプロイの完了後に、RH-SSO 認証システムで Red Hat Decision Manager のコンポーネントの URL が正しいことを確認してください。

3.2.7. KJAR サービスの使用によるイミュータブル Decision Server の LDAP 認証パラメーターの設定

LDAP 認証を使用する必要がある場合は、テンプレートを KJAR サービスを使用してイミュータブル Decision Server をデプロイするように設定する際に追加の設定を実行します。



重要

LDAP 認証および RH-SSO 認証を同じデプロイメントに設定しないようにしてください。

前提条件

- LDAP システムに Red Hat Decision Manager のユーザー名およびパスワードを作成している。利用可能なロールの一覧については、[4章 Red Hat Decision Manager ロールおよびユーザー](#) を

参照してください。この環境のパラメーターを設定するために、少なくとも以下のユーザーを作成する必要があります。

- **kie-server,rest-all,admin** ロールを持つ管理者ユーザー。このユーザーは環境を管理し、これを使用できます。
 - **kie-server,rest-all,user** ロールを持つサーバーユーザー。このユーザーは、Decision Server に対する REST API 呼び出しを実行できます。
- 「[KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

1. LDAP サービスでは、デプロイメントパラメーターですべてのユーザー名を作成します。パラメーターを設定しない場合には、デフォルトのユーザー名を使用してユーザーを作成します。作成したユーザーにはロールに割り当てる必要もあります。
 - **KIE_ADMIN_USER**: デフォルトのユーザー名 **adminUser**、ロール: **kie-server,rest-all,admin**
 - **KIE_SERVER_USER**: デフォルトのユーザー名 **executionUser**、ロール **kie-server,rest-all,guest**
LDAP で設定可能なユーザーロールについては、[ロールおよびユーザー](#) を参照してください。
2. テンプレートの **AUTH_LDAP*** パラメーターを設定します。これらのパラメーターは、Red Hat JBoss EAP の **LdapExtended** ログインモジュールの設定に対応します。これらの設定に関する説明は、[LdapExtended ログインモジュール](#) を参照してください。
LDAP サーバーがデプロイメントに必要な全ロールを定義していない場合は、LDAP グループを Red Hat Decision Manager ロールにマッピングしてください。LDAP のロールマッピングを有効にするには、以下のパラメーターを設定します。
 - **RoleMapping rolesProperties** ファイルパス (**AUTH_ROLE_MAPPER_ROLES_PROPERTIES**):
/opt/eap/standalone/configuration/rolemapping/rolemapping.properties など、ロールのマッピングを定義するファイルの完全修飾パス名。このファイルを指定して、該当するすべてのデプロイメント設定でこのパスにマウントする必要があります。これを実行する方法については、「[\(任意\) LDAP ロールマッピングファイルの指定](#)」を参照してください。
 - **RoleMapping replaceRole** プロパティ (**AUTH_ROLE_MAPPER_REPLACE_ROLE**):
true に設定した場合、マッピングしたロールは、LDAP サーバーに定義したロールに置き換えられます。**false** に設定した場合は、LDAP サーバーに定義したロールと、マッピングしたロールの両方がユーザーアプリケーションロールとして設定されます。デフォルトの設定は **false** です。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行](#)」の手順に従います。

3.2.8. KJAR サービスの使用によるイミュータブル Decision Server からの Prometheus メトリクス収集の有効化

Decision Server デプロイメントを Prometheus を使用してメトリクスを収集し、保存するように設定する必要がある場合、デプロイ時に Decision Server でこの機能のサポートを有効にします。

前提条件

- 「[KJAR サービスでのイミュータブル Decision Server のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

手順

Prometheus メトリクス収集のサポートを有効にするには、**Prometheus Server 拡張無効 (PROMETHEUS_SERVER_EXT_DISABLED)** パラメーターを **false** に設定します。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行](#)」の手順に従います。

Prometheus メトリクス収集の方法については、[Decision Server の管理および監視](#)を参照してください。

3.2.9. KJAR サービスの使用によるイミュータブル Decision Server テンプレートデプロイの実行

OpenShift Web UI またはコマンドラインに必要なすべてのパラメーターを設定した後に、テンプレートのデプロイを実行します。

手順

使用している方法に応じて、以下の手順を実行します。

- OpenShift Web UI の場合は **Create** をクリックします。
 - **This will create resources that may have security or project behavior implications** メッセージが表示された場合は、**Create Anyway** をクリックします。
- コマンドラインに入力して、Enter キーを押します。

3.3. (任意) LDAP ロールマッピングファイルの指定

AUTH_ROLE_MAPPER_ROLES_PROPERTIES パラメーターを設定する場合は、ロールマッピングを定義するファイルを指定する必要があります。影響を受けるすべてのデプロイメント設定にこのファイルをマウントしてください。

手順

1. **my-role-map** など、ロールマッピングのプロパティファイルを作成します。ファイルには、次の形式のエントリが含まれている必要があります。

```
ldap_role = product_role1, product_role2...
```

以下に例を示します。

```
admins = kie-server,rest-all,admin
```

- 以下のコマンドを入力して、このファイルから OpenShift 設定ファイルのマッピングを作成します。

```
oc create configmap ldap-role-mapping --from-file=<new_name>=<existing_name>
```

<new_name> は、Pod に指定するファイルの名前 (**AUTH_ROLE_MAPPER_ROLES_PROPERTIES** ファイルで指定した名前と同じである必要があります) に置き換えます。また、**<existing_name>** は、作成したファイル名に置き換えます。以下に例を示します。

```
oc create configmap ldap-role-mapping --from-file=rolemapping.properties=my-role-map
```

- ロールマッピング用に指定した全デプロイメント設定に設定マップをマウントします。以下のデプロイメント設定は、この環境で影響を受ける可能性があります。

- **myapp-kieserver**: Decision Server

myapp はアプリケーション名に置き換えます。複数の Decision Server のデプロイメントが異なるアプリケーション名で存在する可能性があります。

すべてのデプロイメント設定について、以下のコマンドを実行します。

```
oc set volume dc/<deployment_config_name> --add --type configmap --configmap-name ldap-role-mapping --mount-path=<mapping_dir> --name=ldap-role-mapping
```

<mapping_dir> は、**/opt/eap/standalone/configuration/rolemapping** など、**AUTH_ROLE_MAPPER_ROLES_PROPERTIES** で設定したディレクトリー名 (ファイル名なし) に置き換えます。

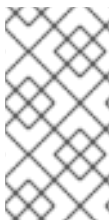
第4章 RED HAT DECISION MANAGER ロールおよびユーザー

Business Central または Decision Server にアクセスするには、サーバーを起動する前にユーザーを作成して適切なロールを割り当てます。

Business Central と Decision Server は、JAVA 認証承認サービス (JAAS) ログインモジュールを使用してユーザーを認証します。Business Central と Decision Server の両方が単一のインスタンスで実行されている場合は、同じ JAAS サブジェクトとセキュリティドメインを共有します。したがって、Business Central に対して認証されたユーザーは、Decision Server にもアクセスできます。

ただし、Business Central と Decision Server が異なるインスタンスで実行されている場合、JAAS ログインモジュールは両方に対して個別にトリガーされます。したがって、Business Central で認証されたユーザーは、Decision Server にアクセス (Business Central でプロセス定義を表示または管理など) するための個別認証が必要となります。ユーザーが Decision Server で認証されていない場合は、ログファイルに 401 エラーが記録され、Business Central に **Invalid credentials to load data from remote server.Contact your system administrator.** メッセージが表示されます。

本セクションでは、利用可能な Red Hat Decision Manager のユーザーロールを説明します。



注記

admin、**analyst**、および **rest-all** のロールは Business Central 用に予約されています。**kie-server** ロールは Decision Server 用に予約されています。このため、Business Central または Decision Server のいずれか、またはそれら両方がインストールされているかどうかによって、利用可能なロールは異なります。

- **admin:** **admin** ロールを持つユーザーは Business Central 管理者です。管理者は、ユーザーの管理や、リポジトリの作成、クローン作成、および管理ができます。アプリケーションで必要な変更をすべて利用できます。**admin** ロールを持つユーザーは、Red Hat Decision Manager の全領域にアクセスできます。
- **analyst:** **analyst** ロールを持つユーザーには、すべてのハイレベル機能へのアクセスがあります。プロジェクトのモデル化が可能です。ただし、このユーザーは、**Design → Projects** ビューでスペースに貢献者を追加したり、スペースを削除したりできません。**analyst** ロールを持つユーザーは、管理者向けの **Deploy → Execution Servers** ビューにアクセスできません。ただし、これらのユーザーは、ライブラリーパースペクティブにアクセスするときに **Deploy** ボタンを使用できます。
- **rest-all:** **rest-all** ロールを持つユーザーは、Business Central REST 機能にアクセスできます。
- **kie-server:** **kie-server** ロールを持つユーザーは Decision Server (KIE サーバー) REST 機能へのアクセスがあります。このロールは、Business Central で Manage ビューおよび Track ビューにアクセスするユーザーに必要になります。

第5章 OPENSIFT テンプレートの参考資料

Red Hat Decision Manager には、以下の OpenShift テンプレートが含まれています。このテンプレートにアクセスするには、Red Hat カスタマーポータルでの [Software Downloads](#) ページから、製品の配信可能ファイル `rhdm-7.4.0-openshift-templates.zip` をダウンロードして展開します。

- `rhdm74-prod-immutable-kieserver.yaml` で、イミュータブル Decision Server が設定されます。このテンプレートのデプロイメントには、Decision Server 上で実行予定の1つまたは複数サービスの source-to-image (S2I) ビルドが含まれます。このテンプレートの詳細は、「[rhdm74-prod-immutable-kieserver.yaml テンプレート](#)」を参照してください。
- `rhdm74-prod-immutable-kieserver-amq.yaml` で、イミュータブル Decision Server が設定されます。このテンプレートのデプロイメントには、Decision Server 上で実行予定の1つまたは複数サービスの source-to-image (S2I) ビルドが含まれます。このバージョンのテンプレートには、JMS 統合が含まれます。このテンプレートの詳細は、「[rhdm74-prod-immutable-kieserver-amq.yaml テンプレート](#)」を参照してください。

5.1. RHDM74-PROD-IMMUTABLE-KIESERVER.YAML テンプレート

Red Hat Decision Manager 7.4 での実稼働環境におけるイミュータブル KIE サーバー向けのアプリケーションテンプレート

5.1.1. パラメーター

テンプレートを使用すると値を引き継ぐパラメーターを定義でき、パラメーターの参照時には、この値が代入されます。この値は、パラメーターの参照時には、この値が代入されます。参照はオブジェクト一覧フィールドの任意のテキストフィールドで定義できます。詳細は、[Openshift ドキュメント](#) を参照してください。

変数名	イメージの環境変数	説明	値の例	必須
APPLICATION_NAME	–	アプリケーションの名前。	myapp	True
KIE_ADMIN_USER	KIE_ADMIN_USER	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PASSWORD	KIE_ADMIN_PASSWORD	KIE 管理者のパスワード	–	False
KIE_SERVER_USER	KIE_SERVER_USER	KIE サーバーのユーザー名。 (org.kie.server.user システムプロパティを設定する)	executionUser	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_PWD	KIE_SERVER_PWD	KIE サーバーへの接続に使用する KIE サーバーパスワード。値はデフォルトで自動的に生成されます。(org.kie.server.pwd システムプロパティを設定する)	–	False
IMAGE_STREAM_NAMESPACE	–	Red Hat ミドルウェアイメージの ImageStreams がインストールされている namespace これらの ImageStreams は通常 OpenShift の名前空間にインストールされています。ImageStreams を別の namespace/プロジェクトにインストールしている場合には、これを変更するだけで結構です。	openshift	True
KIE_SERVER_IMAGE_STREAM_NAME	–	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm74-kieserver-openshift です。	rhdm74-kieserver-openshift	True
IMAGE_STREAM_TAG	–	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 1.0 です。	1.0	True

変数名	イメージの環境変数	説明	値の例	必須
KIE_MBEANS	KIE_MBEANS	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	enabled	False
DROOLS_SERVER_FILTER_CLASSES	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスのフィルターリング。(org.drools.server.filter.classes システムプロパティーを設定)	true	False
PROMETHEUS_SERVER_EXT_DISABLED	PROMETHEUS_SERVER_EXT_DISABLED	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	false	False
KIE_SERVER_HOSTNAME_HTTP	HOSTNAME_HTTP	http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>)。	—	False
KIE_SERVER_HOSTNAME_HTTPS	HOSTNAME_HTTPS	https サービスルートのカスタムのホスト名。デフォルトホスト名の場合は空白にします (例: <application-name>-kieserver- <project>.<default-domain-suffix>)。	—	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_HTTPS_SECRET	–	キーストアファイルを含むシークレット名	kieserver-app-secret	True
KIE_SERVER_HTTPS_KEYSTORE	HTTPS_KEYSTORE	シークレット内のキーストアファイルの名前。	keystore.jks	False
KIE_SERVER_HTTPS_NAME	HTTPS_NAME	サーバー証明書に関連付けられている名前	jboss	False
KIE_SERVER_HTTPS_PASSWORD	HTTPS_PASSWORD	キーストアおよび証明書のパスワード。	mykeystorepass	False
KIE_SERVER_BYPASS_AUTH_USER	KIE_SERVER_BYPASS_AUTH_USER	KIE サーバーはタスク関連の操作は認証済みユーザーをスキップできる。 (org.kie.server.bypass.auth.user システムプロパティを設定)	false	False
KIE_SERVER_CONTAINER_DEPLOYMENT	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE サーバーコンテナのデプロイメント設定。形式: containerId=groupId:artifactId:version c2=g2:a2:v2	rhdm-kieserver-hellorules=org.openshift.quickstarts:rhdm-kieserver-hellorules:1.5.0-SNAPSHOT	True
SOURCE_REPOSITORY_URL	–	アプリケーションの Git ソース URI。	https://github.com/jboss-container-images/rhdm-7-openshift-image.git	True
SOURCE_REPOSITORY_REF	–	Git ブランチ/タグ参照。	master	False

変数名	イメージの環境変数	説明	値の例	必須
CONTEXT_DIR	–	ビルドする Git プロジェクト内のパス。ルートプロジェクトディレクトリの場合には空になります。	quickstarts/hello-rules/hellorules	False
GITHUB_WEBHOOK_SECRET	–	GitHub トリガーシークレット。	–	True
GENERIC_WEBHOOK_SECRET	–	汎用ビルドのトリガーシークレット。	–	True
MAVEN_MIRROR_URL	MAVEN_MIRROR_URL	KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	–	False
MAVEN_MIRROR_OF	MAVEN_MIRROR_OF	KIE Server の Maven ミラー設定。	external:*	False

変数名	イメージの環境変数	説明	値の例	必須
MAVEN_REPO_ID	EXTERNAL_MAVEN_REPO_ID	Maven リポジトリに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、 <code>external:*,!repo-rhdmcentr,!repo-custom</code> などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	repo-custom	False
MAVEN_REPO_URL	EXTERNAL_MAVEN_REPO_URL	Maven リポジトリへの完全修飾 URL。	—	False
MAVEN_REPO_USERNAME	EXTERNAL_MAVEN_REPO_USERNAME	Maven リポジトリにアクセスするユーザー名 (必要な場合)	—	False
MAVEN_REPO_PASSWORD	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)。	—	False
DECISION_CENTRAL_SERVICE	WORKBENCH_SERVICE_NAME	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するのに使用される任意の Decision Central のサービス名。	myapp-rhdmcentr	False

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_MAVEN_USERNAME	RHDMCENTRAL_MAVEN_REPO_USERNAME	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	mavenUser	False
DECISION_CENTRAL_MAVEN_PASSWORD	RHDMCENTRAL_MAVEN_REPO_PASSWORD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	maven!!	False
ARTIFACT_DIR	—	deploymentto フォルダーにコピーするアーカイブ取得元のディレクトリを一覧。指定されていない場合は、全アーカイブまたはターゲットがコピーされます。	—	False
KIE_SERVER_MEMORY_LIMIT	—	KIE Server のコンテナのメモリー制限。	1Gi	False
KIE_SERVER_MGMT_DISABLED	KIE_SERVER_MGMT_DISABLED	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.management.api.disabled プロパティを true に、 org.kie.server.startup.strategy プロパティを LocalContainersStartupStrategy に設定します。	true	True
SSO_URL	SSO_URL	RH-SSO URL	https://rh-sso.example.com/auth	False

変数名	イメージの環境変数	説明	値の例	必須
SSO_REALM	SSO_REALM	RH-SSO レルム名。	–	False
KIE_SERVER_SSO_CLIENT	SSO_CLIENT	KIE Server の RH-SSO クライアント名。	–	False
KIE_SERVER_SSO_SECRET	SSO_SECRET	KIE Server の RH-SSO クライアントシークレット。	252793ed-7118-4ca8-8dab-5622fa97d892	False
SSO_USERNAME	SSO_USERNAME	クライアント作成に使用する RH-SSO レルムの管理者のユーザー名 (存在しない場合)	–	False
SSO_PASSWORD	SSO_PASSWORD	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO が無効な SSL 証明書の検証。	false	False
SSO_PRINCIPAL_ATTRIBUTE	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	preferred_username	False
AUTH_LDAP_URL	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント。	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	AUTH_LDAP_BIND_DN	認証に使用するバインド DN	uid=admin,ou=users,ou=example,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP の認証情報	パスワード	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	–	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_B ASE_CTX_DN	AUTH_LDAP_B ASE_CTX_DN	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	ou=users,ou=example,ou=com	False
AUTH_LDAP_B ASE_FILTER	AUTH_LDAP_B ASE_FILTER	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	(uid={0})	False
AUTH_LDAP_S EARCH_SCOPE	AUTH_LDAP_S EARCH_SCOPE	使用する検索範囲。	SUBTREE_SCOPE	False
AUTH_LDAP_S EARCH_TIME_L IMIT	AUTH_LDAP_S EARCH_TIME_L IMIT	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	10000	False
AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE	AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されず。	distinguishedName	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_PARSE_USERNAME	AUTH_LDAP_PARSE_USERNAME	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、DN はユーザー名に対して解析されます。false に設定した場合には、DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	true	False
AUTH_LDAP_USERNAME_BEGIN_STRING	AUTH_LDAP_USERNAME_BEGIN_STRING	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	–	False
AUTH_LDAP_USERNAME_END_STRING	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	–	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_ROLE_ATTRIBUTE_ID	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前。	memberOf	False
AUTH_LDAP_ROLE_CTX_DN	AUTH_LDAP_ROLE_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	ou=groups,ou=example,ou=com	False
AUTH_LDAP_ROLE_FILTER	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。 {0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。認証済み userDN は {1} が使用されたフィルターに置き換えられます。入力ユーザー名に一致する検索フィルター例は (member={0}) です。認証済み userDN に一致する他の例は (member={1}) です。	(memberOf={1})	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_ROLE_RECURSION	AUTH_LDAP_ROLE_RECURSION	ロール検索が一致するコンテキストで行われる再帰のレベル数。再帰を無効にするには、これを 0 に設定します。	1	False
AUTH_LDAP_DEFAULT_ROLE	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール。	user	False
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。 roleAttributelsDN プロパティを true に設定すると、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定した場合には、DN は roleNameAttributeID に対してチェックされます。false に設定すると、DN は roleNameAttributeID に対して確認されません。このフラグは LDAP クエリーのパフォーマンスを向上できます。	false	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	roleAttributeID にロールオブジェクトの完全修飾 DN が含まれるかどうか。false の場合は、コンテキスト名の roleNameAttributeId 属性の値からこのロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	false	False
AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	リファーラル (referral) を使用しない場合はこのオプションを使用する必要はありません。リファーラルを使用し、ロールオブジェクトがリファーラル内部にあると、このオプションは特定のロール (例: member) に対して定義されたユーザーが含まれる属性名を示します。ユーザーはこの属性名の内容に対して確認されます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファーラルツリーに保存できません。	–	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_ROLE_MAPPER_ROLES_PROPERTIES	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping のログインモジュールで、指定したファイルを使用するように設定します。このパラメーターは、ロールを置換ロールに対してマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	–	False
AUTH_ROLE_MAPPER_REPLACE_ROLE	AUTH_ROLE_MAPPER_REPLACE_ROLE	現在のロールを追加するか、マップされたロールに現在のロールを置き換えるか。true に設定した場合は、置き換えられます。	–	False

5.1.2. オブジェクト

CLI はさまざまなオブジェクトタイプをサポートします。これらのオブジェクトタイプの一覧や略語については、[Openshift ドキュメント](#) を参照してください。

5.1.2.1. サービス

サービスは、Pod の論理セットや、Pod にアクセスするためのポリシーを定義する抽象概念です。詳細は、[コンテナエンジンのドキュメント](#) を参照してください。

サービス	ポート	名前	説明
\${APPLICATION_NAME}-kieserver	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	
\${APPLICATION_NAME}-kieserver-ping	8888	ping	クラスターリング向けの JGroups ping ポート。

5.1.2.2. ルート

ルートとは、**www.example.com** など、外部から到達可能なホスト名を指定して、サービスを公開する手段です。ルーターは、定義したルートや、サービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセクター、セキュリティ設定 (任意) で設定されます。詳細は、[Openshift ドキュメント](#) を参照してください。

サービス	セキュリティ	ホスト名
insecure- \${APPLICATION_NAME}- kieserver-http	なし	\${KIE_SERVER_HOSTNAME}_HTTP
\${APPLICATION_NAME}- kieserver-https	TLS パススルー	\${KIE_SERVER_HOSTNAME}_HTTPS

5.1.2.3. ビルド設定

buildConfig は、単一のビルド定義と、新規ビルドを作成する必要があるタイミングについての一連のトリガーを記述します。**buildConfig** は REST オブジェクトで、API サーバーへの POST で使用して新規インスタンスを作成できます。詳細は、[Openshift ドキュメント](#) を参照してください。

S2I イメージ	リンク	ビルドの出力	BuildTriggers および設定
rhdm74-kieserver-openshift:1.0	rhdm-7/rhdm74-kieserver-openshift	\${APPLICATION_NAME}-kieserver:latest	GitHub、Generic、ImageChange、ConfigChange

5.1.2.4. デプロイメント設定

OpenShift のデプロイメントは、デプロイメント設定と呼ばれるユーザー定義のテンプレートをもとにするレプリケーションコントローラーです。デプロイメントは手動で作成されるか、トリガーされたイベントに対応するために作成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

5.1.2.4.1. トリガー

トリガーは、OpenShift 内外を問わず、イベントが発生すると新規デプロイメントを作成するように促します。詳細は、[Openshift ドキュメント](#) を参照してください。

Deployment	トリガー
\${APPLICATION_NAME}-kieserver	ImageChange

5.1.2.4.2. レプリカ

レプリケーションコントローラーを使用すると、指定した数だけ、Pod のレプリカを一度に実行させることができます。レプリカが増えると、レプリケーションコントローラーが Pod の一部を終了させます。レプリカが足りない場合には、起動させます。詳細は、[コンテナエンジンのドキュメント](#) を参照

してください。

Deployment	レプリカ
<code>\${APPLICATION_NAME}-kieserver</code>	2

5.1.2.4.3. Pod テンプレート

5.1.2.4.3.1. サービスアカウント

サービスアカウントは、各プロジェクト内に存在する API オブジェクトです。他の API オブジェクトのように作成し、削除できます。詳細は、[Openshift ドキュメント](#) を参照してください。

Deployment	サービスアカウント
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>

5.1.2.4.3.2. イメージ

デプロイメント	イメージ
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>

5.1.2.4.3.3. Readiness Probe

`${APPLICATION_NAME}-kieserver`

Http Get on `http://localhost:8080/services/rest/server/readycheck`

5.1.2.4.3.4. Liveness Probe

`${APPLICATION_NAME}-kieserver`

Http Get on `http://localhost:8080/services/rest/server/healthcheck`

5.1.2.4.3.5. 公開されたポート

デプロイメント	名前	ポート	プロトコル
<code>\${APPLICATION_NAME}-kieserver</code>	jolokia	8778	TCP
	http	8080	TCP
	https	8443	TCP

デプロイメント	名前	ポート	プロトコル
	ping	8888	TCP

5.1.2.4.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
\${APPLICATION_NAME}-kieserver	WORKBENCH_SERVICE_NAME	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するのに使用される任意の Decision Central のサービス名。	\${DECISION_CENTRAL_SERVICE}
	KIE_ADMIN_USER	KIE 管理者のユーザー名	\${KIE_ADMIN_USER}
	KIE_ADMIN_PWD	KIE 管理者のパスワード	\${KIE_ADMIN_PWD}
	KIE_SERVER_MODE	–	DEVELOPMENT
	KIE_MBEANS	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	\${KIE_MBEANS}
	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスのフィルターリング。 (org.drools.server.filter.classes システムプロパティーを設定)	\${DROOLS_SERVER_FILTER_CLASSES}
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定すると、prometheus サーバー拡張が有効になります。 (org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	\${PROMETHEUS_SERVER_EXT_DISABLED}
	KIE_SERVER_BYPASS_AUTH_USER	KIE サーバーはタスク関連の操作は認証済みユーザーをスキップできる。 (org.kie.server.bypass.auth.user システムプロパティーを設定)	\${KIE_SERVER_BYPASS_AUTH_USER}
	KIE_SERVER_ID	–	–

デプロイメント	変数名	説明	値の例
	KIE_SERVER_ROUTE_NAME	–	\${APPLICATION_NAME}-kieserver
	KIE_SERVER_USER	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティを設定する)	\${KIE_SERVER_USER}
	KIE_SERVER_PWD	KIE サーバーへの接続に使用する KIE サーバーパスワード。値はデフォルトで自動的に生成されます。(org.kie.server.pwd システムプロパティを設定する)	\${KIE_SERVER_PWD}
	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE サーバーコンテナのデプロイメント設定。 形式: containerId=groupId:artifactId:version c2=g2:a2:v2	\${KIE_SERVER_CONTAINER_DEPLOYMENT}
	MAVEN_MIRROR_URL	KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	\${MAVEN_MIRROR_URL}
	MAVEN_MIRROR_OFF	KIE Server の Maven ミラー設定。	\${MAVEN_MIRROR_OFF}
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_ID	–	repo-rhdmcentr
	RHDMCENTR_MAVEN_REPO_SERVICE	必要かつ到達可能な場合にサービスルックアップ(maven リポジトリの使用など)を許可するのに使用される任意の Decision Central のサービス名。	\${DECISION_CENTRAL_SERVICE}

デプロイメント	変数名	説明	値の例
	RHDMCENTR_MAVEN_REPO_PATH	–	/maven2/
	RHDMCENTR_MAVEN_REPO_USERNAME	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	\${DECISION_CENTRAL_MAVEN_USERNAME}
	RHDMCENTR_MAVEN_REPO_PASSWORD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	\${DECISION_CENTRAL_MAVEN_PASSWORD}
	EXTERNAL_MAVEN_REPO_ID	Maven リポジトリに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	\${MAVEN_REPO_ID}
	EXTERNAL_MAVEN_REPO_URL	Maven リポジトリへの完全修飾 URL。	\${MAVEN_REPO_URL}
	EXTERNAL_MAVEN_REPO_USERNAME	Maven リポジトリにアクセスするユーザー名 (必要な場合)	\${MAVEN_REPO_USERNAME}
	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)。	\${MAVEN_REPO_PASSWORD}
	HTTPS_KEYSTORE_DIR	–	/etc/kieserver-secret-volume

デプロイメント	変数名	説明	値の例
	HTTPS_KEYSTORE	シークレット内のキーストアファイルの名前。	`\${KIE_SERVER_HTTPS_KEYSTORE}`
	HTTPS_NAME	サーバー証明書に関連付けられている名前	`\${KIE_SERVER_HTTPS_NAME}`
	HTTPS_PASSWORD	キーストアおよび証明書のパスワード。	`\${KIE_SERVER_HTTPS_PASSWORD}`
	KIE_SERVER_MGMT_DISABLED	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.management.api.disabled プロパティを true に、 org.kie.server.startup.strategy プロパティを LocalContainersStartupStrategy に設定します。	`\${KIE_SERVER_MGMT_DISABLED}`
	KIE_SERVER_STARTUP_STRATEGY	–	OpenShiftStartupStrategy
	JGROUPS_PING_PROTOCOL	–	openshift.DNS_PING
	OPENSIFT_DNS_PING_SERVICE_NAME	–	`\${APPLICATION_NAME}-kieserver-ping`
	OPENSIFT_DNS_PING_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL	`\${SSO_URL}`
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO レalm名。	`\${SSO_REALM}`
	SSO_SECRET	KIE Server の RH-SSO クライアントシークレット。	`\${KIE_SERVER_SSO_SECRET}`

デプロイメント	変数名	説明	値の例
	SSO_CLIENT	KIE Server の RH-SSO クライアント名。	`\${KIE_SERVER_SSO_CLIENT}`
	SSO_USERNAME	クライアント作成に使用する RH-SSO レルムの管理者のユーザー名 (存在しない場合)	`\${SSO_USERNAME}`
	SSO_PASSWORD	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	`\${SSO_PASSWORD}`
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO が無効な SSL 証明書の検証。	`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`
	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	`\${SSO_PRINCIPAL_ATTRIBUTE}`
	HOSTNAME_HTTP	http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>)。	`\${KIE_SERVER_HOSTNAME_HTTP}`
	HOSTNAME_HTTPS	https サービスルートのカスタムのホスト名。デフォルトホスト名の場合は空白にします (例: <application-name>- kieserver-<project>. <default-domain-suffix>)。	`\${KIE_SERVER_HOSTNAME_HTTPS}`
	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント。	`\${AUTH_LDAP_URL}`
	AUTH_LDAP_BIND_DN	認証に使用するバインド DN	`\${AUTH_LDAP_BIND_DN}`
	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP の認証情報	`\${AUTH_LDAP_BIND_CREDENTIAL}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索を開始する 最上位コンテキストの LDAP ベース DN	`\${AUTH_LDAP_BASE_CTX_DN}`
	AUTH_LDAP_BASE_FILTER	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	`\${AUTH_LDAP_BASE_FILTER}`
	AUTH_LDAP_SEARCH_SCOPE	使用する検索範囲。	`\${AUTH_LDAP_SEARCH_SCOPE}`
	AUTH_LDAP_SEARCH_TIME_LIMIT	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`
	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されません。	`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_PARSE_USERNAME	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、DN はユーザー名に対して解析されます。false に設定した場合には、DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	`\${AUTH_LDAP_PARSE_USERNAME}`
	AUTH_LDAP_USERNAME_BEGIN_STRING	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USERNAME_BEGIN_STRING}`
	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USERNAME_END_STRING}`
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前。	`\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_ROLE_S_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	`\${AUTH_LDAP_ROLE_S_CTX_DN}`
	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。認証済み userDN は {1} が使用されたフィルターに置き換えられます。入力ユーザー名に一致する検索フィルター例は (member={0}) です。認証済み userDN に一致する他の例は (member={1}) です。	`\${AUTH_LDAP_ROLE_FILTER}`
	AUTH_LDAP_ROLE_RECURSION	ロール検索が一致するコンテキストで行われる再帰のレベル数。再帰を無効にするには、これを 0 に設定します。	`\${AUTH_LDAP_ROLE_RECURSION}`
	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール。	`\${AUTH_LDAP_DEFAULT_ROLE}`
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。roleAttributesDN プロパティを true に設定すると、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定した場合には、DN は roleNameAttributeID に対してチェックされます。false に設定すると、DN は roleNameAttributeID に対して確認されません。このフラグは LDAP クエリーのパフォーマンスを向上できます。	`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`
	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	roleAttributeID にロールオブジェクトの完全修飾 DN が含まれるかどうか。false の場合は、コンテキスト名の roleNameAttributeID 属性の値からこのロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`
	AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK	リファール (referral) を使用しない場合はこのオプションを使用する必要はありません。リファールを使用し、ロールオブジェクトがリファール内部にあると、このオプションは特定のロール (例: member) に対して定義されたユーザーが含まれる属性名を示します。ユーザーはこの属性名の内容に対して確認されます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`

デプロイメント	変数名	説明	値の例
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMappingのログインモジュールで、指定したファイルを使用するように設定します。このパラメーターは、ロールを置換ロールに対してマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}
	AUTH_ROLE_MAPPER_REPLACE_ROLE	現在のロールを追加するか、マップされたロールに現在のロールを置き換えるか。true に設定した場合は、置き換えられます。	\${AUTH_ROLE_MAPPER_REPLACE_ROLE}

5.1.2.4.3.7. ボリューム

デプロイメント	名前	mountPath	目的	readOnly
\${APPLICATION_NAME}-kieserver	kieserver-keystore-volume	/etc/kieserver-secret-volume	ssl certs	True

5.1.2.5. 外部の依存関係

5.1.2.5.1. シークレット

このテンプレートでは、アプリケーションを実行するために以下のシークレットをインストールする必要があります。

kieserver-app-secret

5.2. RHDM74-PROD-IMMUTABLE-KIESERVER-AMQ.YAML テンプレート

Red Hat Decision Manager 7.4 の ActiveMQ と統合された実稼働環境におけるイミュータブル KIE サーバー向けのアプリケーションテンプレート

5.2.1. パラメーター

テンプレートを使用すると値を引き継ぐパラメーターを定義でき、パラメーターの参照時には、この値が代入されます。この値は、パラメーターの参照時には、この値が代入されます。参照はオブジェクト一覧フィールドの任意のテキストフィールドで定義できます。詳細は、[Openshift ドキュメント](#) を参照してください。

変数名	イメージの環境変数	説明	値の例	必須
APPLICATION_NAME	–	アプリケーションの名前。	myapp	True
KIE_ADMIN_USER	KIE_ADMIN_USER	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PASSWORD	KIE_ADMIN_PASSWORD	KIE 管理者のパスワード	–	False
KIE_SERVER_USER	KIE_SERVER_USER	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティを設定します)	executionUser	False
KIE_SERVER_PASSWORD	KIE_SERVER_PASSWORD	KIE サーバーへの接続に使用する KIE サーバーパスワード。値はデフォルトで自動的に生成されます。 (org.kie.server.pwd システムプロパティを設定する)	–	False
IMAGE_STREAM_NAMESPACE	–	Red Hat ミドルウェアイメージの ImageStreams がインストールされている namespace これらの ImageStreams は通常 OpenShift の名前空間にインストールされています。ImageStreams を別の namespace/プロジェクトにインストールしている場合には、これを変更するだけで結構です。	openshift	True

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_IMAGE_STREAM_NAME	–	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm74-kieserver-openshift です。	rhdm74-kieserver-openshift	True
IMAGE_STREAM_TAG	–	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 1.0 です。	1.0	True
KIE_MBEANS	KIE_MBEANS	KIE Server の mbeans が有効/無効になっています。(システムプロパティ kie.mbeans および kie.scanner.mbeans を設定)	enabled	False
DROOLS_SERVER_FILTER_CLASSES	DROOLS_SERVER_FILTER_CLASSES	KIE Server のクラスフィルター (org.drools.server.filter.classes システムプロパティを設定)	true	False
PROMETHEUS_SERVER_EXT_DISABLED	PROMETHEUS_SERVER_EXT_DISABLED	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティを設定)	false	False
KIE_SERVER_HOSTNAME_HTTP	HOSTNAME_HTTP	http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>)。	–	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_HOSTNAME_HTTPS	HOSTNAME_HTTPS	https サービスルートのカスタムのホスト名。デフォルトホスト名の場合は空白にします (例: <application-name>-kieserver-<project>.<default-domain-suffix>。	–	False
KIE_SERVER_HTTPS_SECRET	–	キーストアファイルを含むシークレット名	kieserver-app-secret	True
KIE_SERVER_HTTPS_KEYSTORE	HTTPS_KEYSTORE	シークレット内のキーストアファイルの名前。	keystore.jks	False
KIE_SERVER_HTTPS_NAME	HTTPS_NAME	サーバー証明書に関連付けられている名前	jboss	False
KIE_SERVER_HTTPS_PASSWORD	HTTPS_PASSWORD	キーストアおよび証明書のパスワード	mykeystorepass	False
KIE_SERVER_BYPASS_AUTH_USER	KIE_SERVER_BYPASS_AUTH_USER	KIE サーバーのバイパス認証ユーザー (org.kie.server.bypass.auth.user システムプロパティを設定します)	false	False
KIE_SERVER_CONTAINER_DEPLOYMENT	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE サーバーコンテナのデプロイメント設定。形式: containerId=groupId:artifactId:version c2=g2:a2:v2	rhdm-kieserver-hellorules=org.openshift.quickstarts:rhdm-kieserver-hellorules:1.5.0-SNAPSHOT	True
SOURCE_REPOSITORY_URL	–	アプリケーションの Git ソース URI。	https://github.com/jboss-container-images/rhdm-7-openshift-image.git	True

変数名	イメージの環境変数	説明	値の例	必須
SOURCE_REPO_SITORY_REF	–	Git ブランチ/タグ参照。	master	False
CONTEXT_DIR	–	ビルドする Git プロジェクト内のパス。ルートプロジェクトディレクトリの場合は空になります。	quickstarts/hello-rules/hellorules	False
GITHUB_WEBHOOK_SECRET	–	GitHub トリガーシークレット。	–	True
GENERIC_WEBHOOK_SECRET	–	汎用ビルドのトリガーシークレット。	–	True
MAVEN_MIRROR_URL	–	S2I ビルドに使用する Maven ミラー	–	False
MAVEN_REPO_ID	EXTERNAL_MAVEN_REPO_ID	maven リポジトリに使用する id (設定されている場合)。デフォルトは無作為に作成されます。	my-repo-id	False
MAVEN_REPO_URL	EXTERNAL_MAVEN_REPO_URL	Maven リポジトリへの完全修飾 URL。	–	False
MAVEN_REPO_USERNAME	EXTERNAL_MAVEN_REPO_USERNAME	Maven リポジトリにアクセスするユーザー名 (必要な場合)	–	False
MAVEN_REPO_PASSWORD	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)。	–	False

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_SERVICE	WORKBENCH_SERVICE_NAME	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するのに使用される任意の Decision Central のサービス名。	myapp-rhdmcentr	False
DECISION_CENTRAL_MAVEN_USERNAME	RHDMCENTRAL_MAVEN_REPO_USERNAME	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	mavenUser	False
DECISION_CENTRAL_MAVEN_PASSWORD	RHDMCENTRAL_MAVEN_REPO_PASSWORD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	maven1!	False
ARTIFACT_DIR	–	deploymentto フォルダーにコピーするアーカイブ取得元のディレクトリ一覧。指定されていない場合は、全アーカイブまたはターゲットがコピーされます。	–	False
KIE_SERVER_MEMORY_LIMIT	–	KIE Server のコンテナのメモリー制限	1Gi	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_MGMT_DISABLE D	KIE_SERVER_MGMT_DISABLE D	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.mgmt.api.disabled プロパティを true に、 org.kie.server.startup.strategy プロパティを LocalContainersStartupStrategy に設定します。	true	True
KIE_SERVER_JMS_QUEUE_REQUEST	KIE_SERVER_JMS_QUEUE_REQUEST	JMS の要求キューの JNDI 名。デフォルト値は queue/KIE.SERVICE.REQUEST です。	queue/KIE.SERVICE.REQUEST	False
KIE_SERVER_JMS_QUEUE_RESPONSE	KIE_SERVER_JMS_QUEUE_RESPONSE	JMS の応答キューの JNDI 名。デフォルト値は queue/KIE.SERVICE.RESPONSE です。	queue/KIE.SERVICE.RESPONSE	False
AMQ_USERNAME	AMQ_USERNAME	標準ブローカーユーザーのユーザー名。ブローカーに接続するために必要です。空白の場合は生成されます。	–	False
AMQ_PASSWORD	AMQ_PASSWORD	標準ブローカーユーザーのパスワード。ブローカーに接続するために必要です。空白の場合は生成されます。	–	False

変数名	イメージの環境変数	説明	値の例	必須
AMQ_ROLE	AMQ_ROLE	標準ブローカーユーザーのユーザーロール。	admin	True
AMQ_QUEUES	AMQ_QUEUES	コンマで区切られたキュー名。これらのキューは、ブローカーの起動時に自動的に作成されます。さらに、これらは EAP で JNDI リソースとしてアクセス可能になります。これらのキューは KIE Server が必要とするデフォルトキューです。カスタムキューを使用する場合は、 <code>KIE_SERVER_JMS_QUEUE_RESPONSE</code> および <code>KIE_SERVER_JMS_QUEUE_REQUEST</code> と同じ値を使用します。	queue/KIE.SERVE R.REQUEST,queue/KIE.SERVER.RE SPONSE	False
AMQ_GLOBAL_MAX_SIZE	AMQ_GLOBAL_MAX_SIZE	メッセージデータが使用可能な最大メモリー量を指定します。値が指定されていない場合は、システムのメモリーの半分が割り当てられます。	10 gb	False
AMQ_PROTOCOL	AMQ_PROTOCOL	コンマで区切られた、設定するブローカーのプロトコル。許可される値は、 openwire 、 amqp 、 stomp 、および mqtt です。 openwire のみが EAP でサポートされます。	openwire	False

変数名	イメージの環境変数	説明	値の例	必須
AMQ_BROKER_IMAGESTREAM_NAME	–	AMQ ブローカーイメージストリーム名。	amq-broker-73-openshift:7.3	True
SSO_URL	SSO_URL	RH-SSO URL	https://rh-sso.example.com/auth	False
SSO_REALM	SSO_REALM	RH-SSO レalm 名。	–	False
KIE_SERVER_SSO_CLIENT	SSO_CLIENT	KIE Server の RH-SSO クライアント名。	–	False
KIE_SERVER_SSO_SECRET	SSO_SECRET	KIE Server の RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False
SSO_USERNAME	SSO_USERNAME	クライアント作成に使用する RH-SSO レalm の管理者のユーザー名 (存在しない場合)	–	False
SSO_PASSWORD	SSO_PASSWORD	クライアント作成に使用する RH-SSO レalm の管理者のパスワード。	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO が無効な SSL 証明書の検証。	false	False
SSO_PRINCIPAL_ATTRIBUTE	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	preferred_username	False
AUTH_LDAP_URL	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	AUTH_LDAP_BIND_DN	認証に使用するバインド DN。	uid=admin,ou=users,ou=example,ou=com	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_BIND_CREDENTIAL	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP の認証情報。	パスワード	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	–	False
AUTH_LDAP_BASE_CTX_DN	AUTH_LDAP_BASE_CTX_DN	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	ou=users,ou=example,ou=com	False
AUTH_LDAP_BASE_FILTER	AUTH_LDAP_BASE_FILTER	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	(uid={0})	False
AUTH_LDAP_SEARCH_SCOPE	AUTH_LDAP_SEARCH_SCOPE	使用する検索範囲。	SUBTREE_SCOPE	False
AUTH_LDAP_SEARCH_TIME_LIMIT	AUTH_LDAP_SEARCH_TIME_LIMIT	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	10000	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されます。	distinguishedName	False
AUTH_LDAP_PARSE_USERNAME	AUTH_LDAP_PARSE_USERNAME	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、DN はユーザー名に対して解析されます。false に設定した場合には、DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	true	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_USERNAME_BEGIN_STRING	AUTH_LDAP_USERNAME_BEGIN_STRING	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは <code>usernameEndString</code> と合わせて使用し、 <code>parseUsername</code> が <code>true</code> に設定されている場合にのみ考慮されます。	–	False
AUTH_LDAP_USERNAME_END_STRING	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは <code>usernameEndString</code> と合わせて使用し、 <code>parseUsername</code> が <code>true</code> に設定されている場合にのみ考慮されます。	–	False
AUTH_LDAP_ROLE_ATTRIBUTE_ID	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前。	<code>memberOf</code>	False
AUTH_LDAP_ROLE_CONTEXT_DN	AUTH_LDAP_ROLE_CONTEXT_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	<code>ou=groups,ou=example,ou=com</code>	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_ROLE_FILTER	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。 {0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。認証済み userDN は {} が使用されたフィルターに置き換えられます。入力ユーザー名に一致する検索フィルター例は (member={0}) です。認証済み userDN に一致する他の例は (member={1}) です。	(memberOf={1})	False
AUTH_LDAP_ROLE_RECURSION	AUTH_LDAP_ROLE_RECURSION	ロール検索が一致するコンテキストで行われる再帰のレベル数。再帰を無効にするには、これを 0 に設定します。	1	False
AUTH_LDAP_DEFAULT_ROLE	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	user	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。 roleAttributeIsDN プロパティを true に設定すると、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定した場合には、DN は roleNameAttributeID に対してチェックされます。false に設定すると、DN は roleNameAttributeID に対して確認されません。このフラグは LDAP クエリーのパフォーマンスを向上できます。	false	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	roleAttributeID に ロールオブジェクトの完全修飾 DN が含まれるかどうか。false の場合 は、コンテキスト名の roleNameAttribute Id 属性の値からこの ロール名が取得 されます。 Microsoft Active Directory などの特 定のディレクト リースキーマで は、この属性を true に設定する必 要があります。	false	False
AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	リファーラル (referral) を使用し ない場合はこのオ プションを使用す る必要はありませ ん。リファーラル を使用し、ロール オブジェクトがリ ファーラル内部に あると、このオプ ションは特定の ロール (例: member) に対して 定義されたユー ザーが含まれる属 性名を示します。 ユーザーはこの属 性名の内容に対し て確認されます。 このオプションが 設定されていない とチェックは常に 失敗するため、 ロールオブジェク トはリファーラル ツリーに保存でき ません。	-	False

変数名	イメージの環境変数	説明	値の例	必須
AUTH_ROLE_MAPPER_ROLES_PROPERTIES	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping のログインモジュールで、指定したファイルを使用するように設定します。このプロパティーは、ロールを置換ロールに対してマップするプロパティーファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	–	False
AUTH_ROLE_MAPPER_REPLACE_ROLE	AUTH_ROLE_MAPPER_REPLACE_ROLE	現在のロールを追加するか、マップされたロールに現在のロールを置き換えるか。true に設定した場合は、置き換えられます。	–	False

5.2.2. オブジェクト

CLI はさまざまなオブジェクトタイプをサポートします。これらのオブジェクトタイプの一覧や略語については、[Openshift ドキュメント](#) を参照してください。

5.2.2.1. サービス

サービスは、Pod の論理セットや、Pod にアクセスするためのポリシーを定義する抽象概念です。詳細は、[コンテナエンジンのドキュメント](#) を参照してください。

サービス	ポート	名前	説明
\${APPLICATION_NAME}-kieserver	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	
\${APPLICATION_NAME}-kieserver-ping	8888	ping	クラスターリング向けの JGroups ping ポート。

サービス	ポート	名前	説明
\${APPLICATION_NAME}-amq-jolokia	8161	amq-jolokia-console	ブローカーのコンソールおよび Jolokia ポート。
\${APPLICATION_NAME}-amq-amqp	5672	amp-amqp	ブローカーの AMQP ポート。
\${APPLICATION_NAME}-amq-mqtt	1883	amq-mqtt	ブローカーの MQTT ポート。
\${APPLICATION_NAME}-amq-stomp	61613	amp-stomp	ブローカーの STOMP ポート。
\${APPLICATION_NAME}-amq-tcp	61616	amq-tcp	ブローカーの OpenWire ポート。

5.2.2.2. ルート

ルートとは、**www.example.com** など、外部から到達可能なホスト名を指定して、サービスを公開する手段です。ルーターは、定義したルートや、サービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセレクター、セキュリティ設定 (任意) で設定されます。詳細は、[Openshift ドキュメント](#) を参照してください。

サービス	セキュリティ	ホスト名
insecure- \${APPLICATION_NAME}-kieserver-http	なし	\${KIE_SERVER_HOSTNAME_HTTP}
\${APPLICATION_NAME}-kieserver-https	TLS パススルー	\${KIE_SERVER_HOSTNAME_HTTPS}
\${APPLICATION_NAME}-amq-jolokia-console	none	<default>

5.2.2.3. ビルド設定

buildConfig は、単一のビルド定義と、新規ビルドを作成する必要があるタイミングについての一連のトリガーを記述します。**buildConfig** は REST オブジェクトで、API サーバーへの POST で使用して新規インスタンスを作成できます。詳細は、[Openshift ドキュメント](#) を参照してください。

S2I イメージ	リンク	ビルドの出力	BuildTriggers および設定
----------	-----	--------	---------------------

S2I イメージ	リンク	ビルドの出力	BuildTriggers および設定
rhdm74-kieserver-openshift:1.0	rhdm-7/rhdm74-kieserver-openshift	<code>\${APPLICATION_NAME}-kieserver:latest</code>	GitHub、Generic、ImageChange、ConfigChange

5.2.2.4. デプロイメント設定

OpenShift のデプロイメントは、デプロイメント設定と呼ばれるユーザー定義のテンプレートをもとにするレプリケーションコントローラーです。デプロイメントは手動で作成されるか、トリガーされたイベントに対応するために作成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

5.2.2.4.1. トリガー

トリガーは、OpenShift 内外を問わず、イベントが発生すると新規デプロイメントを作成するように促します。詳細は、[Openshift ドキュメント](#) を参照してください。

Deployment	トリガー
<code>\${APPLICATION_NAME}-kieserver</code>	ImageChange
<code>\${APPLICATION_NAME}-amq</code>	ImageChange

5.2.2.4.2. レプリカ

レプリケーションコントローラーを使用すると、指定した数だけ、Pod のレプリカを一度に実行させることができます。レプリカが増えると、レプリケーションコントローラーが Pod の一部を終了させます。レプリカが足りない場合には、起動させます。詳細は、[コンテナエンジンのドキュメント](#) を参照してください。

Deployment	レプリカ
<code>\${APPLICATION_NAME}-kieserver</code>	2
<code>\${APPLICATION_NAME}-amq</code>	1

5.2.2.4.3. Pod テンプレート

5.2.2.4.3.1. サービスアカウント

サービスアカウントは、各プロジェクト内に存在する API オブジェクトです。他の API オブジェクトのように作成し、削除できます。詳細は、[Openshift ドキュメント](#) を参照してください。

Deployment	サービスアカウント
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>

5.2.2.4.3.2. イメージ

デプロイメント	イメージ
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>
<code>\${APPLICATION_NAME}-amq</code>	<code>\${AMQ_BROKER_IMAGESTREAM_NAME}</code>

5.2.2.4.3.3. Readiness Probe

`${APPLICATION_NAME}-kieserver`

Http Get on `http://localhost:8080/services/rest/server/readycheck`

`${APPLICATION_NAME}-amq`

`/bin/bash -c /opt/amq/bin/readinessProbe.sh`

5.2.2.4.3.4. Liveness Probe

`${APPLICATION_NAME}-kieserver`

Http Get on `http://localhost:8080/services/rest/server/healthcheck`

5.2.2.4.3.5. 公開されたポート

デプロイメント	名前	ポート	プロトコル
<code>\${APPLICATION_NAME}-kieserver</code>	<code>jolokia</code>	8778	TCP
	<code>http</code>	8080	TCP
	<code>https</code>	8443	TCP
	<code>ping</code>	8888	TCP
<code>\${APPLICATION_NAME}-amq</code>	<code>console-jolokia</code>	8161	TCP
	<code>amq-amqp</code>	5672	TCP
	<code>amq-mqtt</code>	1883	TCP
	<code>amq-stomp</code>	61613	TCP
	<code>amq-tcp</code>	61616	TCP

5.2.2.4.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
\${APPLICATION_NAME}-kieserver	WORKBENCH_SERVICE_NAME	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するために使用される任意の Decision Central のサービス名。	\${DECISION_CENTRAL_SERVICE}
	KIE_ADMIN_USER	KIE 管理者のユーザー名	\${KIE_ADMIN_USER}
	KIE_ADMIN_PWD	KIE 管理者のパスワード	\${KIE_ADMIN_PWD}
	KIE_SERVER_MODE	–	DEVELOPMENT
	KIE_MBEANS	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	\${KIE_MBEANS}
	DROOLS_SERVER_FILTER_CLASSES	KIE Server のクラスフィルタ (org.drools.server.filter.classes システムプロパティーを設定)	\${DROOLS_SERVER_FILTER_CLASSES}
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	\${PROMETHEUS_SERVER_EXT_DISABLED}
	KIE_SERVER_BYPASS_AUTH_USER	KIE サーバーのバイパス認証ユーザー (org.kie.server.bypass.auth.user システムプロパティーを設定します)	\${KIE_SERVER_BYPASS_AUTH_USER}
	KIE_SERVER_ID	–	–
	KIE_SERVER_ROUTE_NAME	–	\${APPLICATION_NAME}-kieserver

デプロイメント	変数名	説明	値の例
	KIE_SERVER_USER	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティを設定します)	`\${KIE_SERVER_USER}`
	KIE_SERVER_PWD	KIE サーバーへの接続に使用する KIE サーバーパスワード。値はデフォルトで自動的に生成されます。(org.kie.server.pwd システムプロパティを設定する)	`\${KIE_SERVER_PWD}`
	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE サーバーコンテナのデプロイメント設定。形式: containerId=groupId:artifactId:version c2=g2:a2:v2	`\${KIE_SERVER_CONTAINER_DEPLOYMENT}`
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_SERVICE	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するのに使用される任意の Decision Central のサービス名。	`\${DECISION_CENTRAL_SERVICE}`
	RHDMCENTR_MAVEN_REPO_PATH	–	/maven2/
	RHDMCENTR_MAVEN_REPO_USERNAME	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	`\${DECISION_CENTRAL_MAVEN_USERNAME}`
	RHDMCENTR_MAVEN_REPO_PASSWORD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	`\${DECISION_CENTRAL_MAVEN_PASSWORD}`

デプロイメント	変数名	説明	値の例
	EXTERNAL_MAVEN_REPO_ID	maven リポジトリに使用する id (設定されている場合)。デフォルトは無作為に作成されます。	\${MAVEN_REPO_ID}
	EXTERNAL_MAVEN_REPO_URL	Maven リポジトリへの完全修飾 URL。	\${MAVEN_REPO_URL}
	EXTERNAL_MAVEN_REPO_USERNAME	Maven リポジトリにアクセスするユーザー名 (必要な場合)	\${MAVEN_REPO_USERNAME}
	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)。	\${MAVEN_REPO_PASSWORD}
	KIE_SERVER_JMS_QUEUE_REQUEST	JMS の要求キューの JNDI 名。デフォルト値は queue/KIE.SERVER.REQUEST です。	\${KIE_SERVER_JMS_QUEUE_REQUEST}
	KIE_SERVER_JMS_QUEUE_RESPONSE	JMS の応答キューの JNDI 名。デフォルト値は queue/KIE.SERVER.RESPONSE です。	\${KIE_SERVER_JMS_QUEUE_RESPONSE}
	MQ_SERVICE_PREFIX_MAPPING	–	\${APPLICATION_NAME}-amq7=AMQ
	AMQ_USERNAME	標準ブローカーユーザーのユーザー名。ブローカーに接続するために必要です。空白の場合は生成されます。	\${AMQ_USERNAME}
	AMQ_PASSWORD	標準ブローカーユーザーのパスワード。ブローカーに接続するために必要です。空白の場合は生成されます。	\${AMQ_PASSWORD}

デプロイメント	変数名	説明	値の例
	AMQ_PROTOCOL	コンマで区切られた、設定するブローカーのプロトコル。許可される値は、 openwire 、 amqp 、 stomp 、および mqtt です。 openwire のみが EAP でサポートされます。	tcp
	AMQ_QUEUES	コンマで区切られたキュー名。これらのキューは、ブローカーの起動時に自動的に作成されます。さらに、これらは EAP で JNDI リソースとしてアクセス可能になります。これらのキューは KIE Server が必要とするデフォルトキューです。カスタムキューを使用する場合は、 KIE_SERVER_JMS_QUEUE_RESPONSE および KIE_SERVER_JMS_QUEUE_REQUEST と同じ値を使用します。	\${AMQ_QUEUES}
	HTTPS_KEYSTORE_DIR	–	/etc/kieserver-secret-volume
	HTTPS_KEYSTORE	シークレット内のキーストアファイルの名前。	\${KIE_SERVER_HTTPS_KEYSTORE}
	HTTPS_NAME	サーバー証明書に関連付けられている名前	\${KIE_SERVER_HTTPS_NAME}
	HTTPS_PASSWORD	キーストアおよび証明書のパスワード	\${KIE_SERVER_HTTPS_PASSWORD}

デプロイメント	変数名	説明	値の例
	KIE_SERVER_MGMT_DISABLED	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.mgmt.api.disabled プロパティを true に、 org.kie.server.startup.strategy プロパティを LocalContainersStartupStrategy に設定します。	`\${KIE_SERVER_MGMT_DISABLED}`
	KIE_SERVER_STARTUP_STRATEGY	–	OpenShiftStartupStrategy
	JGROUPS_PING_PROTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PING_SERVICE_NAME	–	`\${APPLICATION_NAME}-kieserver-ping`
	OPENSHIFT_DNS_PING_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL	`\${SSO_URL}`
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO レalm名。	`\${SSO_REALM}`
	SSO_SECRET	KIE Server の RH-SSO クライアントシークレット	`\${KIE_SERVER_SSO_SECRET}`
	SSO_CLIENT	KIE Server の RH-SSO クライアント名。	`\${KIE_SERVER_SSO_CLIENT}`
	SSO_USERNAME	クライアント作成に使用する RH-SSO レalmの管理者のユーザー名 (存在しない場合)	`\${SSO_USERNAME}`

デプロイメント	変数名	説明	値の例
	SSO_PASSWORD	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	\${SSO_PASSWORD}
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO が無効な SSL 証明書の検証。	\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}
	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	\${SSO_PRINCIPAL_ATTRIBUTE}
	HOSTNAME_HTTP	http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>)。	\${KIE_SERVER_HOSTNAME_HTTP}
	HOSTNAME_HTTPS	https サービスルートのカスタムのホスト名。デフォルトホスト名の場合は空白にします (例: <application-name>-kieserver-<project>.<default-domain-suffix>)。	\${KIE_SERVER_HOSTNAME_HTTPS}
	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント	\${AUTH_LDAP_URL}
	AUTH_LDAP_BIND_DN	認証に使用するバインド DN。	\${AUTH_LDAP_BIND_DN}
	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP の認証情報。	\${AUTH_LDAP_BIND_CREDENTIAL}
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	\${AUTH_LDAP_BASE_CTX_DN}

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_BASE_FILTER	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	`\${AUTH_LDAP_BASE_FILTER}`
	AUTH_LDAP_SEARCH_SCOPE	使用する検索範囲。	`\${AUTH_LDAP_SEARCH_SCOPE}`
	AUTH_LDAP_SEARCH_TIME_LIMIT	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`
	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されます。	`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`
	AUTH_LDAP_PARSE_USERNAME	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、DN はユーザー名に対して解析されます。false に設定した場合には、DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	`\${AUTH_LDAP_PARSE_USERNAME}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_USER NAME_BEGIN_STR ING	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USE RNAME_BEGIN_STR ING}`
	AUTH_LDAP_USER NAME_END_STRIN G	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USE RNAME_END_STRIN G}`
	AUTH_LDAP_ROLE_ ATTRIBUTE_ID	ユーザーロールを含む属性の名前。	`\${AUTH_LDAP_ROL E_ATTRIBUTE_ID}`
	AUTH_LDAP_ROLE S_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	`\${AUTH_LDAP_ROL ES_CTX_DN}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。認証済み userDN は {1} が使用されたフィルターに置き換えられます。入力ユーザー名に一致する検索フィルター例は (member={0}) です。認証済み userDN に一致する他の例は (member={1}) です。	`\${AUTH_LDAP_ROLE_FILTER}`
	AUTH_LDAP_ROLE_RECURSION	ロール検索が一致するコンテキストで行われる再帰のレベル数。再帰を無効にするには、これを 0 に設定します。	`\${AUTH_LDAP_ROLE_RECURSION}`
	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	`\${AUTH_LDAP_DEFAULT_ROLE}`
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。roleAttributesDN プロパティを true に設定すると、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定した場合には、DN は roleNameAttributeID に対してチェックされます。false に設定すると、DN は roleNameAttributeID に対して確認されません。このフラグは LDAP クエリーのパフォーマンスを向上できます。	`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`
	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	roleAttributeID にロールオブジェクトの完全修飾 DN が含まれるかどうか。false の場合は、コンテキスト名の roleNameAttributeID 属性の値からこのロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK	リファーラル (referral) を使用しない場合はこのオプションを使用する必要はありません。リファーラルを使用し、ロールオブジェクトがリファーラル内部にあると、このオプションは特定のロール (例: member) に対して定義されたユーザーが含まれる属性名を示します。ユーザーはこの属性名の内容に対して確認されます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファーラルツリーに保存できません。	`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping のログインモジュールで、指定したファイルを使用するように設定します。このプロパティは、ロールを置換ロールに対してマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	`\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}`
	AUTH_ROLE_MAPPER_REPLACE_ROLE	現在のロールを追加するか、マップされたロールに現在のロールを置き換えるか。true に設定した場合は、置き換えられます。	`\${AUTH_ROLE_MAPPER_REPLACE_ROLE}`
`\${APPLICATION_NAME}-amq`	AMQ_USER	標準ブローカーユーザーのユーザー名。ブローカーに接続するために必要です。空白の場合は生成されます。	`\${AMQ_USERNAME}`

デプロイメント	変数名	説明	値の例
	AMQ_PASSWORD	標準ブローカーユーザーのパスワード。ブローカーに接続するために必要です。空白の場合は生成されます。	\${AMQ_PASSWORD}
	AMQ_ROLE	標準ブローカーユーザーのユーザーロール。	\${AMQ_ROLE}
	AMQ_NAME	–	\${APPLICATION_NAME}-broker
	AMQ_TRANSPORTS	コンマで区切られた、設定するブローカーのプロトコル。許可される値は、 openwire 、 amqp 、 stomp 、および mqtt です。 openwire のみが EAP でサポートされません。	\${AMQ_PROTOCOL}
	AMQ_QUEUES	コンマで区切られたキュー名。これらのキューは、ブローカーの起動時に自動的に作成されます。さらに、これらは EAP で JNDI リソースとしてアクセス可能になります。これらのキューは KIE Server が必要とするデフォルトキューです。カスタムキューを使用する場合は、 KIE_SERVER_JMS_QUEUE_RESPONSE および KIE_SERVER_JMS_QUEUE_REQUEST と同じ値を使用します。	\${AMQ_QUEUES}
	AMQ_GLOBAL_MAX_SIZE	メッセージデータが使用可能な最大メモリー量を指定します。値が指定されていない場合は、システムのメモリーの半分が割り当てられます。	\${AMQ_GLOBAL_MAX_SIZE}
	AMQ_REQUIRE_LOGIN	–	false

デプロイメント	変数名	説明	値の例
	AMQ_ANYCAST_PR EFIX	–	–
	AMQ_MULTICAST_P REFIX	–	–

5.2.2.4.3.7. ボリューム

デプロイメント	名前	mountPath	目的	readOnly
\${APPLICATION _NAME}- kieserver	kieserver- keystore-volume	/etc/kieserver- secret-volume	ssl certs	True

5.2.2.5. 外部の依存関係

5.2.2.5.1. シークレット

このテンプレートでは、アプリケーションを実行するために以下のシークレットをインストールする必要があります。

kieserver-app-secret

5.3. OPENSIFT の使用に関するクイックリファレンス

Red Hat OpenShift Container Platform で Red Hat Decision Manager テンプレートのデプロイ、モニターリング、管理、デプロイ解除するには、OpenShift Web コンソールまたは **oc** コマンドを使用できます。

Web コンソールの使用に関する説明は、[Web コンソールを使用したイメージの作成およびビルド](#) を参照してください。

oc コマンドの使用方法に関する詳細は、[CLI リファレンス](#) を参照してください。次のコマンドが必要になる可能性があります。

- プロジェクトを作成するには、以下のコマンドを使用します。

```
$ oc new-project <project-name>
```

詳細は、[CLI を使用したプロジェクトの作成](#) を参照してください。

- テンプレートをデプロイするには (またはテンプレートからアプリケーションを作成するには)、以下のコマンドを実行します。

```
$ oc new-app -f <template-name> -p <parameter>=<value> -p <parameter>=<value> ...
```

詳細は、[CLI を使用したアプリケーションの作成](#) を参照してください。

- プロジェクト内のアクティブな Pod の一覧を表示するには、以下のコマンドを使用します。

```
$ oc get pods
```

- Pod のデプロイメントが完了し、実行中の状態になっているかどうかなど、Pod の現在のステータスを表示するには、以下のコマンドを使用します。

```
$ oc describe pod <pod-name>
```

oc describe コマンドを使用して、他のオブジェクトの現在のステータスを表示できます。詳細は、[アプリケーションの変更操作](#) を参照してください。

- Pod のログを表示するには、以下のコマンドを使用します。

```
$ oc logs <pod-name>
```

- デプロイメントログを表示するには、テンプレート参照で **DeploymentConfig** 名を検索し、以下のコマンドを入力します。

```
$ oc logs -f dc/<deployment-config-name>
```

詳細は、[デプロイメントログの表示](#) を参照してください。

- ビルドログを表示するには、テンプレート参照で **BuildConfig** 名を検索し、以下のコマンドを入力します。

```
$ oc logs -f bc/<build-config-name>
```

詳細は、[ビルドログのアクセス](#) を参照してください。

- アプリケーションの Pod をスケーリングするには、テンプレート参照で **DeploymentConfig** 名を検索し、以下のコマンドを入力します。

```
$ oc scale dc/<deployment-config-name> --replicas=<number>
```

詳細は、[手動スケーリング](#) を参照してください。

- アプリケーションのデプロイメントを解除するには、以下のコマンドを使用してプロジェクトを削除します。

```
$ oc delete project <project-name>
```

または、**oc delete** コマンドを使用して、Pod またはレプリケーションコントローラーなど、アプリケーションの一部を削除できます。詳細は、[アプリケーションの修正操作](#) を参照してください。

付録A バージョン情報

本書の最終更新日: 2021年11月15日(月)