



## Red Hat Decision Manager 7.2

# 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メント

ガイド



# Red Hat Decision Manager 7.2 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 © 2023 | You need to change the HOLDER entity in the en-US/Deploying\_a\_Red\_Hat\_Decision\_Manager\_authoring\_or\_managed\_server\_environment\_on\_Red\_hat 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<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

Java<sup>®</sup> is a registered trademark of Oracle and/or its affiliates.

XFS<sup>®</sup> is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL<sup>®</sup> is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js<sup>®</sup> 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<sup>®</sup> 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 7.2 オーサリングまたは管理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. DECISION CENTRAL へのシークレットの作成	8
2.4. GLUSTERFS 設定の変更	9
第3章 オーサリングまたは管理サーバー環境 .....	11
3.1. オーサリングまたは管理サーバー環境での単一の DECISION CENTRAL と DECISION SERVER 1 台のデプロイ	11
3.2. オーサリングまたは管理サーバー環境での高可用性の DECISION CENTRAL と DECISION SERVER 1 台のデプロイ	16
3.3. GIT フックディレクトリーの指定	21
3.4. 追加の DECISION SERVER のデプロイ	23
3.5. LDAP ロールマッピングファイルの指定	26
第4章 OPENSIFT テンプレートの参考資料 .....	28
4.1. RHDM72-AUTHORING.YAML TEMPLATE	28
4.1.1. パラメーター	28
4.1.2. オブジェクト	41
4.1.2.1. サービス	41
4.1.2.2. ルート	42
4.1.2.3. デプロイメント設定	42
4.1.2.3.1. トリガー	42
4.1.2.3.2. レプリカ	42
4.1.2.3.3. Pod テンプレート	43
4.1.2.4. 外部の依存関係	61
4.1.2.4.1. ボリューム要求	61
4.1.2.4.2. シークレット	61
4.2. RHDM72-AUTHORING-HA.YAML TEMPLATE	61
4.2.1. パラメーター	61
4.2.2. オブジェクト	77
4.2.2.1. サービス	77
4.2.2.2. ルート	78
4.2.2.3. デプロイメント設定	78
4.2.2.3.1. トリガー	79
4.2.2.3.2. レプリカ	79
4.2.2.3.3. Pod テンプレート	79
4.2.2.4. 外部の依存関係	100
4.2.2.4.1. ボリューム要求	100
4.2.2.4.2. シークレット	101
4.2.2.4.3. クラスターリング	101
4.3. RHDM72-KIESERVER.YAML TEMPLATE	102
4.3.1. パラメーター	102
4.3.2. オブジェクト	115
4.3.2.1. サービス	115
4.3.2.2. ルート	116
4.3.2.3. デプロイメント設定	116
4.3.2.3.1. トリガー	116

4.3.2.3.2. レプリカ	116
4.3.2.3.3. Pod テンプレート	116
4.3.2.4. 外部の依存関係	127
4.3.2.4.1. シークレット	127
4.4. OPENSIFT の使用に関するクイックリファレンス	127
<b>付録A バージョン情報</b> .....	<b>130</b>



## はじめに

システムエンジニアは、Red Hat OpenShift Container Platform に Red Hat Decision Manager オーサリングまたは管理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開発するプラットフォームを提供します。

### 前提条件

- OpenShift クラスター/名前空間で 4 ギガバイト以上のメモリーが利用できる。
- デプロイメント用の OpenShift プロジェクトが作成されている。
- プロジェクトにログインするには、**oc** コマンドを使用します。**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する必要があります。
- 動的永続ボリューム (PV) のプロビジョニングを有効にする必要があります。または、動的 PV プロビジョニングが有効でない場合には、十分な永続ボリュームが利用できる状態であればなりません。デフォルトでは、Decision Central は 1 Gi 分の PV が必要です。テンプレートパラメーターで、Decision Central 永続ストレージの PV サイズを変更することができます。
- Decision Central Pod をスケーリングする Authoring High Availability テンプレートを使用する場合:
  - Red Hat AMQ バージョン 7.1 以降のイメージストリームは、OpenShift 環境で使用できる必要があります。
  - OpenShift 環境は、ReadWriteMany モードで永続ボリュームをサポートする必要があります。OpenShift Online ボリュームプラグインでのアクセスモードのサポートに関する情報は、[アクセスモード](#) を参照してください。



# 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 のスケールアップと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。

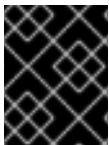
- Decision Server (**実行サーバー (Execution Server)** または **KIE Server** と呼ばれる) は、インフラストラクチャーの要素でデシジョンサービスやその他のデプロイ可能なアセットを実行します (これらすべてで総称で **サービス** と呼ぶ)。サービスのすべてのロジックは実行サーバーで実行されます。

Decision Server Pod は自由に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に必要な数だけ提供できます。Pod をスケールアップまたはスケールダウンすると、そのコピーはすべて同じプロセスで実行します。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。個別の複製 Decision Server Pod を必要な数だけ設定することができます。

- Decision Central は、オーサリングサービス用の Web ベースの対話環境で、Decision Central では管理コンソールが提供されています。Business Central は管理コンソールも提供します。Decision Central を使用してサービスを開発し、Decision Server にデプロイできます。Decision Central は集中型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。

Decision 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、Decision 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、Decision Central の高可用性機能はテクノロジープレビューです。

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:** Decision 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 Decision 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。Decision Central を使用して、各 Decision Server にサービスをデプロイおよびアンデプロイできます。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、Decision 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には、OpenShift ではイメージの場所情報 (イメージストリームと呼ばれる) が必要です。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。

それ以外の場合には、独自のプロジェクトでレジストリーの認証を設定して、その同じプロジェクト内にイメージストリームを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 は、Red Hat のレジストリーアクセス用にユーザー名とパスワードで設定する場合には、以下のコマンドを使用します。

```
$ oc get imagestreamtag -n openshift | grep rhdm72-decisioncentral-openshift
$ oc get imagestreamtag -n openshift | grep rhdm72-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て、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します。
  - 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-7.2.0-openshift-templates.zip](#) 製品の配信可能ファイルをダウンロードし、**rhdm72-image-streams.yaml** ファイルを展開してください。
- g. 以下のアクションの1つを完了します。
- 次のコマンドを実行します。

```
$ oc create -f rhdm72-image-streams.yaml
```

- OpenShift Web UI で **Add to Project** → **Import YAML / JSON** を選択し、ファイルを選択するか、ファイル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。この手順を使用してイメージストリームをインストールした場合には、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。詳細は、OpenShift ドキュメントの [Secrets](#) の章を参照してください。

Decision Server に SSL 証明書を作成し、それをシークレットとして OpenShift 環境に提供します。

### 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。プロダクション環境で、期待する Decision Server の URL に一致する有効な署名付き証明書を生成します。キーストアを **keystore.jks** ファイルに保存します。証明書の名前と、キーストアファイルのパスワードを記録します。  
自己署名型または購入する SSL 証明書を使用して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の生成](#) を参照してください。
2. **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. DECISION CENTRAL へのシークレットの作成

OpenShift 環境に Decision Central をデプロイする場合は、Decision Central に SSL 証明書を作成し、OpenShift 環境にシークレットとして提供します。Decision Central と Decision Server には、同じ証明書とキーストアを使用しないでください。

## 手順

1. Decision Central 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。プロダクション環境で、期待する Decision Central の URL に一致する有効な署名付き証明書を生成します。キーストアを **keystore.jks** ファイルに保存します。証明書の名前と、キーストアファイルのパスワードを記録します。  
自己署名型または購入する SSL 証明書を使用して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の生成](#)を参照してください。
2. **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 **decisioncentral-app-secret** を生成します。

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

## 2.4. GLUSTERFS 設定の変更

OpenShift 環境が GlusterFS を使用して永続的なストレージボリュームを提供するかどうかを確認します。GlusterFS を使用している場合は最適なパフォーマンスを確保するために、ストレージクラスの設定を変更して GlusterFS ストレージをチューニングします。

## 手順

1. お使いの環境で GlusterFS が使用されているかどうかを確認するには、以下のコマンドを実行します。

```
oc get storageclass
```

この結果で、**(default)** マーカーが、**glusterfs** をリストするストレージクラスにあるかどうかを確認します。たとえば、以下の結果では、デフォルトのストレージクラスが **gluster-container** であり、**glusterfs** をリストします。

```
NAME                PROVISIONER          AGE
gluster-block      gluster.org/glusterblock  8d
gluster-container (default)  kubernetes.io/glusterfs  8d
```

結果に、**glusterfs** をリストしないデフォルトストレージクラスが含まれる場合、または結果が空の場合は、変更する必要がありません。変更しない場合は、残りの手順を省略します。

2. デフォルトストレージクラスの設定を YAML ファイルに保存するには、以下のコマンドを実行します。

```
oc get storageclass <class-name> -o yaml >storage_config.yaml
```

**class-name** は、デフォルトのストレージクラスの名前です。以下に例を示します。

```
oc get storageclass gluster-container -o yaml >storage_config.yaml
```

3. **storage\_config.yaml** ファイルを編集します。
  - a. 以下のキーがある行を削除します。

- **creationTimestamp**
- **resourceVersion**
- **selfLink**
- **uid**

- b. **volumeoptions** キーのある行に、**features.cache-invalidation on** および **performance.nl-cache on** の 2 つのパラメーターを追加します。以下に例を示します。

```
volumeoptions: client.ssl off, server.ssl off, features.cache-invalidation on,  
performance.nl-cache on
```

4. 既存のデフォルトストレージクラスを削除するには、以下のコマンドを実行します。

```
oc delete storageclass <class-name>
```

**class-name** は、デフォルトのストレージクラスの名前です。以下に例を示します。

```
oc delete storageclass gluster-container
```

5. 新しい設定を使用してストレージクラスを再作成するには、以下のコマンドを実行します。

```
oc create -f storage_config.yaml
```

## 第3章 オーサリングまたは管理サーバー環境

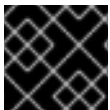
Decision Central を使用してサービスを作成および変更し、Decision Central によって管理される Decision Server でサービスを実行するための環境をデプロイできます。この環境は、Decision Central と1つ以上の Decision Server で設定されます。

Decision Central を使用して、サービスを開発するだけでなく、このサービスを1つまたは複数の Decision Server にもデプロイできます。たとえば、サービスのテスト版を Decision Server 1台にデプロイして、別の Decision Server に実稼働版をデプロイできます。

実稼働の Decision Server に違うバージョンを誤ってデプロイしないように、サービスをオーサリングする環境 (**オーサリング環境**) と、実稼働サービスのデプロイメントを管理する環境 (**管理サーバー環境**) を別個作成できます。オーサリング環境にデプロイしたサービスを管理サーバー環境で利用できるように、これらの環境間を共有する外部 Maven リポジトリを使用できます。ただし、これらの環境をデプロイする手順は同じです。

ニーズに合わせて、単一または高可用性の Decision Central をデプロイできます。単一の Decision Central Pod は複製されません。Decision Central の1つのコピーのみが使用されます。HA Decision Central デプロイメントでは、Decision Central をスケーリングできます。

HA Decision Central では、オーサリングサービスの信頼性や応答性を最大化できますが、メモリーとストレージ要件が高くなり、ReadWriteMany モードのある永続ボリュームのサポートが必要です。



### 重要

現在のバージョンでは、高可用性機能はテクノロジープレビューです。

オーサリングまたは管理サーバー環境では、必要に応じて Decision Server Pod をスケーリングできます。

オーサリングまたは管理サーバー環境をデプロイするには、まずオーサリングテンプレートを使用して単一または高可用性の Business Central と Decision Server 1台をデプロイします。

さらに Decision Server を追加するには、同じプロジェクトで Decision Server テンプレートをデプロイできます。

### 3.1. オーサリングまたは管理サーバー環境での単一の DECISION CENTRAL と DECISION SERVER 1台のデプロイ

オーサリングまたは管理サーバー環境に単一の Decision Central および Decision Server 1台をデプロイするには、**rhdm72-authoring.yaml** テンプレートファイルを使用します。**rhdm-7.2.0-openshift-templates.zip** の製品配信可能ファイルからこのファイルを展開できます。[Software Downloads](#) ページからこのファイルをダウンロードできます。

#### 手順

1. 以下の方法を使用してテンプレートをデプロイします。
  - OpenShift Web UI では、**Add to Project** → **Import YAML / JSON**を選択し、**rhdm72-authoring.yaml** ファイルを選択またはその内容を貼り付けます。**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>/rhdm72-authoring.yaml -p
DECISION_CENTRAL_HTTPS_SECRET=decisioncentral-app-secret -p
KIE_SERVER_HTTPS_SECRET=kieserver-app-secret
```

このコマンドラインで以下を行います。

- **<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。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。

2. 必要に応じて以下のパラメーターを設定します。

- **Decision Central サーバーキーストアのシークレット名 (DECISION\_CENTRAL\_HTTPS\_SECRET):** 「[Decision Central へのシークレットの作成](#)」で作成した Decision Central のシークレットの名前。
- **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。
- **アプリケーション名 (APPLICATION\_NAME):** OpenShift アプリケーションの名前。Decision Central 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で、Decision Server が参加する Decision Central でサーバー設定 (サーバーテンプレート) の名前が決まります。
- **Decision Central サーバーの証明署名 (DECISION\_CENTRAL\_HTTPS\_NAME):** 「[Decision Central へのシークレットの作成](#)」で作成したキーストアの証明書の名前。
- **Decision Central サーバーキーストアのパスワード (DECISION\_CENTRAL\_HTTPS\_PASSWORD):** 「[Decision Central への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。
- **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。
- **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。以下のユーザー名およびパスワードを設定することもできます。
- **KIE Admin User (KIE\_ADMIN\_USER) および KIE Admin Password (KIE\_ADMIN\_PWD):** Decision Central の管理ユーザーのユーザー名およびパスワード。
- **KIE Server ユーザー (KIE\_SERVER\_USER) および KIE Server パスワード (KIE\_SERVER\_PWD):** Decision Server に接続するのにクライアントアプリケーションが使用するユーザー名およびパスワード。



3. Decision Server を追加でデプロイして、この Decision Central に接続するには、以下のパラメーターを設定します。
  - KIE Server コントローラーのユーザー名(**KIE\_SERVER\_CONTROLLER\_USER**) および KIE Server コントローラーのパスワード(**KIE\_SERVER\_CONTROLLER\_PWD**): Decision Central への接続に Decision Server が使用する必要のあるユーザー名とパスワード。
4. ビルドした KJAR ファイルを外部の Maven リポジトリに置く場合は、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 リポジトリのユーザー名(**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。
  - Maven リポジトリ ID(**MAVEN\_REPO\_ID**): Maven ID。Maven リポジトリの **id** 設定と一致する必要があります。



### 重要

Decision Central プロジェクトを KJAR アーティファクトとして外部の Maven リポジトリにエクスポートまたはプッシュするには、全プロジェクトの **pom.xml** ファイルにもリポジトリ情報を追加する必要があります。Decision Central プロジェクトの外部リポジトリへのエクスポートに関する情報は、[Red Hat Decision Manager プロジェクトのパッケージ化およびデプロイ](#) を参照してください。

または、Decision Central に組み込まれている Maven リポジトリを使用し、Decision Central に Decision Server を追加で接続する場合には、以下のパラメーターを設定します。

- Decision Central がホストする Maven サービスのユーザー名 (**DECISION\_CENTRAL\_MAVEN\_USERNAME**): ビルドインの Maven リポジトリのユーザー名。
  - Decision Central がホストする Maven サービスのパスワード (**DECISION\_CENTRAL\_MAVEN\_PASSWORD**): ビルドインの Maven リポジトリのパスワード。
5. Git フックを使用して Decision Central の内部 Git リポジトリと外部 Git リポジトリの対話を容易にすることができます。Git フックを設定するには、以下のパラメーターを設定します。
    - Git フックディレクトリー (**GIT\_HOOKS\_DIR**): Git フックディレクトリーへの完全修飾パス (例: **/opt/eap/standalone/data/kie/git/hooks**)。このディレクトリーのコンテンツを渡して、指定のパスにマウントする必要があります。方法は、「[Git フックディレクトリーの指定](#)」を参照してください。
  6. RH-SSO または LDAP 認証を使用する場合は、以下の追加設定を実行します。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。
    - a. RH-SSO または LDAP サービスでは、デプロイメントパラメーターで全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\_CONTROLLER\_USER**: デフォルトのユーザー名 **controllerUser**、ロール: **kie-server,rest-all,guest**
  - **DECISION\_CENTRAL\_MAVEN\_USERNAME** (外部の Maven リポジトリを使用するように設定している場合には必要なし): デフォルトのユーザー名 **mavenUser**。ロールは必要ありません。
  - **KIE\_SERVER\_USER**: デフォルトのユーザー名 **executionUser**、ロール **kie-server,rest-all,guest**
- b. Red Hat Single Sign On (RH-SSO) 認証を設定する場合には、Red Hat Decision Manager を適用する RH-SSO レalmが必要です。クライアントが存在しない場合は、テンプレートを使用してデプロイメント中に作成できます。また、RH-SSO 内のクライアントは、Business Central 用と Decision Server 用が必要です。RH-SSO 内のクライアントは、Decision Central および Decision Server にも存在する必要があります。クライアントがまだ存在しない場合は、デプロイメント中にテンプレートで作成できます。RH-SSO で設定可能なユーザールールについては、[ロールおよびユーザー](#) を参照してください。

以下の手順の1つを使用します。

- i. RH-SSO 内にすでに Red Hat Decision Manager のクライアントが存在する場合には、テンプレートで以下のパラメーターを設定してください。
- **RH-SSO URL (SSO\_URL)**: RH-SSO の URL。
  - **RH-SSO レalm名 (SSO\_REALM)**: Red Hat Decision Manager の RH-SSO レalm。
  - **Decision Central RH-SSO クライアント名 (DECISION\_CENTRAL\_SSO\_CLIENT)**: Decision Central の RH-SSO クライアント名。
  - **Decision Central RH-SSO クライアントのシークレット (DECISION\_CENTRAL\_SSO\_SECRET)**: Decision Central のクライアント向けに RH-SSO で設定するシークレット文字列。
  - **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。
  - **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。
- ii. 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。
- **RH-SSO URL (SSO\_URL)**: RH-SSO の URL。

- **RH-SSO レalm名 (SSO\_REALM):** Red Hat Decision Manager の RH-SSO レalm。
  - **Decision Central RH-SSO クライアント名 (DECISION\_CENTRAL\_SSO\_CLIENT):** Decision Central 向けに RH-SSO に作成するクライアント名。
  - **Decision Central RH-SSO クライアントのシークレット (DECISION\_CENTRAL\_SSO\_SECRET):** Decision Central のクライアント向けに RH-SSO で設定するシークレット文字列。
  - **Decision Central カスタムの http ルートホスト名 (DECISION\_CENTRAL\_HOSTNAME\_HTTP):** Decision Central の HTTP エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **Decision Central カスタムの https ルートホスト名 (DECISION\_CENTRAL\_HOSTNAME\_HTTPS):** Decision Central の HTTPS エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **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。
  - **KIE Server カスタムの http ルートホスト名 (KIE\_SERVER\_HOSTNAME\_HTTP):** Decision Server の HTTP エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **KIE Server カスタムの https ルートホスト名 (KIE\_SERVER\_HOSTNAME\_HTTPS):** Decision Server の HTTPS エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **RH-SSO レalmの管理者のユーザー名 (SSO\_USERNAME) および RH-SSO レalmの管理者のパスワード (SSO\_PASSWORD):** Red Hat Decision Manager の RH-SSO レalmの管理者ユーザーに指定するユーザー名とパスワード
  - **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。
- c. LDAP を設定するには、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、「[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。

7. 使用している方法に応じて、環境の作成を終了します。

- 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。
- 完了し、コマンドラインを実行します。

## 3.2. オーサリングまたは管理サーバー環境での高可用性の DECISION CENTRAL と DECISION SERVER 1 台のデプロイ

高可用性の Decision Central と Decision Server 1 台をオーサリングまたは管理サーバー環境にデプロイするには、**rhdm72-authoring-ha.yaml** テンプレートファイルを使用します。[Software Downloads](#) ページからこのファイルをダウンロードできます。



### 重要

現在のバージョンでは、高可用性機能はテクノロジープレビューです。

### 手順

1. 以下の方法を使用してテンプレートをデプロイします。

- OpenShift Web UI では、**Add to Project** → **Import YAML / JSON** を選択し、**rhdm72-authoring-ha.yaml** ファイルを選択またはその内容を貼り付けます。**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>/rhdm72-authoring-ha.yaml -p
DECISION_CENTRAL_HTTPS_SECRET=decisioncentral-app-secret -p
KIE_SERVER_HTTPS_SECRET=kieserver-app-secret
```

このコマンドラインで以下を行います。

- **<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。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。

2. 必要に応じて以下のパラメーターを設定します。

- **Decision Central サーバーキーストアのシークレット名 (DECISION\_CENTRAL\_HTTPS\_SECRET):** 「[Decision Central へのシークレットの作成](#)」で作成した Decision Central のシークレットの名前。
- **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。
- **アプリケーション名 (APPLICATION\_NAME):** OpenShift アプリケーションの名前。Decision Central 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で、Decision Server が参加する Decision Central でサーバー設定 (サーバーテンプレート) の名前が決まります。
- **Decision Central サーバーの証明署名 (DECISION\_CENTRAL\_HTTPS\_NAME):** 「[Decision Central へのシークレットの作成](#)」で作成したキーストアの証明書の名前。
- **Decision Central サーバーキーストアのパスワード (DECISION\_CENTRAL\_HTTPS\_PASSWORD):** 「[Decision Central への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。
- **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。
- **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。以下のユーザー名およびパスワードを設定することもできます。
- **KIE Admin User (KIE\_ADMIN\_USER) および KIE Admin Password (KIE\_ADMIN\_PWD):** Decision Central の管理ユーザーのユーザー名およびパスワード。
- **KIE Server ユーザー (KIE\_SERVER\_USER) および KIE Server パスワード (KIE\_SERVER\_PWD):** Decision Server に接続するのにクライアントアプリケーションが使用するユーザー名およびパスワード。

3. Decision Server を追加でデプロイして、この Decision Central に接続するには、以下のパラメーターを設定します。

- **KIE Server コントローラーのユーザー r (KIE\_SERVER\_CONTROLLER\_USER) および KIE Server コントローラーのパスワード (KIE\_SERVER\_CONTROLLER\_PWD):** Decision Central への接続に Decision Server が使用する必要のあるユーザー名とパスワード。

4. ビルドした KJAR ファイルを外部の Maven リポジトリに置く場合は、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 リポジトリのユーザー名 (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。
- **Maven リポジトリ ID (MAVEN\_REPO\_ID):** Maven ID。Maven リポジトリの **id** 設定と一致する必要があります。



### 重要

Decision Central プロジェクトを KJAR アーティファクトとして外部の Maven リポジトリにエクスポートまたはプッシュするには、全プロジェクトの **pom.xml** ファイルにもリポジトリ情報を追加する必要があります。Decision Central プロジェクトの外部リポジトリへのエクスポートに関する情報は、[Red Hat Decision Manager プロジェクトのパッケージ化およびデプロイ](#) を参照してください。

または、Decision Central に組み込まれている Maven リポジトリを使用し、Decision Central に Decision Server を追加で接続する場合には、以下のパラメーターを設定します。

- **Decision Central がホストする Maven サービスのユーザー名 (DECISION\_CENTRAL\_MAVEN\_USERNAME):** ビルドインの Maven リポジトリのユーザー名。
  - **Decision Central がホストする Maven サービスのパスワード (DECISION\_CENTRAL\_MAVEN\_PASSWORD):** ビルドインの Maven リポジトリのパスワード。
5. Git フックを使用して Decision Central の内部 Git リポジトリと外部 Git リポジトリの対話を容易にすることができます。Git フックを設定するには、以下のパラメーターを設定します。
- **Git フックディレクトリー (GIT\_HOOKS\_DIR):** Git フックディレクトリーへの完全修飾パス (例: `/opt/eap/standalone/data/kie/git/hooks`)。このディレクトリーのコンテンツを渡して、指定のパスにマウントする必要があります。方法は、「[Git フックディレクトリーの指定](#)」を参照してください。
6. RH-SSO または LDAP 認証を使用する場合は、以下の追加設定を実行します。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。
- RH-SSO または LDAP サービスでは、デプロイメントパラメーターで全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\_CONTROLLER\_USER:** デフォルトのユーザー名 `controllerUser`、ロール: `kie-server,rest-all,guest`
    - **DECISION\_CENTRAL\_MAVEN\_USERNAME** (外部の Maven リポジトリを使用するように設定している場合には必要なし): デフォルトのユーザー名 `mavenUser`。ロールは必要ありません。
    - **KIE\_SERVER\_USER:** デフォルトのユーザー名 `executionUser`、ロール `kie-server,rest-all,guest`

- b. Red Hat Single Sign On (RH-SSO) 認証を設定する場合には、Red Hat Decision Manager を適用する RH-SSO レalmが必要です。クライアントが存在しない場合は、テンプレートを使用してデプロイメント中に作成できます。また、RH-SSO 内のクライアントは、Business Central 用と Decision Server 用が必要です。RH-SSO 内のクライアントは、Decision Central および Decision Server にも存在する必要があります。クライアントがまだ存在しない場合は、デプロイメント中にテンプレートで作成できます。RH-SSO で設定可能なユーザールールについては、[ロールおよびユーザー](#) を参照してください。

以下の手順の1つを使用します。

- i. RH-SSO 内にすでに Red Hat Decision Manager のクライアントが存在する場合には、テンプレートで以下のパラメーターを設定してください。
- **RH-SSO URL (SSO\_URL):** RH-SSO の URL。
  - **RH-SSO レalm名 (SSO\_REALM):** Red Hat Decision Manager の RH-SSO レalm。
  - **Decision Central RH-SSO クライアント名 (DECISION\_CENTRAL\_SSO\_CLIENT):** Decision Central の RH-SSO クライアント名。
  - **Decision Central RH-SSO クライアントのシークレット (DECISION\_CENTRAL\_SSO\_SECRET):** Decision Central のクライアント向けに RH-SSO で設定するシークレット文字列。
  - **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。
  - **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。
- ii. 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。
- **RH-SSO URL (SSO\_URL):** RH-SSO の URL。
  - **RH-SSO レalm名 (SSO\_REALM):** Red Hat Decision Manager の RH-SSO レalm。
  - **Decision Central RH-SSO クライアント名 (DECISION\_CENTRAL\_SSO\_CLIENT):** Decision Central 向けに RH-SSO に作成するクライアント名。
  - **Decision Central RH-SSO クライアントのシークレット (DECISION\_CENTRAL\_SSO\_SECRET):** Decision Central のクライアント向けに RH-SSO で設定するシークレット文字列。
  - **Decision Central カスタムの http ルートホスト名 (DECISION\_CENTRAL\_HOSTNAME\_HTTP):** Decision Central の HTTP エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要があります。

る場合には、このパラメーターを空白のままにしてください。

- **Decision Central カスタムの https ルートホスト名 (DECISION\_CENTRAL\_HOSTNAME\_HTTPS):** Decision Central の HTTPS エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **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。
  - **KIE Server カスタムの http ルートホスト名 (KIE\_SERVER\_HOSTNAME\_HTTP):** Decision Server の HTTP エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **KIE Server カスタムの https ルートホスト名 (KIE\_SERVER\_HOSTNAME\_HTTPS):** Decision Server の HTTPS エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **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
  - **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。
- c. LDAP を設定するには、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、「[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。

7. デフォルト設定の **openshift** namespace で AMQ 7.1 イメージを使用できない場合は、次のパラメーターを設定します。



- **AMQ ImageStream namespace (AMQ\_IMAGE\_STREAM\_NAMESPACE)**: AMQ イメージの ImageStream がインストールされる namespace。デフォルト設定は **openshift** です。
  - **AMQ ImageStream Name (AMQ\_IMAGE\_STREAM\_NAME)**: AMQ ブローカーのイメージストリームの名前。デフォルト設定は **amq-broker71-openshift** です。
  - **AMQ ImageStream タグ (AMQ\_IMAGE\_STREAM\_TAG)**: AMQ イメージストリームタグ。デフォルト設定は **1.0** です。
8. 使用している方法に応じて、環境の作成を終了します。
- 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。
  - 完了し、コマンドラインを実行します。

### 3.3. GIT フックディレクトリーの指定

**GIT\_HOOKS\_DIR** パラメーターを設定した場合には、Git フックのディレクトリーを指定して、Decision Central デプロイメントにこのディレクトリーをマウントする必要があります。

Git フックは一般的に、アップストリームのリポジトリーとの対話に使用します。Git フックを使用して、アップストリームのリポジトリーにコミットをプッシュできるようにするには、アップストリームのリポジトリーで設定した公開鍵に対応する秘密鍵を指定する必要があります。

#### 手順

1. SSH 認証を使用してアップストリームリポジトリーを操作する必要がある場合は、次の手順を実行して、必要なファイルを含むシークレットを作成してマウントします。
  - a. リポジトリーに格納されている公開鍵に一致する秘密鍵を使用して、**id\_rsa** ファイルを作成します。
  - b. リポジトリーの正しい名前、アドレス、公開鍵で **known\_hosts** ファイルを作成します。
  - c. 以下のように **oc** コマンドを使用して、2つのファイルでシークレットを作成します。

```
oc create secret git-hooks-secret --from-file=id_rsa=id_rsa --from-file=known_hosts=known_hosts
```

- d. シークレットを Decision Central デプロイメントの SSH キーパスにマウントします。次に例を示します。

```
oc set volume dc/<myapp>-rhdmcenr --add --type secret --secret-name git-hooks-secret --mount-path=/home/jboss/.ssh --name=ssh-key
```

**<myapp>** は、テンプレート設定時に指定したアプリケーション名に置き換えます。

2. Git フックディレクトリーを作成します。方法は、[Git hooks reference documentation](#) を参照してください。  
たとえば、単純な git フックのディレクトリーでは、アップストリームの変更をプッシュするコミット後のフックを提供可能です。プロジェクトがリポジトリーから Decision Central にインポートされた場合、このリポジトリーはアップストリームリポジトリーとして設定されたま

まになります。パーミッションを **755** の値に指定し、以下の内容を含めて **post-commit** という名前のファイルを作成します。

```
git push
```

3. Git hooks ディレクトリーを Decision Central デプロイメントに提供します。設定マップまたは永続ボリュームを使用できます。
  - a. Git フックに1つまたは複数の固定スクリプトファイルが含まれる場合は、設定マップを使用します。以下の手順を実行してください。

- i. 作成した Git フックディレクトリーに移動します。

- ii. ディレクトリーのファイルから OpenShift 設定マップを作成します。次のコマンドを実行します。

```
oc create configmap git-hooks --from-file=<file_1>=<file_1> --from-file=<file_2>=<file_2> ...
```

**file\_1**、**file\_2** などは、git フックのスクリプトファイルに置き換えます。以下に例を示します。

```
oc create configmap git-hooks --from-file=post-commit=post-commit
```

- iii. Decision Central デプロイメントの設定したパスに設定マップをマウントします。

```
oc set volume dc/<myapp>-rhdmcentr --add --type configmap --configmap-name git-hooks --mount-path=<git_hooks_dir> --name=git-hooks
```

**<myapp>** は、テンプレートの設定時に指定したアプリケーション名に、**<git\_hooks\_dir>** はテンプレート設定時に指定した **GIT\_HOOKS\_DIR** の値に置き換えます。

- b. Git フックが長いファイルで設定されているか、または実行可能なファイルや KJAR ファイルなどのバイナリーに依存する場合は、永続ボリュームを使用します。永続ボリュームを作成し、永続ボリューム要求を作成してその要求をボリュームに関連付けてから、そのボリュームにファイルを転送して、**myapp-rhdmcentr** デプロイメント設定にこのボリュームをマウントしてください (**myapp** はアプリケーション名に置き換えてください)。永続ボリュームの作成およびマウント方法は、[永続ボリュームの使用](#) を参照してください。永続ボリュームへのファイルのコピー方法は、[Transferring files in and out of containers](#) を参照してください。
4. 数分待つてから、プロジェクト内のリストと Pod のステータスを確認します。Decision Central は git フックディレクトリーが指定されるまで開始されないのので、Decision Server はまったく起動されない可能性があります。Process Server が起動しているかどうかを確認するには、以下のコマンドの出力で確認します。

```
oc get pods
```

稼働中の Decision Server Pod がない場合には、起動します。

```
oc rollout latest dc/<myapp>-kieserver
```

**<myapp>** は、テンプレート設定時に指定したアプリケーション名に置き換えます。

### 3.4. 追加の DECISION SERVER のデプロイ

追加の Decision Server は、管理対象サーバーのインフラストラクチャーの一部として、OpenShift インフラストラクチャーにデプロイ可能です。デプロイ後は、Decision Central を使用して、この Decision Server にサーバーのデプロイ、デプロイ解除および管理が可能です。

追加の Decision Server をデプロイするには、**rhdm72-kieserver.yaml** テンプレートファイルを使用します。[Software Downloads](#) ページからこのファイルをダウンロードできます。

#### 手順

1. 以下の方法を使用してテンプレートをデプロイします。

- OpenShift Web UI では、**Add to Project → Import YAML / JSON**を選択し、**rhdm72-kieserver.yaml** ファイルを選択またはその内容を貼り付けます。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>/rhdm72-kieserver.yaml -p
KIE_SERVER_HTTPS_SECRET=kieserver-app-secret
```

このコマンドラインで以下を行います。

- **<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。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。

2. 以下のパラメーターを設定します。

- **KIE サーバーコントローラーのサービス (KIE\_SERVER\_CONTROLLER\_SERVICE)**: この環境にインストールした Decision Central に対する OpenShift サービス名。
- **KIE サーバーコントローラーのユーザー (KIE\_SERVER\_CONTROLLER\_USER)**: 設定した Decision Central にログインするコントローラーのユーザー名。
- **KIE サーバーコントローラーのパスワード (KIE\_SERVER\_CONTROLLER\_PWD)**: 設定した Decision Central にログインするコントローラーのパスワード。
- **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。
- **アプリケーション名 (APPLICATION\_NAME)**: OpenShift アプリケーションの名前。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で、Decision Server が参加する Decision Central でサーバー設定 (サーバーテンプレート) の名前が決まります。
- **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。
3. Decision Central で使用するリポジトリにビルドインか、外部のリポジトリのどちらを設定したのかに合わせて、Maven リポジトリにアクセスするためのパラメーターを設定します。
- a. ビルドインリポジトリの場合:
- **Decision Central がホストする Maven サービスの名前 (DECISION\_CENTRAL\_MAVEN\_SERVICE):** Decision Central の組み込み Maven リポジトリのサービス名。
  - **Decision Central がホストする Maven サービスのユーザー名 (DECISION\_CENTRAL\_MAVEN\_USERNAME):** Decision Central にビルドインの Maven リポジトリのユーザー名。 **DECISION\_CENTRAL\_MAVEN\_USERNAME** として Decision Central に設定したユーザー名を入力してください。
  - **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):** Decision Central にビルドインされている Maven リポジトリのパスワード。 Decision Central に **DECISION\_CENTRAL\_MAVEN\_PASSWORD** として設定されているパスワードを入力します。
- b. 外部リポジトリの場合:
- **Maven リポジトリの URL (MAVEN\_REPO\_URL):** サービスが含まれている Maven リポジトリの URL。
  - **Maven リポジトリのユーザー名 (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。



#### 注記

お使いのサービスが Decision Central にビルドインされている Maven リポジトリと、外部 Maven リポジトリの両方に依存している場合には、両方のリポジトリに対するアクセスを設定できます。

4. RH-SSO または LDAP 認証を使用する場合は、以下の追加設定を実行します。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。
- a. RH-SSO または LDAP サービスでは、デプロイメントパラメーターで全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**
- b. Red Hat Single Sign On (RH-SSO) 認証を設定する場合には、Red Hat Decision Manager を適用する RH-SSO レルムが必要です。また、RH-SSO 内にクライアントが必要です。RH-SSO で設定可能なユーザールールについては、[ロールおよびユーザー](#) を参照してください。

以下の手順の1つを使用します。

- i. RH-SSO 内にすでに Red Hat Decision Manager のクライアントが存在する場合には、テンプレートで以下のパラメーターを設定してください。
  - **RH-SSO URL (SSO\_URL)**: RH-SSO の URL。
  - **RH-SSO レalm名 (SSO\_REALM)**: Red Hat Decision Manager の RH-SSO レalm。
  - **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。
  - **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。
- ii. 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。
  - **RH-SSO URL (SSO\_URL)**: RH-SSO の URL。
  - **RH-SSO レalm名 (SSO\_REALM)**: Red Hat Decision Manager の RH-SSO レalm。
  - **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。
  - **KIE Server カスタムの http ルートホスト名 (KIE\_SERVER\_HOSTNAME\_HTTP)**: Decision Server の HTTP エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **KIE Server カスタムの https ルートホスト名 (KIE\_SERVER\_HOSTNAME\_HTTPS)**: Decision Server の HTTPS エンドポイントに使用する完全修飾ホスト名。RH-SSO にクライアントを作成する必要がある場合には、このパラメーターを空白のままにしてください。
  - **RH-SSO レalmの管理者のユーザー名 (SSO\_USERNAME) および RH-SSO レalmの管理者のパスワード (SSO\_PASSWORD)**: Red Hat Decision Manager の RH-SSO レalmの管理者ユーザーに指定するユーザー名とパスワード
  - **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。
- c. LDAP を設定するには、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、「[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。

5. 使用している方法に応じて、環境の作成を終了します。

- 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** のポップアップメッセージが表示される可能性があります。このメッセージが表示された場合は、**Create Anyway** をクリックします。
- 完了し、コマンドラインを実行します。

### 3.5. 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
```

2. ファイルから OpenShift 設定マップを作成します。次のコマンドを実行します。

```
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
```

- 
- 3. 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。この環境では、次のデプロイメント設定が影響を受ける可能性があります。
  - **myapp-rhdmcentr**: Decision Central
  - **myapp-kieserver**: Decision Server

**myapp** はアプリケーション名です。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 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[の Software Downloads ページ](#)から、製品の配信可能ファイル `rhdm-7.2.0-openshift-templates.zip` をダウンロードして展開します。

- **rhdm72-authoring.yaml** は、Decision Central と、Decision Central に接続された Decision Server を提供します。この環境を使用して、サービスや他のビジネスアセットをオーサリングしたり、ステージングまたは実稼働環境でこれらのサービスを実行できます。このテンプレートの詳細は、「[rhdm72-authoring.yaml template](#)」を参照してください。
- **rhdm72-authoring-ha.yaml** は、高可用性の Decision Central と、Decision Central に接続された Decision Server を提供します。この環境を使用して、サービスや他のビジネスアセットをオーサリングしたり、ステージングまたは実稼働環境でこれらのサービスを実行できます。高可用性の機能は、テクノロジープレビューとなります。このテンプレートの詳細は、「[rhdm72-authoring-ha.yaml template](#)」を参照してください。
- **rhdm72-kieserver.yaml** は Decision Server を設定します。Decision Server を Decision Central に接続するように設定できます。この方法で、Decision Central が複数の異なる Decision Server を管理するステージングまたは実稼働環境を設定できます。このテンプレートの詳細は、「[rhdm72-kieserver.yaml template](#)」を参照してください。

### 4.1. RHDM72-AUTHORING.YAML TEMPLATE

Red Hat Decision Manager 7.2 の HA 以外の永続オーサリング環境向けのアプリケーションテンプレート

#### 4.1.1. 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
<b>APPLICATION_NAME</b>	–	アプリケーションの名前。	myapp	True
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE 管理者のパスワード	–	False



変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_CONTROLLER_USER</b>	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティーを設定します)	controllerUser	False
<b>KIE_SERVER_CONTROLLER_PWD</b>	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティーを設定します)	–	False
<b>KIE_SERVER_CONTROLLER_TOKEN</b>	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティーを設定します)	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティーを設定します)	executionUser	False
<b>KIE_SERVER_PWD</b>	<b>KIE_SERVER_PWD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティーを設定します)	–	False
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	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)	false	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	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ーを設定)	true	False
<b>DECISION_CENTRAL_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	http サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr- <project>.<default-domain-suffix>)。	–	False
<b>DECISION_CENTRAL_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします。例: secure- <application-name>-rhdmcentr- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	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: <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
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします (例: secure- <application-name>-kieserver- <project>.<default-domain-suffix>)。	–	False
<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	True の場合、secure-APPLICATION_NAME-kieserver vs APPLICATION_NAME-kieserver をルート名として使用します。	false	False
<b>DECISION_CENTRAL_HTTPS_SECRET</b>	–	キーストアファイルを含むシークレット名	decisioncentral-app-secret	True
<b>DECISION_CENTRAL_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	keystore.jks	False
<b>DECISION_CENTRAL_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False
<b>DECISION_CENTRAL_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	mykeystorepass	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	キーストアファイルを含むシークレット名	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	keystore.jks	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	mykeystorepass	False
<b>IMAGE_STREAM_NAMESPACE</b>	–	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
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	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 "rhdm72-kieserver-openshift" です。	rhdm72-kieserver-openshift	True
<b>IMAGE_STREAM_TAG</b>	–	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 1.1 です。	1.1	True
<b>MAVEN_REPO_ID</b>	<b>MAVEN_REPO_ID</b>	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

変数名	イメージの環境変数	説明	値の例	必須
<b>MAVEN_REPO_URL</b>	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<a href="http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/">http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/</a>	False
<b>MAVEN_REPO_USERNAME</b>	<b>MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	–	False
<b>DECISION_CENTRAL_MAVEN_USERNAME</b>	<b>KIE_MAVEN_USER</b>	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	True
<b>DECISION_CENTRAL_MAVEN_PASSWORD</b>	<b>KIE_MAVEN_PASSWORD</b>	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	–	True
<b>GIT_HOOKS_DIR</b>	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリー (必要な場合)。	<b>/opt/eap/standalone/data/kie/git/hooks</b>	False
<b>DECISION_CENTRAL_VOLUME_CAPACITY</b>	–	Decision Central のランタイムデータに向けた永続ストレージのサイズ。	1Gi	True
<b>DECISION_CENTRAL_MEMORY_LIMIT</b>	–	Decision Central コンテナのメモリー制限	2 Gi	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	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
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL	<a href="https://rh-ss0.example.com/auth">https://rh-ss0.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO レルム名。	–	False
<b>DECISION_CENTRAL_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	–	False
<b>DECISION_CENTRAL_SSO_SECRET</b>	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	–	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	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
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	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
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	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
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント	ldap://myldap.example.com	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN。	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報。	パスワード	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	—	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	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
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	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
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。	<b>SUBTREE_SCOPE</b>	False
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	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
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	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
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	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



変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	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
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	<code>memberOf</code>	False
<b>AUTH_LDAP_ROLE_CONTEXT_DN</b>	<b>AUTH_LDAP_ROLE_CONTEXT_DN</b>	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
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	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
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	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
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール	guest	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	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
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	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
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	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
<b>AUTH_LDAP_REFERRAL_USE_ROLE_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_ROLE_ATTRIBUTE_ID_TO_CHECK</b>	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
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	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。	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	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

## 4.1.2. 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。

### 4.1.2.1. 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
<b>\${APPLICATION_NAME}-rhdmcenr</b>	8080	http	Decision Central のすべての Web サーバーのポート。
	8443	https	

サービス	ポート	名前	説明
	8001	git-ssh	
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	

#### 4.1.2.2. 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	Hostname
<b>\${APPLICATION_NAME}-rhdmcenr-http</b>	none	<b>\${DECISION_CENTRAL_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-rhdmcenr-https</b>	TLS パススルー	<b>\${DECISION_CENTRAL_HOSTNAME_HTTPS}</b>
<b>\${APPLICATION_NAME}-kieserver-http</b>	なし	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS パススルー	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

#### 4.1.2.3. 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。

##### 4.1.2.3.1. 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
<b>\${APPLICATION_NAME}-rhdmcenr</b>	ImageChange
<b>\${APPLICATION_NAME}-kieserver</b>	ImageChange

##### 4.1.2.3.2. 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}-rhdmcentr</code>	1
<code>\${APPLICATION_NAME}-kieserver</code>	1

#### 4.1.2.3.3. Pod テンプレート

##### 4.1.2.3.3.1. 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}-rhdmcentr</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>

##### 4.1.2.3.3.2. イメージ

デプロイメント	イメージ
<code>\${APPLICATION_NAME}-rhdmcentr</code>	rhdm72-decisioncentral-openshift
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${KIE_SERVER_IMAGE_STREAM_NAME}</code>

##### 4.1.2.3.3.3. Readiness Probe

`${APPLICATION_NAME}-rhdmcentr`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/kie-drools-wb.jsp
```

`${APPLICATION_NAME}-kieserver`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/services/rest/server/readycheck
```

##### 4.1.2.3.3.4. Liveness Probe

`${APPLICATION_NAME}-rhdmcentr`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/kie-drools-wb.jsp
```

#### **\${APPLICATION\_NAME}-kieserver**

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/services/rest/server/readycheck
```

#### 4.1.2.3.3.5. 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
<b>\${APPLICATION_NAME}-rhdmcentr</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	git-ssh	8001	<b>TCP</b>
<b>\${APPLICATION_NAME}-kieserver</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>

#### 4.1.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
<b>\${APPLICATION_NAME}-rhdmcentr</b>	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	<b>\${KIE_ADMIN_USER}</b>
	<b>KIE_ADMIN_PWD</b>	KIE 管理者のパスワード	<b>\${KIE_ADMIN_PWD}</b>
	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	<b>\${KIE_MBEANS}</b>
	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティーを設定します)	<b>\${KIE_SERVER_CONTROLLER_USER}</b>



デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティを設定します)	<b>\${KIE_SERVER_CONTROLLER_PWD}</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティを設定します)	<b>\${KIE_SERVER_CONTROLLER_TOKEN}</b>
	<b>KIE_SERVER_USER</b>	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)	<b>\${KIE_SERVER_USER}</b>
	<b>KIE_SERVER_PWD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティを設定します)	<b>\${KIE_SERVER_PWD}</b>
	<b>WORKBENCH_ROUTE_NAME</b>	–	<b>\${APPLICATION_NAME}-rhdmcenr</b>
	<b>MAVEN_REPO_ID</b>	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せん。	<b>\${MAVEN_REPO_ID}</b>
	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<b>\${MAVEN_REPO_URL}</b>
	<b>MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)	<b>\${MAVEN_REPO_USERNAME}</b>
	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	<b>\${MAVEN_REPO_PASSWORD}</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_MAVEN_USER</b>	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	<b>`\${DECISION_CENTRAL_MAVEN_USERNAME}`</b>
	<b>KIE_MAVEN_PWD</b>	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	<b>`\${DECISION_CENTRAL_MAVEN_PASSWORD}`</b>
	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリー (必要な場合)。	<b>`\${GIT_HOOKS_DIR}`</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/decisioncentral-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	<b>`\${DECISION_CENTRAL_HTTPS_KEYSTORE}`</b>
	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	<b>`\${DECISION_CENTRAL_HTTPS_NAME}`</b>
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	<b>`\${DECISION_CENTRAL_HTTPS_PASSWORD}`</b>
	<b>SSO_URL</b>	RH-SSO URL	<b>`\${SSO_URL}`</b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レルム名。	<b>`\${SSO_REALM}`</b>
	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット	<b>`\${DECISION_CENTRAL_SSO_SECRET}`</b>
	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	<b>`\${DECISION_CENTRAL_SSO_CLIENT}`</b>

デプロイメント	変数名	説明	値の例
	<b>SSO_USERNAME</b>	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)	<b>\${SSO_USERNAME}</b>
	<b>SSO_PASSWORD</b>	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。	<b>\${SSO_PASSWORD}</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性	<b>\${SSO_PRINCIPAL_ATTRIBUTE}</b>
	<b>HOSTNAME_HTTP</b>	http サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr-<project>.<default-domain-suffix>)。	<b>\${DECISION_CENTRAL_HOSTNAME_HTTP}</b>
	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします。例: secure-<application-name>-rhdmcentr-<project>.<default-domain-suffix>	<b>\${DECISION_CENTRAL_HOSTNAME_HTTPS}</b>
	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント	<b>\${AUTH_LDAP_URL}</b>
	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN。	<b>\${AUTH_LDAP_BIND_DN}</b>
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報。	<b>\${AUTH_LDAP_BIND_CREDENTIAL}</b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	<b>\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_BASE_CTX_DN</b>	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	<b>`\${AUTH_LDAP_BASE_CTX_DN}`</b>
	<b>AUTH_LDAP_BASE_FILTER</b>	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。	<b>`\${AUTH_LDAP_BASE_FILTER}`</b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。	<b>`\${AUTH_LDAP_SEARCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	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)。	<b>`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`</b>
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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slash 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。	<b>`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_PARSE_USERNAME</b>	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。	<b>`\${AUTH_LDAP_PARSE_USERNAME}`</b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	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。	<b>`\${AUTH_LDAP_USERNAME_BEGIN_STRING}`</b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	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。	<b>`\${AUTH_LDAP_USERNAME_END_STRING}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	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。	<b>`\${AUTH_LDAP_ROLE_S_CTX_DN}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_ROLE_FILTER</b>	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。	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	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。	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	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。	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	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。	<b>\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	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。	<b>\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}</b>
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	リファラール (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。リファラールを使用し、ロールオブジェクトがリファラール内部にあると、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ラールツリーに保存できません。	<b>\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	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。	<b>`\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}`</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	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。	<b>`\${AUTH_ROLE_MAPPER_REPLACE_ROLE}`</b>
<b>`\${APPLICATION_NAME}`-kieserver</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	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)	<b>`\${DROOLS_SERVER_FILTER_CLASSES}`</b>
	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	<b>`\${KIE_ADMIN_USER}`</b>
	<b>KIE_ADMIN_PWD</b>	KIE 管理者のパスワード	<b>`\${KIE_ADMIN_PWD}`</b>
	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティ kie.mbeans および kie.scanner.mbeans を設定)。	<b>`\${KIE_MBEANS}`</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	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)	<b>`\${KIE_SERVER_BYPASS_AUTH_USER}`</b>



デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティを設定します)	<b>`\${KIE_SERVER_CONTROLLER_USER}`</b>
	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティを設定します)	<b>`\${KIE_SERVER_CONTROLLER_PWD}`</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティを設定します)	<b>`\${KIE_SERVER_CONTROLLER_TOKEN}`</b>
	<b>KIE_SERVER_CONTROLLER_SERVICE</b>	–	<b>`\${APPLICATION_NAME}-rhdmcenr</b>
	<b>KIE_SERVER_CONTROLLER_PROTOCOL</b>	–	ws
	<b>KIE_SERVER_ID</b>	–	<b>`\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_ROUTE_NAME</b>	–	<b>`\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	True の場合、secure-APPLICATION_NAME-kieserver vs APPLICATION_NAME-kieserver をルート名として使用します。	<b>`\${KIE_SERVER_USE_SECURE_ROUTE_NAME}`</b>
	<b>KIE_SERVER_USER</b>	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)	<b>`\${KIE_SERVER_USER}`</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_PWD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティを設定します)	<b>\${KIE_SERVER_PWD}</b>
	<b>MAVEN_REPOS</b>	–	RHDMCENTR,EXTERNAL
	<b>RHDMCENTR_MAVEN_REPO_SERVICE</b>	–	<b>\${APPLICATION_NAME}-rhdmcen</b>
	<b>RHDMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>
	<b>RHDMCENTR_MAVEN_REPO_USERNAME</b>	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	<b>\${DECISION_CENTRAL_MAVEN_USERNAME}</b>
	<b>RHDMCENTR_MAVEN_REPO_PASSWORD</b>	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	<b>\${DECISION_CENTRAL_MAVEN_PASSWORD}</b>
	<b>EXTERNAL_MAVEN_REPO_ID</b>	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せん。	<b>\${MAVEN_REPO_ID}</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<b>\${MAVEN_REPO_URL}</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)	<b>\${MAVEN_REPO_USERNAME}</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	<b>\${MAVEN_REPO_PASSWORD}</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/kieserver-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	<b>\${KIE_SERVER_HTTPS_KEYSTORE}</b>

デプロイメント	変数名	説明	値の例
	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	<b>`\${KIE_SERVER_HTTPS_NAME}`</b>
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	<b>`\${KIE_SERVER_HTTPS_PASSWORD}`</b>
	<b>SSO_URL</b>	RH-SSO URL	<b>`\${SSO_URL}`</b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レalm名。	<b>`\${SSO_REALM}`</b>
	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット	<b>`\${KIE_SERVER_SSO_SECRET}`</b>
	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	<b>`\${KIE_SERVER_SSO_CLIENT}`</b>
	<b>SSO_USERNAME</b>	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)	<b>`\${SSO_USERNAME}`</b>
	<b>SSO_PASSWORD</b>	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。	<b>`\${SSO_PASSWORD}`</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b>`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性	<b>`\${SSO_PRINCIPAL_ATTRIBUTE}`</b>
	<b>HOSTNAME_HTTP</b>	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: <application-name>-kieserver-<project>.<default-domain-suffix>)。	<b>`\${KIE_SERVER_HOSTNAME_HTTP}`</b>

デプロイメント	変数名	説明	値の例
	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします (例: secure- <application-name>- kieserver-<project>. <default-domain- suffix>)。	<b>`\${KIE_SERVER_HOS TNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_ DN</b>	認証に使用するバインド DN。	<b>`\${AUTH_LDAP_BIND _DN}`</b>
	<b>AUTH_LDAP_BIND_ CREDENTIAL</b>	認証に使用する LDAP の認証情報。	<b>`\${AUTH_LDAP_BIND _CREDENTIAL}`</b>
	<b>AUTH_LDAP_JAAS_ SECURITY_DOMAIN</b>	パスワードの復号に使用 する JaasSecurityDomain の JMX ObjectName。	<b>`\${AUTH_LDAP_JAA S_SECURITY_DOMA IN}`</b>
	<b>AUTH_LDAP_BASE_ CTX_DN</b>	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	<b>`\${AUTH_LDAP_BAS E_CTX_DN}`</b>
	<b>AUTH_LDAP_BASE_ FILTER</b>	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。	<b>`\${AUTH_LDAP_BAS E_FILTER}`</b>
	<b>AUTH_LDAP_SEAR CH_SCOPE</b>	使用する検索範囲。	<b>`\${AUTH_LDAP_SEA RCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEAR CH_TIME_LIMIT</b>	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)。	<b>`\${AUTH_LDAP_SEA RCH_TIME_LIMIT}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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。	<b>`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`</b>
	<b>AUTH_LDAP_PARSE_USERNAME</b>	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。	<b>`\${AUTH_LDAP_PARSE_USERNAME}`</b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	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のみ考慮されます。	<b>`\${AUTH_LDAP_USERNAME_BEGIN_STRING}`</b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	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のみ考慮されます。	<b>`\${AUTH_LDAP_USERNAME_END_STRING}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	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。	<b>`\${AUTH_LDAP_ROLE_S_CTX_DN}`</b>
	<b>AUTH_LDAP_ROLE_FILTER</b>	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。	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	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。	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<p>ロール名を含む roleCtxDN コンテキスト内の属性の名前。</p> <p>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。</p>	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<p>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。</p>	<b>`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<p>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。</p> <p>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。</p>	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	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。	<b><code>\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}</code></b>
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	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 <code>original_role=role1,role2,role3</code> になります。	<b><code>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</code></b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	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。	<b><code>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</code></b>

#### 4.1.2.3.3.7. ボリューム

デプロイメント	名前	mountPath	目的	readOnly
<b><code>\${APPLICATION_NAME}-rhdmcentr</code></b>	decisioncentral-keystore-volume	<b><code>/etc/decisioncentral-secret-volume</code></b>	ssl certs	True



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

#### 4.1.2.4. 外部の依存関係

##### 4.1.2.4.1. ボリューム要求

**PersistentVolume** オブジェクトは、OpenShift クラスターのストレージリソースです。管理者が GCE Persistent Disks、AWS Elastic Block Store (EBS)、NFS マウントなどのソースから **PersistentVolume** オブジェクトを作成して、ストレージをプロビジョニングします。詳細は、[Openshift ドキュメント](#) を参照してください。

名前	アクセスモード
<code>\${APPLICATION_NAME}-rhdmcentr-claim</code>	ReadWriteMany

##### 4.1.2.4.2. 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。

decisioncentral-app-secret kieserver-app-secret

## 4.2. RHDM72-AUTHORING-HA.YAML TEMPLATE

Red Hat Decision Manager 7.2 の HA の永続オーサリング環境向けのアプリケーションテンプレート

### 4.2.1. 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
<b>APPLICATION_NAME</b>	–	アプリケーションの名前。	myapp	True
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE 管理者のパスワード	–	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_CONTROLLER_USER</b>	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティーを設定します)	controllerUser	False
<b>KIE_SERVER_CONTROLLER_PWD</b>	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティーを設定します)	–	False
<b>KIE_SERVER_CONTROLLER_TOKEN</b>	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティーを設定します)	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティーを設定します)	executionUser	False
<b>KIE_SERVER_PWD</b>	<b>KIE_SERVER_PWD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティーを設定します)	–	False
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	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)	false	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	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ーを設定)	true	False
<b>DECISION_CENTRAL_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	http サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr- <project>.<default-domain-suffix>)。	—	False
<b>DECISION_CENTRAL_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします。例: secure- <application-name>-rhdmcentr- <project>.<default-domain-suffix>	—	False
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	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: <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
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします (例: secure- <application-name>-kieserver- <project>.<default-domain-suffix>)。	–	False
<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	True の場合、secure-APPLICATION_NAME-kieserver vs APPLICATION_NAME-kieserver をルート名として使用します。	false	False
<b>DECISION_CENTRAL_HTTPS_SECRET</b>	–	キーストアファイルを含むシークレット名	decisioncentral-app-secret	True
<b>DECISION_CENTRAL_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	keystore.jks	False
<b>DECISION_CENTRAL_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False
<b>DECISION_CENTRAL_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	mykeystorepass	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	キーストアファイルを含むシークレット名	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	mykeystorepass	False
<b>APPFORMER_ELASTIC_RETRIES</b>	<b>APPFORMER_ELASTIC_RETRIES</b>	接続を中止するまでに appformer が elasticsearch ノードに接続試行する回数	–	False
<b>APPFORMER_JMS_BROKER_PORT</b>	<b>APPFORMER_JMS_BROKER_PORT</b>	JMS ブローカーに接続するためのポート。デフォルトは 61616 です。	–	False
<b>APPFORMER_JMS_BROKER_USER</b>	<b>APPFORMER_JMS_BROKER_USER</b>	JMS ブローカーに接続するためのユーザー名	jmsBrokerUser	True
<b>APPFORMER_JMS_BROKER_PASSWORD</b>	<b>APPFORMER_JMS_BROKER_PASSWORD</b>	JMS ブローカーに接続するためのパスワード。	–	True
<b>ES_HOSTNAME_HTTP</b>	–	http サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします。例: <application-name>- rhdindex- <project>.<default-domain-suffix>	–	False
<b>APPFORMER_ELASTIC_CLUSTER_NAME</b>	<b>APPFORMER_ELASTIC_CLUSTER_NAME</b>	ES cluster.name を設定して、Decision Central で設定します。デフォルトは、kie-cluster です。	–	False
<b>ES_NODE_NAME</b>	<b>ES_NODE_NAME</b>	ES node.name プロパティを設定します。デフォルトは HOSTNAME env の値です。	–	False

変数名	イメージの環境変数	説明	値の例	必須
<b>ES_TRANSPORT_HOST</b>	<b>ES_TRANSPORT_HOST</b>	ES transport.host プロパティを設定します。これで、メインの ES クラスターノードのポートアドレスが設定されます。クラスター内のノード間の通信に使用します。デフォルトはコンテナのアドレスです。	–	False
<b>APPFORMER_ELASTIC_PORT</b>	<b>APPFORMER_ELASTIC_PORT</b>	ES http.host プロパティを設定します。これで、メインの ES クラスターノードの http アドレスが設定されます。クラスター内のノード間の通信と、Decision Central との通信に使用します。	–	False
<b>ES_HTTP_HOST</b>	<b>ES_HTTP_HOST</b>	ES http.host プロパティを設定します。これで、メインの ES クラスターノードの http アドレスが設定されます。クラスターの REST API との対話に使用します。デフォルトは、コンテナの IP アドレスです。	–	False

変数名	イメージの環境変数	説明	値の例	必須
<b>ES_HTTP_PORT</b>	<b>ES_HTTP_PORT</b>	ES http.port プロパティを設定します。これで、メインの ES クラスターノードの http ポートが設定されます。クラスター REST API と対話するために使用されます。	–	False
<b>ES_JAVA_OPTS</b>	<b>ES_JAVA_OPTS</b>	カスタムの jvm 設定/プロパティを ES jvm.options 設定ファイルに追加します。	-Xms1024m -Xmx1024m	False
<b>AMQ_IMAGE_STREAM_NAMESPACE</b>	–	AMQ イメージの ImageStream がインストールされる名前空間。デフォルトは openshift です。	openshift	True
<b>AMQ_IMAGE_STREAM_NAME</b>	–	AMQ ブローカーに使用するイメージストリームの名前。デフォルトは "amq-broker72-openshift" です。	amq-broker72-openshift	True
<b>AMQ_IMAGE_STREAM_TAG</b>	–	AMQ イメージストリームのタグ。デフォルトは 1.1 です。	1.1	True
<b>AMQ_ROLE</b>	<b>AMQ_ROLE</b>	標準ブローカーユーザーのユーザーロール。	admin	True
<b>AMQ_NAME</b>	<b>AMQ_NAME</b>	ブローカーの名前	broker	True
<b>AMQ_GLOBAL_MAX_SIZE</b>	<b>AMQ_GLOBAL_MAX_SIZE</b>	メッセージデータが消費するメモリの最大量 (デフォルト: 未定義、システムのメモリの半分)。	100 gb	False

変数名	イメージの環境変数	説明	値の例	必須
<b>ES_VOLUME_CAPACITY</b>	–	Elasticsearch ボリュームの永続ストレージサイズ	1Gi	True
<b>IMAGE_STREAM_NAMESPACE</b>	–	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
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	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 "rhdm72-kieserver-openshift" です。	rhdm72-kieserver-openshift	True
<b>IMAGE_STREAM_TAG</b>	–	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 1.1 です。	1.1	True
<b>MAVEN_REPO_ID</b>	<b>MAVEN_REPO_ID</b>	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



変数名	イメージの環境変数	説明	値の例	必須
<b>MAVEN_REPO_URL</b>	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<a href="http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/">http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/</a>	False
<b>MAVEN_REPO_USERNAME</b>	<b>MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	–	False
<b>DECISION_CENTRAL_MAVEN_USERNAME</b>	<b>KIE_MAVEN_USERNAME</b>	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	True
<b>DECISION_CENTRAL_MAVEN_PASSWORD</b>	<b>KIE_MAVEN_PASSWORD</b>	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	–	True
<b>GIT_HOOKS_DIR</b>	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリー (必要な場合)。	<b>/opt/eap/standalone/data/kie/git/hooks</b>	False
<b>DECISION_CENTRAL_VOLUME_CAPACITY</b>	–	Decision Central のランタイムデータに向けた永続ストレージのサイズ。	1Gi	True
<b>DECISION_CENTRAL_MEMORY_LIMIT</b>	–	Decision Central コンテナのメモリー制限	2 Gi	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	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
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO レalm 名。	–	False
<b>DECISION_CENTRAL_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	–	False
<b>DECISION_CENTRAL_SSO_SECRET</b>	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	–	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	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
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	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
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	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
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント	ldap://myldap.example.com	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN。	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報。	パスワード	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	—	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	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
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	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
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。	<b>SUBTREE_SCOPE</b>	False
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	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
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	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
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	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

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	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
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	<code>memberOf</code>	False
<b>AUTH_LDAP_ROLE_CONTEXT_DN</b>	<b>AUTH_LDAP_ROLE_CONTEXT_DN</b>	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
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	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
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	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
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール	guest	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<p>ロール名を含む roleCtxDN コンテキスト内の属性の名前。</p> <p>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。</p>	name	False
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<p>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。</p>	false	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	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
<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	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
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	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。	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	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

## 4.2.2. 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。

### 4.2.2.1. 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
<b>\${APPLICATION_NAME}-rhdmcentr</b>	8080	http	Decision Central のすべての Web サーバーのポート。
	8443	https	
	8001	git-ssh	

サービス	ポート	名前	説明
<b>\${APPLICATION_NAME}-ping</b>	8888	ping	クラスターリング向けの JGroups ping ポート。
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	
<b>\${APPLICATION_NAME}-rhdminindex</b>	9200	rest	Decision Central がインデックス化する Elasticsearch ポートすべて
	9300	transport	
<b>\${APPLICATION_NAME}-amq-tcp</b>	61616	–	ブローカーの OpenWire ポート。

#### 4.2.2.2. 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	Hostname
<b>\${APPLICATION_NAME}-rhdmcenr-http</b>	none	<b>\${DECISION_CENTRAL_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-rhdmcenr-https</b>	TLS パススルー	<b>\${DECISION_CENTRAL_HOSTNAME_HTTPS}</b>
<b>\${APPLICATION_NAME}-kieserver-http</b>	なし	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS パススルー	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>
<b>\${APPLICATION_NAME}-rhdminindex-http</b>	none	<b>\${ES_HOSTNAME_HTTP}</b>

#### 4.2.2.3. 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。

#### 4.2.2.3.1. 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}-rhdmcentr</code>	ImageChange
<code>\${APPLICATION_NAME}-kieserver</code>	ImageChange
<code>\${APPLICATION_NAME}-rhdmindex</code>	ImageChange
<code>\${APPLICATION_NAME}-amq</code>	ImageChange

#### 4.2.2.3.2. 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}-rhdmcentr</code>	2
<code>\${APPLICATION_NAME}-kieserver</code>	2
<code>\${APPLICATION_NAME}-rhdmindex</code>	1
<code>\${APPLICATION_NAME}-amq</code>	1

#### 4.2.2.3.3. Pod テンプレート

##### 4.2.2.3.3.1. 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}-rhdmcentr</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>

##### 4.2.2.3.3.2. イメージ

デプロイメント	イメージ
<code>\${APPLICATION_NAME}-rhdmcentr</code>	rhdm72-decisioncentral-openshift
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${KIE_SERVER_IMAGE_STREAM_NAME}</code>
<code>\${APPLICATION_NAME}-rhdmindex</code>	rhdm72-decisioncentral-indexing-openshift
<code>\${APPLICATION_NAME}-amq</code>	<code>\${AMQ_IMAGE_STREAM_NAME}</code>

#### 4.2.2.3.3.3. Readiness Probe

##### `${APPLICATION_NAME}-rhdmcentr`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/kie-drools-wb.jsp
```

##### `${APPLICATION_NAME}-kieserver`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/services/rest/server/readycheck
```

##### `${APPLICATION_NAME}-rhdmindex`

```
Http Get on http://localhost:9200/_cluster/health
```

##### `${APPLICATION_NAME}-amq`

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

#### 4.2.2.3.3.4. Liveness Probe

##### `${APPLICATION_NAME}-rhdmcentr`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/kie-drools-wb.jsp
```

##### `${APPLICATION_NAME}-kieserver`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/services/rest/server/readycheck
```

#### 4.2.2.3.3.5. 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
<b>\${APPLICATION_NAME}-rhdmcentr</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	ping	8888	<b>TCP</b>
<b>\${APPLICATION_NAME}-kieserver</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
<b>\${APPLICATION_NAME}-rhdmindex</b>	es	9300	<b>TCP</b>
	http	9200	<b>TCP</b>
<b>\${APPLICATION_NAME}-amq</b>	jolokia	8161	<b>TCP</b>
	amqp	5672	<b>TCP</b>
	mqtt	1883	<b>TCP</b>
	stomp	61613	<b>TCP</b>
	artemis	61616	<b>TCP</b>

## 4.2.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
<b>\${APPLICATION_NAME}-rhdmcentr</b>	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	<b>\${KIE_ADMIN_USER}</b>
	<b>KIE_ADMIN_PWD</b>	KIE 管理者のパスワード	<b>\${KIE_ADMIN_PWD}</b>
	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	<b>\${KIE_MBEANS}</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティーを設定します)	<b>`\${KIE_SERVER_CONTROLLER_USER}`</b>
	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティーを設定します)	<b>`\${KIE_SERVER_CONTROLLER_PWD}`</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティーを設定します)	<b>`\${KIE_SERVER_CONTROLLER_TOKEN}`</b>
	<b>KIE_SERVER_USER</b>	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティーを設定します)	<b>`\${KIE_SERVER_USER}`</b>
	<b>KIE_SERVER_PWD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティーを設定します)	<b>`\${KIE_SERVER_PWD}`</b>
	<b>WORKBENCH_ROUTE_NAME</b>	–	<b>`\${APPLICATION_NAME}-rhdmcen</b> <b>tr`</b>
	<b>MAVEN_REPO_ID</b>	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せん。	<b>`\${MAVEN_REPO_ID}`</b>
	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<b>`\${MAVEN_REPO_URL}`</b>
	<b>MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)	<b>`\${MAVEN_REPO_USERNAME}`</b>
	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	<b>`\${MAVEN_REPO_PASSWORD}`</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_MAVEN_USER</b>	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	<b>`\${DECISION_CENTRAL_MAVEN_USERNAME}`</b>
	<b>KIE_MAVEN_PWD</b>	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	<b>`\${DECISION_CENTRAL_MAVEN_PASSWORD}`</b>
	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリー (必要な場合)。	<b>`\${GIT_HOOKS_DIR}`</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/decisioncentral-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	<b>`\${DECISION_CENTRAL_HTTPS_KEYSTORE}`</b>
	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	<b>`\${DECISION_CENTRAL_HTTPS_NAME}`</b>
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	<b>`\${DECISION_CENTRAL_HTTPS_PASSWORD}`</b>
	<b>JGROUPS_PING_PROTOCOL</b>	–	openshift.DNS_PING
	<b>OPENSIFT_DNS_PING_SERVICE_NAME</b>	–	<b>`\${APPLICATION_NAME}-ping`</b>
	<b>OPENSIFT_DNS_PING_SERVICE_PORT</b>	–	8888
	<b>APPFORMER_ELASTIC_PORT</b>	ES http.host プロパティを設定します。これで、メインの ES クラスターノードの http アドレスが設定されます。クラスター内のノード間の通信と、Decision Central との通信に使用します。	<b>`\${APPFORMER_ELASTIC_PORT}`</b>

デプロイメント	変数名	説明	値の例
	<b>APPFORMER_ELASTIC_CLUSTER_NAME</b>	ES cluster.name を設定して、Decision Central で設定します。デフォルトは、kie-cluster です。	<b>\${APPFORMER_ELASTIC_CLUSTER_NAME}</b>
	<b>APPFORMER_ELASTIC_RETRIES</b>	接続を中止するまでに appformer が elasticsearch ノードに接続試行する回数	<b>\${APPFORMER_ELASTIC_RETRIES}</b>
	<b>APPFORMER_ELASTIC_HOST</b>	–	<b>\${APPLICATION_NAME}-rhdmindex</b>
	<b>APPFORMER_JMS_BROKER_ADDRESS</b>	–	<b>\${APPLICATION_NAME}-amq-tcp</b>
	<b>APPFORMER_JMS_BROKER_PORT</b>	JMS ブローカーに接続するためのポート。デフォルトは 61616 です。	<b>\${APPFORMER_JMS_BROKER_PORT}</b>
	<b>APPFORMER_JMS_BROKER_USER</b>	JMS ブローカーに接続するためのユーザー名	<b>\${APPFORMER_JMS_BROKER_USER}</b>
	<b>APPFORMER_JMS_BROKER_PASSWORD</b>	JMS ブローカーに接続するためのパスワード。	<b>\${APPFORMER_JMS_BROKER_PASSWORD}</b>
	<b>SSO_URL</b>	RH-SSO URL	<b>\${SSO_URL}</b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レalm名。	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット	<b>\${DECISION_CENTRAL_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	<b>\${DECISION_CENTRAL_SSO_CLIENT}</b>
	<b>SSO_USERNAME</b>	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)	<b>\${SSO_USERNAME}</b>



デプロイメント	変数名	説明	値の例
	<b>SSO_PASSWORD</b>	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。	<b>`\${SSO_PASSWORD}`</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b>`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性	<b>`\${SSO_PRINCIPAL_ATTRIBUTE}`</b>
	<b>HOSTNAME_HTTP</b>	http サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr-<project>.<default-domain-suffix>)。	<b>`\${DECISION_CENTRAL_HOSTNAME_HTTP}`</b>
	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします。例: secure-<application-name>-rhdmcentr-<project>.<default-domain-suffix>	<b>`\${DECISION_CENTRAL_HOSTNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN。	<b>`\${AUTH_LDAP_BIND_DN}`</b>
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報。	<b>`\${AUTH_LDAP_BIND_CREDENTIAL}`</b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	<b>`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`</b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	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	<b>`\${AUTH_LDAP_BASE_CTX_DN}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_BASE_FILTER</b>	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。	<b>`\${AUTH_LDAP_BASE_FILTER}`</b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。	<b>`\${AUTH_LDAP_SEARCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	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)。	<b>`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`</b>
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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。	<b>`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`</b>
	<b>AUTH_LDAP_PARSE_USERNAME</b>	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。	<b>`\${AUTH_LDAP_PARSE_USERNAME}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_USER NAME_BEGIN_STR ING</b>	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。	<b>`\${AUTH_LDAP_USE RNAME_BEGIN_STR ING}`</b>
	<b>AUTH_LDAP_USER NAME_END_STRIN G</b>	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。	<b>`\${AUTH_LDAP_USE RNAME_END_STRIN G}`</b>
	<b>AUTH_LDAP_ROLE_ ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	<b>`\${AUTH_LDAP_ROL E_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_ROLE S_CTX_DN</b>	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。	<b>`\${AUTH_LDAP_ROL ES_CTX_DN}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_ROLE_FILTER</b>	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。	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	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。	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	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。	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	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。	<b>`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	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。	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`</b>
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	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。	<b>`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	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。	<b>`\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}`</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	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。	<b>`\${AUTH_ROLE_MAPPER_REPLACE_ROLE}`</b>
<b>`\${APPLICATION_NAME}`-kieserver</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	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)	<b>`\${DROOLS_SERVER_FILTER_CLASSES}`</b>
	<b>KIE_ADMIN_PWD</b>	KIE 管理者のパスワード	<b>`\${KIE_ADMIN_PWD}`</b>
	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	<b>`\${KIE_ADMIN_USER}`</b>
	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティ kie.mbeans および kie.scanner.mbeans を設定)。	<b>`\${KIE_MBEANS}`</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	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)	<b>`\${KIE_SERVER_BYPASS_AUTH_USER}`</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティを設定します)	<b>\${KIE_SERVER_CONTROLLER_USER}</b>
	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティを設定します)	<b>\${KIE_SERVER_CONTROLLER_PWD}</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティを設定します)	<b>\${KIE_SERVER_CONTROLLER_TOKEN}</b>
	<b>KIE_SERVER_CONTROLLER_SERVICE</b>	–	<b>\${APPLICATION_NAME}-rhdmcen</b>
	<b>KIE_SERVER_CONTROLLER_PROTOCOL</b>	–	ws
	<b>KIE_SERVER_ID</b>	–	<b>\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_ROUTE_NAME</b>	–	<b>\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	True の場合、secure-APPLICATION_NAME-kieserver vs APPLICATION_NAME-kieserver をルート名として使用します。	<b>\${KIE_SERVER_USE_SECURE_ROUTE_NAME}</b>
	<b>KIE_SERVER_PWD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティを設定します)	<b>\${KIE_SERVER_PWD}</b>
	<b>KIE_SERVER_USER</b>	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)	<b>\${KIE_SERVER_USER}</b>

デプロイメント	変数名	説明	値の例
	<b>MAVEN_REPOS</b>	–	RHDMCENTR,EXTERNAL
	<b>RHDMCENTR_MAVEN_REPO_SERVICE</b>	–	<b>\${APPLICATION_NAME}-rhdmcen</b>
	<b>RHDMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>
	<b>RHDMCENTR_MAVEN_REPO_USERNAME</b>	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	<b>\${DECISION_CENTRAL_MAVEN_USERNAME}</b>
	<b>RHDMCENTR_MAVEN_REPO_PASSWORD</b>	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	<b>\${DECISION_CENTRAL_MAVEN_PASSWORD}</b>
	<b>EXTERNAL_MAVEN_REPO_ID</b>	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せん。	<b>\${MAVEN_REPO_ID}</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<b>\${MAVEN_REPO_URL}</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)	<b>\${MAVEN_REPO_USERNAME}</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	<b>\${MAVEN_REPO_PASSWORD}</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/kieserver-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	<b>\${KIE_SERVER_HTTPS_KEYSTORE}</b>
	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	<b>\${KIE_SERVER_HTTPS_NAME}</b>



デプロイメント	変数名	説明	値の例
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	<b>`\${KIE_SERVER_HTTPS_PASSWORD}`</b>
	<b>SSO_URL</b>	RH-SSO URL	<b>`\${SSO_URL}`</b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レalm名。	<b>`\${SSO_REALM}`</b>
	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット	<b>`\${KIE_SERVER_SSO_SECRET}`</b>
	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	<b>`\${KIE_SERVER_SSO_CLIENT}`</b>
	<b>SSO_USERNAME</b>	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)	<b>`\${SSO_USERNAME}`</b>
	<b>SSO_PASSWORD</b>	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。	<b>`\${SSO_PASSWORD}`</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b>`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性	<b>`\${SSO_PRINCIPAL_ATTRIBUTE}`</b>
	<b>HOSTNAME_HTTP</b>	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: <application-name>-kieserver-<project>.<default-domain-suffix>)。	<b>`\${KIE_SERVER_HOSTNAME_HTTP}`</b>

デプロイメント	変数名	説明	値の例
	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします (例: secure- <application-name>- kieserver-<project>. <default-domain- suffix>)。	<b>`\${KIE_SERVER_HOS TNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_ DN</b>	認証に使用するバインド DN。	<b>`\${AUTH_LDAP_BIND_ DN}`</b>
	<b>AUTH_LDAP_BIND_ CREDENTIAL</b>	認証に使用する LDAP の認証情報。	<b>`\${AUTH_LDAP_BIND_ CREDENTIAL}`</b>
	<b>AUTH_LDAP_JAAS_ SECURITY_DOMAIN</b>	パスワードの復号に使用 する JaasSecurityDomain の JMX ObjectName。	<b>`\${AUTH_LDAP_JAA S_SECURITY_DOMA IN}`</b>
	<b>AUTH_LDAP_BASE_ CTX_DN</b>	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	<b>`\${AUTH_LDAP_BAS E_CTX_DN}`</b>
	<b>AUTH_LDAP_BASE_ FILTER</b>	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。	<b>`\${AUTH_LDAP_BAS E_FILTER}`</b>
	<b>AUTH_LDAP_SEAR CH_SCOPE</b>	使用する検索範囲。	<b>`\${AUTH_LDAP_SEA RCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEAR CH_TIME_LIMIT</b>	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)。	<b>`\${AUTH_LDAP_SEA RCH_TIME_LIMIT}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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。	<b>`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`</b>
	<b>AUTH_LDAP_PARSE_USERNAME</b>	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。	<b>`\${AUTH_LDAP_PARSE_USERNAME}`</b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	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。	<b>`\${AUTH_LDAP_USERNAME_BEGIN_STRING}`</b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	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。	<b>`\${AUTH_LDAP_USERNAME_END_STRING}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	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。	<b>`\${AUTH_LDAP_ROLE_S_CTX_DN}`</b>
	<b>AUTH_LDAP_ROLE_FILTER</b>	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。	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	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。	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	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。	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	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。	<b>\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	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。	<b>\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	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。	<b>`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`</b>
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	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。	<b>`\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}`</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	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。	<b>`\${AUTH_ROLE_MAPPER_REPLACE_ROLE}`</b>
<b>`\${APPLICATION_NAME}`-rhdminindex</b>	<b>ES_CLUSTER_NAME</b>	ES cluster.name を設定して、Decision Central で設定します。デフォルトは、kie-cluster です。	<b>`\${APPFORMER_ELASTIC_CLUSTER_NAME}`</b>

デプロイメント	変数名	説明	値の例
	<b>ES_NODE_NAME</b>	ES node.name プロパティを設定します。デフォルトは HOSTNAME env の値です。	<b>`\${ES_NODE_NAME}`</b>
	<b>ES_TRANSPORT_HOST</b>	ES transport.host プロパティを設定します。これで、メインの ES クラスターノードのトランスポートアドレスが設定されます。クラスター内のノード間の通信に使用します。デフォルトはコンテナのアドレスです。	<b>`\${ES_TRANSPORT_HOST}`</b>
	<b>ES_TRANSPORT_TCP_PORT</b>	ES http.host プロパティを設定します。これで、メインの ES クラスターノードの http アドレスが設定されます。クラスター内のノード間の通信と、Decision Central との通信に使用します。	<b>`\${APPFORMER_ELASTIC_PORT}`</b>
	<b>ES_HTTP_PORT</b>	ES http.port プロパティを設定します。これで、メインの ES クラスターノードの http ポートが設定されます。クラスター REST API と対話するために使用されます。	<b>`\${ES_HTTP_PORT}`</b>
	<b>ES_HTTP_HOST</b>	ES http.host プロパティを設定します。これで、メインの ES クラスターノードの http アドレスが設定されます。クラスターの REST API との対話に使用します。デフォルトは、コンテナの IP アドレスです。	<b>`\${ES_HTTP_HOST}`</b>
	<b>ES_JAVA_OPTS</b>	カスタムの jvm 設定/プロパティを ES jvm.options 設定ファイルに追加します。	<b>`\${ES_JAVA_OPTS}`</b>

デプロイメント	変数名	説明	値の例
<b>\${APPLICATION_NAME}-amq</b>	<b>AMQ_USER</b>	JMS ブローカーに接続するためのユーザー名	<b>\${APPFORMER_JMS_BROKER_USER}</b>
	<b>AMQ_PASSWORD</b>	JMS ブローカーに接続するためのパスワード。	<b>\${APPFORMER_JMS_BROKER_PASSWORD}</b>
	<b>AMQ_ROLE</b>	標準ブローカーユーザーのユーザーロール。	<b>\${AMQ_ROLE}</b>
	<b>AMQ_NAME</b>	ブローカーの名前	<b>\${AMQ_NAME}</b>
	<b>AMQ_TRANSPORTS</b>	–	openwire
	<b>AMQ_GLOBAL_MAX_SIZE</b>	メッセージデータが消費するメモリの最大量 (デフォルト: 未定義、システムのメモリの半分)。	<b>\${AMQ_GLOBAL_MAX_SIZE}</b>

#### 4.2.2.3.3.7. ボリューム

デプロイメント	名前	mountPath	目的	readOnly
<b>\${APPLICATION_NAME}-rhdmcentr</b>	decisioncentral-keystore-volume	<b>/etc/decisioncentral-secret-volume</b>	ssl certs	True
<b>\${APPLICATION_NAME}-kieserver</b>	kieserver-keystore-volume	<b>/etc/kieserver-secret-volume</b>	ssl certs	True
<b>\${APPLICATION_NAME}-rhdmindex</b>	<b>\${APPLICATION_NAME}-rhdmindex-pvol</b>	<b>/opt/elasticsearch/data</b>	rhdmindex	false

#### 4.2.2.4. 外部の依存関係

##### 4.2.2.4.1. ボリューム要求

**PersistentVolume** オブジェクトは、OpenShift クラスターのストレージリソースです。管理者が GCE Persistent Disks、AWS Elastic Block Store (EBS)、NFS マウントなどのソースから **PersistentVolume** オブジェクトを作成して、ストレージをプロビジョニングします。詳細は、[Openshift ドキュメント](#) を参照してください。



名前	アクセスモード
<code>\${APPLICATION_NAME}-rhdmcentr-claim</code>	ReadWriteMany
<code>\${APPLICATION_NAME}-rhdmindex-claim</code>	ReadWriteOnce

#### 4.2.2.4.2. 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。

```
decisioncentral-app-secret kieserver-app-secret
```

#### 4.2.2.4.3. クラスターリング

OpenShift EAP では、Kubernetes または DNS の検出メカニズム 2 つの内 1 つを使用してクラスターリングを実現できます。これには、`standalone-openshift.xml` で `<openshift.KUBE_PING/>` 要素または `<openshift.DNS_PING/>` 要素のいずれかを指定して JGroups プロトコルスタックを設定します。テンプレートは、`DNS_PING` を使用するように設定しますが、イメージで使用するデフォルトは ``KUBE_PING`` となっています。

使用される検出メカニズムは、`JGROUPS_PING_PROTOCOL` 環境変数によって指定されます。これは `openshift.DNS_PING` または `openshift.KUBE_PING` のいずれかに設定できます。`OpenShift.KUBE_PING` は、`JGROUPS_PING_PROTOCOL` に値が指定されていない場合は、イメージによって使用されるデフォルトです。

`DNS_PING` を機能させるには、以下の手順を実行する必要があります。

1. `OPENSIFT_DNS_PING_SERVICE_NAME` 環境変数は、クラスターの ping サービス名に設定する必要があります (上記の表を参照)。設定していない場合には、サーバーは単一ノードのクラスター (ノードが 1 つのクラスター) のように機能します。
2. `OPENSIFT_DNS_PING_SERVICE_PORT` 環境変数は、ping サービスを公開するポート番号に設定する必要があります (上記の表を参照)。`DNS_PING` プロトコルは可能な場合には SRV レコードからのポートを識別しようとします。デフォルト値は 8888 です。
3. ping ポートを公開する ping サービスは定義する必要があります。このサービスはヘッドレス (ClusterIP=None) で、以下の条件を満たす必要があります。
  - a. ポートは、ポート検出が機能するように、名前を指定する必要があります。
  - b. `service.alpha.kubernetes.io/tolerate-unready-endpoints` を `"true"` に指定してアノテーションを設定する必要があります。このアノテーションを省略すると、起動時にノードごとに独自の単一ノードのクラスターが形成され、(起動後でない)他のノードが検出されない (ので) 起動後にこのクラスターが他のノードのクラスターにマージされます。

#### DNS\_PING で使用する ping サービスの例

```
kind: Service
apiVersion: v1
spec:
  clusterIP: None
  ports:
```

```

- name: ping
  port: 8888
  selector:
    deploymentConfig: eap-app
metadata:
  name: eap-app-ping
  annotations:
    service.alpha.kubernetes.io/tolerate-unready-endpoints: "true"
    description: "The JGroups ping port for clustering."

```

**KUBE\_PING** を機能させるには以下の手順を実行する必要があります。

1. **OPENSIFT\_KUBE\_PING\_NAMESPACE** 環境変数を設定する必要があります (上記の表を参照)。設定していない場合には、サーバーは単一ノードのクラスター (ノードが1つのクラスター) のように機能します。
2. **OPENSIFT\_KUBE\_PING\_LABELS** 環境変数を設定する必要があります (上記の表を参照)。設定されていない場合には、アプリケーション外の Pod (namespace に関係なく) が参加しようとしています。
3. Kubernetes の REST API にアクセスできるようにするには、Pod が実行されているサービスアカウントに対して承認を行う必要があります。これはコマンドラインで行います。

#### 例4.1 policy コマンド

myproject の namespace におけるデフォルトのサービスアカウントの使用:

```
oc policy add-role-to-user view system:serviceaccount:myproject:default -n myproject
```

myproject の namespace における eap-service-account の使用:

```
oc policy add-role-to-user view system:serviceaccount:myproject:eap-service-account -n myproject
```

## 4.3. RHDM72-KIESERVER.YAML TEMPLATE

Red Hat Decision Manager 7.2 での管理対象 KIE サーバー向けのアプリケーションテンプレート

### 4.3.1. 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
<b>APPLICATION_NAME</b>	-	アプリケーションの名前。	myapp	True

変数名	イメージの環境変数	説明	値の例	必須
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	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
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<a href="http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/">http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/</a>	True
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	–	False
<b>DECISION_CENTRAL_MAVEN_SERVICE</b>	<b>RHDMCENTRAL_MAVEN_REPO_SERVICE</b>	必要な場合にはオプションの Decision Central (maven リポジトリの使用向け) で使用する OpenShift サービス名	myapp-rhdmcentr	False
<b>DECISION_CENTRAL_MAVEN_USERNAME</b>	<b>RHDMCENTRAL_MAVEN_REPO_USERNAME</b>	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
<b>DECISION_CENTRAL_MAVEN_PASSWORD</b>	<b>RHDMCENTRAL_MAVEN_REPO_PASSWORD</b>	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
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	adminUser	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_ADMIN_PWD</b>	<b>KIE_ADMIN_PWD</b>	KIE 管理者のパスワード	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	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
<b>KIE_SERVER_PASSWORD</b>	<b>KIE_SERVER_PASSWORD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティを設定します)	–	False
<b>IMAGE_STREAM_NAMESPACE</b>	–	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
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	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 "rhdm72-kieserver-openshift" です。	rhdm72-kieserver-openshift	True

変数名	イメージの環境変数	説明	値の例	必須
<b>IMAGE_STREAM_TAG</b>	–	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 1.1 です。	1.1	True
<b>KIE_SERVER_CONTROLLER_USER</b>	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティーを設定します)	controllerUser	False
<b>KIE_SERVER_CONTROLLER_PWD</b>	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティーを設定します)	–	False
<b>KIE_SERVER_CONTROLLER_TOKEN</b>	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティーを設定します)	–	False
<b>KIE_SERVER_CONTROLLER_SERVICE</b>	<b>KIE_SERVER_CONTROLLER_SERVICE</b>	オプションのスタンドアロンコントローラーのサービス名。アプリケーションは、このサービス名を使用してコントローラーに登録します。(設定されている場合は、ホストとポートの検出に使用されます)	–	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_CONTROLLER_HOST</b>	<b>KIE_SERVER_CONTROLLER_HOST</b>	KIE サーバーコントローラーのホスト (org.kie.server.controller システムプロパティーの設定に使用)	my-app-controller-ocpuser.os.example.com	False
<b>KIE_SERVER_CONTROLLER_PORT</b>	<b>KIE_SERVER_CONTROLLER_PORT</b>	KIE サーバーコントローラーのポート (org.kie.server.controller システムプロパティーの設定に使用)	8080	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	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ーを設定)	true	False
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	enabled	False
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	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: <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
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします (例: secure- <application-name>-kieserver- <project>.<default-domain-suffix>)。	–	False
<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	True の場合、secure-APPLICATION_NAME-kieserver vs APPLICATION_NAME-kieserver をルート名として使用します。	false	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	キーストアファイルを含むシークレット名	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	mykeystorepass	False
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	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
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	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
<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	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-library=org.openshift.quickstarts:rhdm-kieserver-library:1.4.0-SNAPSHOT	False
<b>KIE_SERVER_MGMT_DISABLED</b>	<b>KIE_SERVER_MGMT_DISABLED</b>	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	False
<b>KIE_SERVER_STARTUP_STRATEGY</b>	<b>KIE_SERVER_STARTUP_STRATEGY</b>	LocalContainersStartupStrategy に設定した場合には、コントローラーが設定されていて利用できないときでも KIE サーバーが起動し、ローカルの設定で機能できます。	LocalContainersStartupStrategy	False
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO レalm 名。	–	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	–	False



変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	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
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	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
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	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
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN。	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報。	パスワード	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	–	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	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

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	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
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。	<b>SUBTREE_SCOPE</b>	False
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	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
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	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
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	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
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	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
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	memberOf	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_ROLE_SCTX_DN</b>	<b>AUTH_LDAP_ROLE_SCTX_DN</b>	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
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	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
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	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
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール	guest	False
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	ロール名を含む roleCtxDN コンテキスト内の属性の名前。 roleAttributelsDN プロパティーを true に設定すると、このプロパティー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
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	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
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	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
<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	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
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	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。	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	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

### 4.3.2. 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。

#### 4.3.2.1. 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
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	
<b>\${APPLICATION_NAME}-kieserver-ping</b>	8888	ping	クラスターリング向けの JGroups ping ポート。

#### 4.3.2.2. 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
<code>\${APPLICATION_NAME}-kieserver-http</code>	なし	<code>\${KIE_SERVER_HOSTNAME_HTTP}</code>
<code>\${APPLICATION_NAME}-kieserver-https</code>	TLS パススルー	<code>\${KIE_SERVER_HOSTNAME_HTTPS}</code>

#### 4.3.2.3. 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。

##### 4.3.2.3.1. 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

##### 4.3.2.3.2. 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>	1

##### 4.3.2.3.3. Pod テンプレート

###### 4.3.2.3.3.1. 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>

## 4.3.2.3.3.2. イメージ

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

## 4.3.2.3.3.3. Readiness Probe

`${APPLICATION_NAME}-kieserver`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/services/rest/server/readycheck
```

## 4.3.2.3.3.4. Liveness Probe

`${APPLICATION_NAME}-kieserver`

```
/bin/bash -c curl --fail --silent -u '${KIE_ADMIN_USER}:${KIE_ADMIN_PWD}'
http://localhost:8080/services/rest/server/readycheck
```

## 4.3.2.3.3.5. 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
	ping	8888	TCP

## 4.3.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
<code>\${APPLICATION_NAME}-kieserver</code>	<code>DROOLS_SERVER_FILTER_CLASSES</code>	KIE Server のクラスフィルタ (org.drools.server.filter.classes システムプロパティを設定)	<code>\${DROOLS_SERVER_FILTER_CLASSES}</code>

デプロイメント	変数名	説明	値の例
	<b>KIE_ADMIN_USER</b>	KIE 管理者のユーザー名	<b>`\${KIE_ADMIN_USER}`</b>
	<b>KIE_ADMIN_PWD</b>	KIE 管理者のパスワード	<b>`\${KIE_ADMIN_PWD}`</b>
	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	<b>`\${KIE_MBEANS}`</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	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)	<b>`\${KIE_SERVER_BYPASS_AUTH_USER}`</b>
	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE サーバーのコントローラーのユーザー名 (org.kie.server.controller.user システムプロパティーを設定します)	<b>`\${KIE_SERVER_CONTROLLER_USER}`</b>
	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE サーバーのコントローラーのパスワード (org.kie.server.controller.pwd システムプロパティーを設定します)	<b>`\${KIE_SERVER_CONTROLLER_PWD}`</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	Bearer 認証用の KIE サーバーコントローラーのトークン (org.kie.server.controller.token システムプロパティーを設定します)	<b>`\${KIE_SERVER_CONTROLLER_TOKEN}`</b>
	<b>KIE_SERVER_CONTROLLER_SERVICE</b>	オプションのスタンドアロンコントローラーのサービス名。アプリケーションは、このサービス名を使用してコントローラーに登録します。(設定されている場合は、ホストとポートの検出に使用されます)	<b>`\${KIE_SERVER_CONTROLLER_SERVICE}`</b>
	<b>KIE_SERVER_CONTROLLER_PROTOCOL</b>	–	ws

デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_CONTROLLER_HOST</b>	KIE サーバーコントローラーのホスト (org.kie.server.controller システムプロパティの設定に使用)	<b>\${KIE_SERVER_CONTROLLER_HOST}</b>
	<b>KIE_SERVER_CONTROLLER_PORT</b>	KIE サーバーコントローラーのポート (org.kie.server.controller システムプロパティの設定に使用)	<b>\${KIE_SERVER_CONTROLLER_PORT}</b>
	<b>KIE_SERVER_ID</b>	–	<b>\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_ROUTE_NAME</b>	–	<b>\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_USE_SECURE_ROUTE_NAME</b>	True の場合、secure-APPLICATION_NAME-kieserver vs APPLICATION_NAME-kieserver をルート名として使用します。	<b>\${KIE_SERVER_USE_SECURE_ROUTE_NAME}</b>
	<b>KIE_SERVER_USER</b>	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)	<b>\${KIE_SERVER_USER}</b>
	<b>KIE_SERVER_PWD</b>	KIE サーバーパスワード (org.kie.server.pwd システムプロパティを設定します)	<b>\${KIE_SERVER_PWD}</b>
	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	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
	<b>\${KIE_SERVER_CONTAINER_DEPLOYMENT}</b>	<b>MAVEN_REPOS</b>	–

デプロイメント	変数名	説明	値の例
	RHDMCENTR,EXTERNAL	<b>RHDMCENTR_MAVEN_REPO_SERVICE</b>	必要な場合にはオプションの Decision Central (maven リポジトリの使用向け) で使用する OpenShift サービス名
	<b>\${DECISION_CENTRAL_MAVEN_SERVICE}</b>	<b>RHDMCENTR_MAVEN_REPO_PATH</b>	–
	<b>/maven2/</b>	<b>RHDMCENTR_MAVEN_REPO_USERNAME</b>	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
	<b>\${DECISION_CENTRAL_MAVEN_USERNAME}</b>	<b>RHDMCENTR_MAVEN_REPO_PASSWORD</b>	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
	<b>\${DECISION_CENTRAL_MAVEN_PASSWORD}</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	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。
	<b>\${MAVEN_REPO_ID}</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。
	<b>\${MAVEN_REPO_URL}</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするユーザー名 (必要な場合)
	<b>\${MAVEN_REPO_USERNAME}</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。

デプロイメント	変数名	説明	値の例
	<code>\${MAVEN_REPO_PASSWORD}</code>	<code>KIE_SERVER_MGMT_DISABLED</code>	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。
	<code>\${KIE_SERVER_MGMT_DISABLED}</code>	<code>KIE_SERVER_STARTUP_STRATEGY</code>	LocalContainersStartupStrategy に設定した場合には、コントローラーが設定されていて利用できないときでも KIE サーバーが起動し、ローカルの設定で機能できます。
	<code>\${KIE_SERVER_STARTUP_STRATEGY}</code>	<code>HTTPS_KEYSTORE_DIR</code>	—
	<code>/etc/kieserver-secret-volume</code>	<code>HTTPS_KEYSTORE</code>	シークレット内のキーストアファイルの名前。
	<code>\${KIE_SERVER_HTTPS_KEYSTORE}</code>	<code>HTTPS_NAME</code>	サーバー証明書に関連付けられている名前
	<code>\${KIE_SERVER_HTTPS_NAME}</code>	<code>HTTPS_PASSWORD</code>	キーストアおよび証明書のパスワード
	<code>\${KIE_SERVER_HTTPS_PASSWORD}</code>	<code>JGROUPS_PING_PROTOCOL</code>	—
	<code>openshift.DNS_PING</code>	<code>OPENSIFT_DNS_PING_SERVICE_NAME</code>	—
	<code>\${APPLICATION_NAME}-kieserver-ping</code>	<code>OPENSIFT_DNS_PING_SERVICE_PORT</code>	—
	8888	<code>SSO_URL</code>	RH-SSO URL
	<code>\${SSO_URL}</code>	<code>SSO_OPENIDCONNECT_DEPLOYMENTS</code>	—

デプロイメント	変数名	説明	値の例
	ROOT.war	<b>SSO_REALM</b>	RH-SSO レルム名。
	<b>\${SSO_REALM}</b>	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット
	<b>\${KIE_SERVER_SSO_SECRET}</b>	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。
	<b>\${KIE_SERVER_SSO_CLIENT}</b>	<b>SSO_USERNAME</b>	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)
	<b>\${SSO_USERNAME}</b>	<b>SSO_PASSWORD</b>	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。
	<b>\${SSO_PASSWORD}</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。
	<b>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性
	<b>\${SSO_PRINCIPAL_ATTRIBUTE}</b>	<b>HOSTNAME_HTTP</b>	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: <application-name>-kieserver-<project>.<default-domain-suffix>)。
	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合には空白にします (例: secure-<application-name>-kieserver-<project>.<default-domain-suffix>)。
	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント

デプロイメント	変数名	説明	値の例
	<code>\${AUTH_LDAP_URL}</code>	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN。
	<code>\${AUTH_LDAP_BIND_DN}</code>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報。
	<code>\${AUTH_LDAP_BIND_CREDENTIAL}</code>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。
	<code>\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}</code>	<b>AUTH_LDAP_BASE_CTX_DN</b>	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
	<code>\${AUTH_LDAP_BASE_CTX_DN}</code>	<b>AUTH_LDAP_BASE_FILTER</b>	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。検索フィルター一般的な例は (uid={0}) です。
	<code>\${AUTH_LDAP_BASE_FILTER}</code>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。
	<code>\${AUTH_LDAP_SEARCH_SCOPE}</code>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	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)。
	<code>\${AUTH_LDAP_SEARCH_TIME_LIMIT}</code>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	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。

デプロイメント	変数名	説明	値の例
	<code>\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}</code>	<code>AUTH_LDAP_PARSE_USERNAME</code>	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、 <code>usernameBeginString</code> および <code>usernameEndString</code> とともに使用されます。
	<code>\${AUTH_LDAP_PARSE_USERNAME}</code>	<code>AUTH_LDAP_USERNAME_BEGIN_STRING</code>	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 true に設定されている場合にのみ考慮されます。
	<code>\${AUTH_LDAP_USERNAME_BEGIN_STRING}</code>	<code>AUTH_LDAP_USERNAME_END_STRING</code>	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 true に設定されている場合にのみ考慮されます。
	<code>\${AUTH_LDAP_USERNAME_END_STRING}</code>	<code>AUTH_LDAP_ROLE_ATTRIBUTE_ID</code>	ユーザーロールを含む属性の名前。
	<code>\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}</code>	<code>AUTH_LDAP_ROLE_S_CTX_DN</code>	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。



デプロイメント	変数名	説明	値の例
	<b>`\${AUTH_LDAP_ROLE_CTX_DN}`</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	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={}) です。
	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	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。
	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	認証された全ユーザーに対して含まれるロール
	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	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。

デプロイメント	変数名	説明	値の例
	<b><code>\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}</code></b>	<b><code>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</code></b>	クエリーによって返された DN に <code>roleNameAttributeID</code> 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 <code>roleNameAttributeID</code> に対してチェックされません。false に設定すると、DN は <code>roleNameAttributeID</code> 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。
	<b><code>\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}</code></b>	<b><code>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</code></b>	<code>roleAttributeID</code> 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 <code>roleNameAttributeID</code> 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。
	<b><code>\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}</code></b>	<b><code>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</code></b>	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: <code>member</code> ) 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せん。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。

デプロイメント	変数名	説明	値の例
	<code>\${AUTH_LDAP_REFERENCE_USER_ATTRIBUTE_ID_TO_CHECK}</code>	<code>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</code>	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 <code>original_role=role1,role2,role3</code> になります。
	<code>\${AUTH_ROLE_MAPPER_ROLES_REPLACE}</code>	<code>AUTH_ROLE_MAPPER_REPLACE_ROLE</code>	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、置き換えられません。

#### 4.3.2.3.3.7. ボリューム

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

#### 4.3.2.4. 外部の依存関係

##### 4.3.2.4.1. 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

## 4.4. 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、テンプレートリファレンスで **DeploymentConfig** の名前を検索して、以下のコマンドを実行します。

```
$ 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、テンプレートリファレンスで **BuildConfig** の名前を検索して、以下のコマンドを実行します。

```
$ 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 をスケールするには、テンプレートリファレンスで **DeploymentConfig** の名前を検索して、以下のコマンドを実行します。

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

詳細は、[手動スケールリング](#) 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)