Red Hat Decision Manager 7.5

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

Last Updated: 2023-03-08

Red Hat Decision Manager 7.5 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

概要

本書では、Red Hat Decision Manager 7.5 オーサリングまたは管理サーバー環境を Red Hat OpenShift Container Platform にデプロイする方法について説明します。

目次

はじめに 4

第1章 RED HAT OPENSHIFT CONTAINER PLATFORM における RED HAT DECISION MANAGER の概要 5

第2章 OPENSHIFT 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. BUSINESS CENTRAL へのシークレットの作成 9
2.4. オフラインで使用する MAVEN ミラーリポジトリーの用意 9
2.5. GLUSTERFS 設定の変更 10

第3章 オーサリングまたは管理サーバー環境 13
3.1. オーサリング環境のデプロイメント 13
3.1.1. オーサリング環境用のテンプレートの設定開始 13
3.1.2. オーサリング環境に必要なパラメーターの設定 14
3.1.3. オーサリング環境用のイメージストリーム namespace の設定 15
3.1.4. オーサリング環境用のオプションの Maven リポジトリーの設定 16
3.1.5. オーサリング環境のビルドイン Maven リポジトリーにアクセスするための認証情報の指定 16
3.1.6. オーサリング環境の公開インターネットへの接続のない環境に Maven ミラーへのアクセスを設定する 17
3.1.7. オーサリング環境用の Git フックディレクトリーの指定 18
3.1.8. オーサリング環境用の RH-SSO 認証パラメーターの設定 18
3.1.9. オーサリング環境用の LDAP 認証パラメーターの設定 20
3.1.10. オーサリング環境用の Prometheus メトリクス収集の有効化 21
3.1.11. オーサリング環境用テンプレートのデプロイの実行 22
3.2. (オプション) GIT フックディレクトリーの指定 22
3.3. オーサリング環境または管理環境向けの追加の管理 DECISION SERVER のデプロイ 24
3.3.1. 追加の管理 Decision Server テンプレート設定の開始 24
3.3.2. 追加の管理 Decision Server に必要なパラメーターの設定 24
3.3.3. 追加の管理 Decision Server のイメージストリーム namespace の設定 25
3.3.4. 追加の管理 Decision Server 用の Business Central インスタンスについての情報の設定 26
3.3.5. 追加の管理 Decision Server の公開インターネットへの接続のない環境に Maven ミラーへのアクセスを設定する 27
3.3.6. 追加の管理 Decision Server の RH-SSO 認証パラメーターの設定 28
3.3.7. 追加の管理 Decision Server の LDAP 認証パラメーターの設定 29
3.3.8. 追加の管理 Decision Server の Prometheus メトリクス収集の有効化 30
3.3.9. 追加の管理 Decision Server テンプレートデプロイの開始 31
3.4. (任意) LDAP ロールマッピングファイルの指定 31

第4章 RED HAT DECISION MANAGER ロールおよびユーザー 33

第5章 OPENSHIFT テンプレートの参考資料 34
5.1. RHDM75-AUTHORING.YAML テンプレート 34
5.1.1. パラメーター 34
5.1.2. オブジェクト 49
5.1.2.1. サービス 49
5.1.2.2. ルート 50
5.1.2.3. デプロイメント設定 50
5.1.2.3.1. トリガー 50
5.1.2.3.2. レプリカ 50
5.1.2.3.3. Pod テンプレート 51
5.1.2.4. 外部の依存関係 71
5.1.2.4.1. ボリューム要求 71

5.1.2.4.2. シークレット 71
5.2. RHDM75-AUTHORING-HA.YAML TEMPLATE 71
5.2.1. パラメーター 71
5.2.2. オブジェクト 88
5.2.2.1. サービス 88
5.2.2.2. ルート 89
5.2.2.3. デプロイメント設定 90
5.2.2.3.1. トリガー 90
5.2.2.3.2. レプリカ 90
5.2.2.3.3. Pod テンプレート 90
5.2.2.4. 外部の依存関係 110
5.2.2.4.1. ボリューム要求 110
5.2.2.4.2. シークレット 111
5.2.2.4.3. クラスターリング 111
5.3. RHDM75-KIESERVER.YAML TEMPLATE 112
5.3.1. パラメーター 112
5.3.2. オブジェクト 125
5.3.2.1. サービス 125
5.3.2.2. ルート 126
5.3.2.3. デプロイメント設定 126
5.3.2.3.1. トリガー 126
5.3.2.3.2. レプリカ 126
5.3.2.3.3. Pod テンプレート 126
5.3.2.4. 外部の依存関係 137
5.3.2.4.1. シークレット 137
5.4. OPENSHIFT の使用に関するクイックリファレンス 137

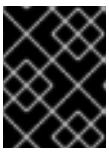
付録A バージョン情報 **140**

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

- Red Hat OpenShift Container Platform バージョン 3.11 がデプロイされている。
- OpenShift クラスター/namespace で 4 ギガバイト以上のメモリーが利用可能である。
- デプロイメントに使用する OpenShift プロジェクトが作成されている。
- **oc** コマンドを使用してプロジェクトにログインしている。**oc** コマンドランツールに関する詳細は、OpenShift の CLI リファレンス を参照してください。OpenShift Web コンソールを使用してテンプレートをデプロイするには、Web コンソールを使用してログインしている必要もあります。
- 動的永続ボリューム (PV) のプロビジョニングが有効になっている。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なければなりません。デフォルトでは、Business 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、Business 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。
- お使いの OpenShift 環境で **ReadWriteMany** モードを使用した永続ボリュームをサポートしている。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。



重要

ReadWriteMany モードは、OpenShift Online および OpenShift Dedicated ではサポートされません。

注記

Red Hat Decision Manager バージョン 7.5 以降、Automation Broker (Ansible Playbook) や全テンプレートを使用したインストールを含む、Red Hat OpenShift Container Platform 3.x へのサポートが非推奨になりました。新機能が追加されない可能性があり、この機能は今後のリリースで削除予定です。

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

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

この場合、Red Hat Decision Manager のコンポーネントは、別の OpenShift Pod としてデプロイされます。各 Pod のスケールアップおよびスケールダウンを個別に行い、特定のコンポーネントに必要な数だけコンテナーを提供できます。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。

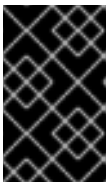
以下の Red Hat Decision Manager の主要コンポーネントが OpenShift で利用できます。

- Decision Server (**実行サーバー (Execution Server)** または **KIE Server** とも呼ばれる) 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 (これらすべて総称で **サービス** と呼ぶ)。サービスのすべてのロジックは実行サーバーで実行されます。
  Decision Server Pod をスケールアップして、同一または異なるホストで実行するコピーを必要な数だけ提供できます。Pod のスケールアップまたはスケールダウンを行うと、そのコピーはすべて同じサービスを実行します。OpenShift は負荷分散を提供しているため、要求はどの Pod でも処理できます。

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

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

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



重要

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

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

以下の環境タイプが一般的です。

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

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

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

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

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

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

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

2.1. イメージストリームとイメージレジストリーの可用性確認

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

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

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

手順

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

2. Red Hat OpenShift Container Platform が Red Hat レジストリーへのアクセス用のユーザー名とパスワードで設定されている場合は、以下のコマンドを実行します。

```
$ oc get imagestreamtag -n openshift | grep -F rhdm75-decisioncentral-openshift
$ oc get imagestreamtag -n openshift | grep -F rhdm75-kieserver-openshift
```

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

3. コマンドの 1 つまたは複数の出力が空白の場合や、Red Hat レジストリーにアクセスするために、OpenShift をユーザー名およびパスワードで設定していない場合は、以下の手順を実行してください。

   a. **oc** コマンドで OpenShift にログインして、プロジェクトがアクティブであることを確認します。

   b. Registry Service Accounts for Shared Environments で説明されている手順を実行します。Red Hat カスタマーポータルにログインし、このドキュメントにアクセスし、レジストリーサービスアカウントを作成する手順を実行する必要があります。

   c. **OpenShift Secret** タブを選択し、**Download secret** のリンクをクリックして、YAML シークレットファイルをダウンロードします。

   d. ダウンロードしたファイルを確認して、**name:** エントリーに記載の名前をメモします。

e. 以下のコマンドを実行します。

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

<file_name> はダウンロードしたファイルに、**<secret_name>** はファイルの **name:** のエントリー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-7.5.1-openshift-templates.zip** の製品配信可能ファイルをダウンロードし、**rhdm75-image-streams.yaml** ファイルを展開します。

g. 以下のコマンドを入力します。

```
$ oc apply -f rhdm75-image-streams.yaml
```

注記

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

2.2. DECISION SERVER にシークレットの作成

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

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

手順

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

注記

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

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

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

2.3. BUSINESS CENTRAL へのシークレットの作成

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

Business Central と Decision Server に同じ証明書およびキーストアを使用しないでください。

手順

1. Business 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。自己署名または購入した SSL 証明書でキーストアを作成する方法は、SSL 暗号化キーおよび証明書 を参照してください。

注記

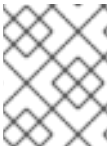
実稼働環境で、Business Central の予想される URL と一致する有効な署名済み証明書を生成します。

2. キーストアを **keystore.jks** ファイルに保存します。
3. 証明書の名前をメモします。Red Hat Decision Manager 設定におけるこのデフォルト名は **jboss** です。
4. キーストアファイルのパスワードをメモします。Red Hat Decision Manager 設定におけるこのデフォルト名は **mykeystorepass** です。
5. **oc** コマンドを使用して、新しいキーストアファイルからシークレット **decisioncentral-app-secret** を生成します。

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

2.4. オフラインで使用する MAVEN ミラーリポジトリーの用意

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



注記

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

前提条件

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

手順

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

セスが必要です。OpenShift 環境に、Nexus リポジトリーマネージャーをデプロイできます。OpenShift への Nexus の設定方法は、Nexus の設定を参照してください。このリポジトリーを別個のミラーリポジトリーとして使用します。
または、サービスにカスタムの外部リポジトリー (Nexus など) を使用する場合、同じリポジトリーをミラーリポジトリーとして使用できます。

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

   a. 最新版の Offliner tool をダウンロードします。

   b. Red Hat カスタマーポータルの Software Downloads ページから利用可能な **rhdm-7.5.1-offliner.txt** の製品配信可能ファイルをダウンロードします。

   c. 以下のコマンドを入力して、Offliner ツールを使用し、必要なアーティファクトをダウンロードします。

   ```
   java -jar offliner-<version>.jar -r https://maven.repository.redhat.com/ga/ -r
   https://repo1.maven.org/maven2/ -d /home/user/temp rhdm-7.5.1-offliner.txt
   ```

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

   d. 一時ディレクトリーから作成した Maven リポジトリーにすべてのアーティファクトをアップロードします。アーティファクトのアップロードには、Maven リポジトリープロビジョナー ユーティリティーを使用できます。

3. Business Central 外でサービスを開発し、追加の依存関係がある場合は、ミラーリポジトリーにその依存関係を追加します。サービスを Maven プロジェクトとして開発した場合は、以下の手順を使用し、これらの依存関係を自動的に用意します。公開インターネットへに送信接続できるコンピューターで、この手順を実行します。

   a. ローカルの Maven キャッシュディレクトリー (~/**.m2/repository**) のバックアップを作成して、ディレクトリーを削除します。

   b. **mvn clean install** コマンドを使用してプロジェクトのソースをビルドします。

   c. すべてのプロジェクトで以下のコマンドを入力し、Maven を使用してプロジェクトで生成したすべてのアーティファクトのランタイムの依存関係をすべてダウンロードするようにします。

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

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

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

2.5. GLUSTERFS 設定の変更

OpenShift 環境が GlusterFS を使用して永続ストレージボリュームを提供するかどうかを確認する必要

があります。GlusterFS を使用している場合は、Business Central の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する必要があります。

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名に置き換えます。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. Business Central を、高可用性設定がない単一の Pod としてのみ使用する予定の場合は、**volumeoptions** キーが含まれる行に、以下のオプションを追加します。

```
features.cache-invalidation on
performance.nl-cache on
```

以下に例を示します。

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

c. Business Central を高可用性設定で使用する予定の場合は、**volumeoptions** キーが含まれる行に、以下のオプションを追加します。

```
features.cache-invalidation on
nfs.trusted-write on
nfs.trusted-sync on
performance.nl-cache on
performance.stat-prefetch off
performance.read-ahead off
performance.write-behind off
performance.readdir-ahead off
performance.io-cache off
performance.quick-read off
performance.open-behind off
locks.mandatory-locking off
performance.strict-o-direct on
```

以下に例を示します。

volumeoptions: client.ssl off, server.ssl off, features.cache-invalidation on, nfs.trusted-write on, nfs.trusted-sync on, performance.nl-cache on, performance.stat-prefetch off, performance.read-ahead off, performance.write-behind off, performance.readdir-ahead off, performance.io-cache off, performance.quick-read off, performance.open-behind off, locks.mandatory-locking off, performance.strict-o-direct 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名に置き換えます。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

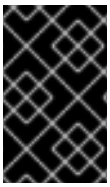
Business Central を使用してサービスの作成や変更を行う環境や、Business Central が管理する Decision Server でサービスを実行するう環境をデプロイできます。この環境には、Business Central と 1 つまたは複数の Decision Server が含まれます。

Business 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 リポジトリーを使用できます。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 (HA) のいずれかの Business Central をデプロイできます。単一の Business Central Pod は複製されず、Business Central のコピー 1 つだけが使用されます。HA Business Central のデプロイメントでは、Business Central をスケーリングできます。

HA Business 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

Red Hat Decision Manager 7.5 では、Business Central の高可用性機能はテクノロジープレビューとしてのみの提供となっています。Red Hat のテクノロジープレビュー機能のサポートの詳細は、テクノロジープレビュー機能のサポート範囲 を参照してください。

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 Business Central と単一の Decision Server 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. オーサリング環境のデプロイメント

OpenShift テンプレートを使用し、単一または高可用性オーサリング環境をデプロイできます。この環境は、Business Central および単一の Decision Server で設定されます。

3.1.1. オーサリング環境用のテンプレートの設定開始

単一オーサリング環境をデプロイする必要がある場合は、**rhdm75-authoring.yaml** テンプレートファイルを使用します。

高可用性オーサリング環境をデプロイする必要がある場合は、 **rhdm75-authoring-ha.yaml** テンプレートファイルを使用します。

手順

1. Red Hat カスタマーポータルの Software Downloads ページから製品配信可能ファイル **rhdm-7.5.1-openshift-templates.zip** をダウンロードします。
2. 必要なテンプレートファイルを展開します。
3. 以下のいずれかの方法を使用してテンプレートのデプロイを開始します。
   - OpenShift Web UI を使用するには、OpenShift アプリケーションコンソールで **Add to Project → Import YAML / JSON** を選択してから **<template-file-name>.yaml** ファイルを選択または貼り付けます。**Add Template** ウィンドウで、**Process the template** が選択されていることを確認し、**Continue** をクリックします。
   - OpenShift コマンドラインコンソールを使用するには、以下のコマンドラインを準備します。

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

     このコマンドラインで、以下のように変更します。
     - **<template-path>** を、ダウンロードしたテンプレートファイルのパスに置き換えます。
     - **<template-file-name>** は、テンプレート名に置き換えます。
     - 必要なパラメーターに設定するために必要な数だけ **-p PARAMETER=value** ペアを使用します。

次のステップ

テンプレートのパラメーターを設定します。「オーサリング環境に必要なパラメーターの設定」の手順に従い、共通のパラメーターを設定します。テンプレートファイルを表示して、すべてのパラメーターの説明を確認します。

3.1.2. オーサリング環境に必要なパラメーターの設定

テンプレートをオーサリング環境をデプロイするように設定する場合は、いずれの場合でも以下のパラメーターを設定する必要があります。

前提条件

- 「オーサリング環境用のテンプレートの設定開始」に説明されているようにテンプレートの設定を開始している。

手順

1. 以下のパラメーターを設定します。
   - **Business Central サーバーキーストアのシークレット名 (DECISION_CENTRAL_HTTPS_SECRET)**: 「Business Central へのシークレットの作成」で作成した Business 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。
   - **Business Central サーバーの証明署名 (DECISION_CENTRAL_HTTPS_NAME)**: 「Business 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。

- **Business Central サーバーキーストアのパスワード** (**DECISION_CENTRAL_HTTPS_PASSWORD**): 「Business 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。
- **アプリケーション名** (**APPLICATION_NAME**): OpenShift アプリケーションの名前。これは Business Central Monitoring および Decision Server のデフォルト URL で使用されます。OpenShift はアプリケーション名を使用して、デプロイメント設定、サービス、ルート、ラベル、およびアーティファクトの個別のセットを作成します。
- **Enable KIE server global discovery** (**KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED**): 同じ namespace 内にある **OpenShiftStartupStrategy** が指定された Decision Server をすべて、Business Central に検出させるには、このパラメーターを **true** に設定します。デフォルトでは、 Business Central は **APPLICATION_NAME** パラメーターが Business Central と同じ値でデプロイされた Decision Server のみを検出します。
- **ImageStream 名前空間** (**IMAGE_STREAM_NAMESPACE**): イメージストリームが利用可能な名前空間。OpenShift 環境でイメージストリームが利用可能な場合 (「イメージストリームとイメージレジストリーの可用性確認」 を参照) は、namespace が **openshift** になります。イメージストリームファイルをインストールしている場合は、名前空間が OpenShift プロジェクトの名前になります。

2. 以下のユーザー名とパスワードを設定できます。デフォルトでは、デプロイメントはパスワードを自動的に生成します。
   - **KIE Admin User**(**KIE_ADMIN_USER**) および **KIE Admin Password**(**KIE_ADMIN_PWD**): 管理者ユーザーのユーザー名およびパスワード。Business Central を使用して同じテンプレートでデプロイされる Decision Server 以外の Decision Server を制御するか、またはモニターする場合、ユーザー名およびパスワードを設定し、これらを記録する必要があります。
   - **KIE Server User**(**KIE_SERVER_USER**) および **KIE Server Password** (**KIE_SERVER_PWD**): Decision Server に接続するためにクライアントアプリケーションが使用できるユーザー名およびパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

3.1.3. オーサリング環境用のイメージストリーム namespace の設定

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

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

前提条件

- 「オーサリング環境用のテンプレートの設定開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

3.1.4. オーサリング環境用のオプションの Maven リポジトリーの設定

テンプレートをオーサリング環境をデプロイするように設定する際、ビルドされた KJAR ファイルを外部の Maven リポジトリーに配置する必要がある場合は、リポジトリーにアクセスするためにパラメーターを設定する必要があります。

前提条件

- 「オーサリング環境用のテンプレートの設定開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

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

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

重要

Business Central プロジェクトを KJAR アーティファクトとして外部の Maven リポジトリー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ー情報を追加する必要があります。Business Central プロジェクトの外部リポジトリー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。

3.1.5. オーサリング環境のビルドイン Maven リポジトリーにアクセスするための認証情報の指定

テンプレートをオーサリング環境をデプロイするように設定する際に、Business Central に組み込まれている Maven リポジトリーを使用し、追加の Decision Server を Business Central に接続する必要がある場合、この Maven リポジトリーにアクセスするための認証情報を設定する必要があります。次に、これらの認証情報を使用して Decision Server を設定できます。

また、RH-SSO または LDAP 認証を設定している場合、ビルトイン Maven リポジトリーの認証情報を、RH-SSO または LDAP で設定されるユーザー名およびパスワードに設定する必要があります。この設定は、Decision Server が Maven リポジトリーにアクセスできるようにするために必要です。

前提条件

- 「オーサリング環境用のテンプレートの設定開始」 に説明されているようにテンプレートの設定を開始している。

手順

ビルトイン Maven リポジトリーの認証情報を設定するには、以下のパラメーターを設定します。

- **Business 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 リポジトリーのユーザー名。
- **Business 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 リポジトリーのパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

3.1.6. オーサリング環境の公開インターネットへの接続のない環境に Maven ミラーへのアクセスを設定する

テンプレートをオーサリング環境をデプロイするように設定する際に、 OpenShift 環境に公開インターネットへの接続がない場合は、「オフラインで使用する Maven ミラーリポジトリーの用意」 に従って設定した Maven ミラーへのアクセスを設定する必要があります。

前提条件

- 「オーサリング環境用のテンプレートの設定開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

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

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

3.1.7. オーサリング環境用の Git フックディレクトリーの指定

Git フックを使用して Business Central の内部 Git リポジトリーと外部 Git リポジトリーの対話を容易にすることができます。

Git フックを使用する必要がある場合は、Git フックディレクトリーを設定する必要があります。

前提条件

- 「オーサリング環境用のテンプレートの設定開始」 に説明されているようにテンプレートの設定を開始している。

手順

Git フックディレクトリーを設定するには、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/kie/data/git/hooks**)。ディレクトリーの内容を指定し、これを指定されたパスにマウントする必要があります。設定マップまたは永続ボリュームを使用して Git フックディレクトリーを指定し、マウントする方法は、「(オプション) Git フックディレクトリーの指定」 を参照してください。

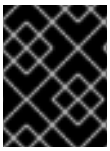
次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

3.1.8. オーサリング環境用の RH-SSO 認証パラメーターの設定

RH-SSO 認証を使用する必要がある場合、テンプレートをオーサリング環境をデプロイするように設定する際に追加の設定を実行します。



重要

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

前提条件

- Red Hat Decision Manager のレルムが RH-SSO 認証システムに作成されている。
- Red Hat Decision Manager のユーザー名およびパスワードが RH-SSO 認証システムに作成されている。利用可能なロールの一覧については、*4章Red Hat Decision Manager ロールおよびユーザー* を参照してください。以下のユーザーは、環境のパラメーターを設定するために必要です。
  - **kie-server,rest-all,admin** ロールを持つ管理者ユーザー。このユーザーは環境を管理し、これを使用できます。Decision Server はこのユーザーを使用して Business Central で認証します。

- **kie-server,rest-all,user** ロールを持つサーバーユーザー。このユーザーは、Decision Server に対する REST API 呼び出しを実行できます。Business Central はこのユーザーを使用して Decision Server で認証します。

- デプロイしている Red Hat Decision Manager 環境の全コンポーネントに対して、クライアントが RH-SSO 認証システムに作成されている。クライアントのセットアップには、コンポーネントの URL が含まれます。環境のデプロイ後に URL を確認し、編集できます。または、Red Hat Decision Manager のデプロイメントでクライアントを作成できます。ただし、このオプションの環境に対する制御の詳細度合はより低くなります。

- 「オーサリング環境用のテンプレートの設定開始」 に説明されているようにテンプレートの設定を開始している。

手順

1. テンプレートの **KIE_ADMIN_USER** および **KIE_ADMIN_PASSWORD** パラメーターを、RH-SSO 認証システムで作成したユーザー名およびパスワードに設定します。

2. テンプレートの **KIE_SERVER_USER** および **KIE_SERVER_PASSWORD** パラメーターを、RH-SSO 認証システムで作成したサーバーユーザーのユーザー名およびパスワードに設定します。

3. 以下のパラメーターを設定します。

   - **RH-SSO URL** (**SSO_URL**): RH-SSO の URL。

   - **RH-SSO レルム名** (**SSO_REALM**): Red Hat Decision Manager の RH-SSO レルム。

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

4. 以下の手順のいずれかを実行します。

   a. RH-SSO で Red Hat Decision Manager のクライアントを作成した場合は、テンプレートで以下のパラメーターを設定します。

      - **Business Central RH-SSO クライアント名** (**DECISION_CENTRAL_SSO_CLIENT**): Business Central の RH-SSO クライアント名。

      - **Business Central RH-SSO クライアントのシークレット** (**DECISION_CENTRAL_SSO_SECRET**): Business 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。

   b. RH-SSO に Red Hat Decision Manager のクライアントを作成する場合は、テンプレートで以下のパラメーターを設定します。

      - **Business Central RH-SSO クライアント名** (**DECISION_CENTRAL_SSO_CLIENT**): Business Central 向けに RH-SSO に作成するクライアント名。

- **Business Central RH-SSO クライアントのシークレット (DECISION_CENTRAL_SSO_SECRET)**: Business 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 向けに RH-SSO に作成するクライアント名。
- **KIE Server の RH-SSO クライアントのシークレット (KIE_SERVER_SSO_SECRET)**: Decision Server のクライアントに対して RH-SSO に設定するシークレットの文字列。
- **RH-SSO レルムの管理者のユーザー名 (SSO_USERNAME)** および **RH-SSO レルムの管理者のパスワード (SSO_PASSWORD)**: Red Hat Decision Manager の RH-SSO レルムの管理者ユーザーに指定するユーザー名とパスワード必要なクライアントを作成するためにこのユーザー名およびパスワードを指定する必要があります。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

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

3.1.9. オーサリング環境用の LDAP 認証パラメーターの設定

LDAP 認証を使用する必要がある場合は、テンプレートをオーサリング環境をデプロイするように設定する際に追加の設定を実行します。

重要

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

前提条件

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

手順

1. LDAP サービスでは、デプロイメントパラメーターですべてのユーザー名を作成します。パラメーターを設定しない場合には、デフォルトのユーザー名を使用してユーザーを作成します。作成したユーザーにはロールに割り当てる必要もあります。

- **KIE_ADMIN_USER**: デフォルトのユーザー名 **adminUser**、ロール: **kie-server,rest-all,admin**
- **KIE_SERVER_USER**: デフォルトのユーザー名 **executionUser**、ロール **kie-server,rest-all,guest**
  LDAP で設定可能なユーザーロールについては、ロールおよびユーザー を参照してください。

2. テンプレートの **AUTH_LDAP*** パラメーターを設定します。これらのパラメーターは、Red Hat JBoss EAP の **LdapExtended** ログインモジュールの設定に対応します。これらの設定に関する説明は、LdapExtended ログインモジュール を参照してください。
   LDAP サーバーがデプロイメントに必要な全ロールを定義していない場合は、LDAP グループを Red Hat Decision Manager ロールにマッピングしてください。LDAP のロールマッピングを有効にするには、以下のパラメーターを設定します。

   - RoleMapping rolesProperties ファイルパス (**AUTH_ROLE_MAPPER_ROLES_PROPERTIES**): **/opt/eap/standalone/configuration/rolemapping/rolemapping.properties** など、ロールのマッピングを定義するファイルの完全修飾パス名。このファイルを指定して、該当するすべてのデプロイメント設定でこのパスにマウントする必要があります。これを実行する方法については、「(任意) LDAP ロールマッピングファイルの指定」 を参照してください。
   - RoleMapping replaceRole プロパティー (**AUTH_ROLE_MAPPER_REPLACE_ROLE**): **true** に設定した場合、マッピングしたロールは、LDAP サーバーに定義したロールに置き換えられます。**false** に設定した場合は、LDAP サーバーに定義したロールと、マッピングしたロールの両方がユーザーアプリケーションロールとして設定されます。デフォルトの設定は **false** です。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

3.1.10. オーサリング環境用の Prometheus メトリクス収集の有効化

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

前提条件

- 「オーサリング環境用のテンプレートの設定開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「オーサリング環境用テンプレートのデプロイの実行」 の手順に従います。

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

3.1.11. オーサリング環境用テンプレートのデプロイの実行

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

手順

使用している方法に応じて、以下の手順を実行します。

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

3.2. (オプション) 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、Business 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. 以下の例では、Business Central デプロイメントの ssh キーパスにこのシークレットをマウントします。

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

   <myapp> をテンプレートの設定時に設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 フックディレクトリーで、変更をアップストリームにプッシュする post-commit フックを指定できます。プロジェクトがリポジトリーから Business 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 フックディレクトリーを Business Central デプロイメントに指定します。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名に置き換えます。以下に例を示します。

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

      iii. Business 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> をテンプレートの設定時に設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設定した **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ボリュームを要求に関連付け、ファイルをボリュームに転送し、ボリュームを **myapp-rhdmcentr** デプロイメント設定にマウントする必要があります (**myapp**をアプリケーション名に置き換えます)。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. 数分待機してから、プロジェクト内の Pod の一覧およびステータスを確認します。Business 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> を、テンプレートの設定時に設定されたアプリケーション名に置き換えます。

3.3. オーサリング環境または管理環境向けの追加の管理 DECISION SERVER のデプロイ

追加の管理 Decision Server をオーサリング環境または管理環境にデプロイできます。サーバーを Business Central デプロイメントと同じプロジェクトにデプロイします。

Decision Server は Maven リポジトリーからサービスをロードします。サーバーを Business Central ビルトインリポジトリーまたは外部リポジトリーのいずれかを使用するように設定する必要があります。

サーバーは、サービスが読み込まれていない状態で起動します。Business Central または Decision Server の REST API を使用してサーバー上にサービスをデプロイまたはデプロイ解除します。

3.3.1. 追加の管理 Decision Server テンプレート設定の開始

追加の管理 Decision Server をデプロイするには、**rhdm75-kieserver.yaml** テンプレートファイルを使用します。

手順

1. Red Hat カスタマーポータルの Software Downloads ページから製品配信可能ファイル **rhdm-7.5.1-openshift-templates.zip** をダウンロードします。
2. **rhdm75-kieserver.yaml** テンプレートファイルを展開します。
3. 以下のいずれかの方法を使用してテンプレートのデプロイを開始します。
   - OpenShift Web UI を使用するには、OpenShift アプリケーションコンソールで **Add to Project → Import YAML / JSON** を選択してから、**rhdm75-kieserver.yaml** ファイルを選択するか、またはこれを貼り付けます。**Add Template** ウィンドウで、**Process the template** が選択されていることを確認し、**Continue** をクリックします。
   - OpenShift コマンドラインコンソールを使用するには、以下のコマンドラインを準備します。

     ```
     oc new-app -f <template-path>/rhdm75-kieserver.yaml -p
     KIE_SERVER_HTTPS_SECRET=kieserver-app-secret -p PARAMETER=value
     ```

     このコマンドラインで、以下のように変更します。
     - **<template-path>** を、ダウンロードしたテンプレートファイルのパスに置き換えます。
     - 必要なパラメーターに設定するために必要な数だけ **-p PARAMETER=value** ペアを使用します。

次のステップ

テンプレートのパラメーターを設定します。「追加の管理 Decision Server に必要なパラメーターの設定」の手順に従い、共通のパラメーターを設定します。テンプレートファイルを表示して、すべてのパラメーターの説明を確認します。

3.3.2. 追加の管理 Decision Server に必要なパラメーターの設定

テンプレートを追加の管理 Decision Server をデプロイするように設定する際、いずれの場合でも以下のパラメーターを設定する必要があります。

前提条件

- 「追加の管理 Decision Server テンプレート設定の開始」 に説明されているようにテンプレートの設定を開始している。

手順

1. 以下のパラメーターを設定します。
   - **KIE Server キーストアのシークレット名 (KIE_SERVER_HTTPS_SECRET)**: 「Decision Server にシークレットの作成」で作成した Decision Server のシークレットの名前。
   - **KIE Server Certificate Name (KIE_SERVER_HTTPS_NAME)**: 「Decision Server にシークレットの作成」 で作成したキーストアの証明書名。
   - **KIE Server Keystore Password (KIE_SERVER_HTTPS_PASSWORD)**: 「Decision Server にシークレットの作成」 で作成したキーストアのパスワード。
   - **アプリケーション名 (APPLICATION_NAME)**: OpenShift アプリケーションの名前。これは Business Central Monitoring および Decision Server のデフォルト URL で使用されます。OpenShift はアプリケーション名を使用して、デプロイメント設定、サービス、ルート、ラベル、およびアーティファクトの個別のセットを作成します。同じテンプレートを同じプロジェクトで使用して複数のアプリケーションをデプロイすることもできますが、その場合はアプリケーション名を同じにすることはできません。また、アプリケーション名は、Decision Server が Business Central で参加するサーバーの設定 (サーバーテンプレート) の名前を決定するものとなります。複数の Decision Server をデプロイする場合には、サーバーごとに異なるアプリケーション名を指定する必要があります。
   - **KIE Server Mode (KIE_SERVER_MODE)**: **rhdm75-kieserver.yaml** テンプレートで、デフォルト値は **PRODUCTION** です。**PRODUCTION** モードでは、**SNAPSHOT** バージョンの KJAR アーティファクトは Decision Server にデプロイできず、既存のコンテナーでアーティファクトのバージョンを変更することはできません。**PRODUCTION** モードで新規バージョンをデプロイするには、同じ Decision Server で新規コンテナーを作成します。**SNAPSHOT** バージョンをデプロイするか、または既存コンテナーのアーティファクトのバージョンを変更するには、このパラメーターを **DEVELOPMENT** に設定します。
   - **ImageStream 名前空間 (IMAGE_STREAM_NAMESPACE)**: イメージストリームが利用可能な名前空間。OpenShift 環境でイメージストリームが利用可能な場合 (「イメージストリームとイメージレジストリーの可用性確認」 を参照) は、namespace が **openshift** になります。イメージストリームファイルをインストールしている場合は、名前空間が OpenShift プロジェクトの名前になります。
2. 以下のユーザー名とパスワードを設定できます。デフォルトでは、デプロイすると、パスワードが自動生成されます。
   - **KIE Server User (KIE_SERVER_USER)** および **KIE Server Password (KIE_SERVER_PWD)**: Decision Server に接続するためにクライアントアプリケーションが使用できるユーザー名およびパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「追加の管理 Decision Server テンプレートデプロイの開始」 の手順に従います。

3.3.3. 追加の管理 Decision Server のイメージストリーム namespace の設定

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

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

前提条件

- 「追加の管理 Decision Server テンプレート設定の開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

3.3.4. 追加の管理 Decision Server 用の Business Central インスタンスについての情報の設定

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

前提条件

- 「追加の管理 Decision Server テンプレート設定の開始」 に説明されているようにテンプレートの設定を開始している。

手順

1. 以下のパラメーターを設定します。
   - **KIE Admin User** (**KIE_ADMIN_USER**) および **KIE Admin Password** (**KIE_ADMIN_PWD**): 管理者ユーザーのユーザー名およびパスワード。これらの値は Business Central の **KIE_ADMIN_USER** および **KIE_ADMIN_PWD** 設定と同じである必要があります。Business Central で RH-SSO または LDAP 認証を使用する場合には、これらのユーザー名とパスワードの値は、Business Central の管理者ロールを使用して認証システムに設定したユーザー名およびパスワードである必要があります。
   - **Business Central サービスの名前** (**DECISION_CENTRAL_SERVICE**): Business Central の OpenShift サービス名。
2. サーバーがサービスを読み込むに使用する Maven リポジトリーへのアクセスを設定します。Business Central が使用するものと同じリポジトリーを設定する必要があります。
   - Business Central が独自のビルトインリポジトリーを使用する場合、以下のパラメーターを設定します。
     - **Business Central の Maven サービスの名前** (**DECISION_CENTRAL_MAVEN_SERVICE**): Business Central の OpenShift サービス名。
     - **Business Central がホストする Maven サービスのユーザー名** (**DECISION_CENTRAL_MAVEN_USERNAME**): Business Central にビルドインの Maven リポジトリーのユーザー名。**DECISION_CENTRAL_MAVEN_USERNAME** として Business Central に設定したユーザー名を入力してください。

- **Business 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**): Business Central にビルドインされている Maven リポジトリーのパスワード。Business 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。

- Business Central を外部 Maven リポジトリーを使用するように設定している場合は、以下のパラメーターを設定します。
  - **Maven リポジトリーの URL** (**MAVEN_REPO_URL**): Business Central が使用する外部 Maven リポジトリーの URL。
  - **Maven リポジトリーの ID** (**MAVEN_REPO_ID**): Maven リポジトリーの ID。デフォルト値は **repo-custom** です。
  - **Maven repository username** (**MAVEN_REPO_USERNAME**): Maven リポジトリーのユーザー名。
  - **Maven リポジトリーのパスワード** (**MAVEN_REPO_PASSWORD**): Maven リポジトリーのパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「追加の管理 Decision Server テンプレートデプロイの開始」 の手順に従います。

3.3.5. 追加の管理 Decision Server の公開インターネットへの接続のない環境に Maven ミラーへのアクセスを設定する

テンプレートを追加の管理 Decision Server をデプロイするように設定する際に、OpenShift 環境に公開インターネットへの接続がない場合は、「オフラインで使用する Maven ミラーリポジトリーの用意」 に従って設定した Maven ミラーへのアクセスを設定する必要があります。

前提条件

- 「追加の管理 Decision Server テンプレート設定の開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

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

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

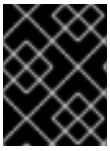
次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「追加の管理 Decision Server テンプレートデプロイの開始」 の手順に従います。

3.3.6. 追加の管理 Decision Server の RH-SSO 認証パラメーターの設定

RH-SSO 認証を使用する必要がある場合は、テンプレートを管理 Decision Server をデプロイするように設定する際に追加の設定を実行します。



重要

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

前提条件

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

手順

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

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

3. 以下の手順のいずれかを実行します。

   a. RH-SSO で Red Hat Decision Manager のクライアントを作成した場合は、テンプレートで以下のパラメーターを設定します。

      - **Business Central RH-SSO クライアント名** (**DECISION_CENTRAL_SSO_CLIENT**): Business Central の RH-SSO クライアント名。
      - **KIE Server の RH-SSO クライアント名** (**KIE_SERVER_SSO_CLIENT**): Decision Server の RH-SSO クライアント名。
      - **KIE Server の RH-SSO クライアントのシークレット** (**KIE_SERVER_SSO_SECRET**): Decision Server のクライアントに対して RH-SSO に設定するシークレットの文字列。

   b. RH-SSO に Red Hat Decision Manager のクライアントを作成する場合は、テンプレートで以下のパラメーターを設定します。

      - **KIE Server の RH-SSO クライアント名** (**KIE_SERVER_SSO_CLIENT**): Decision Server 向けに RH-SSO に作成するクライアント名。
      - **KIE Server の RH-SSO クライアントのシークレット** (**KIE_SERVER_SSO_SECRET**): Decision Server のクライアントに対して RH-SSO に設定するシークレットの文字列。
      - **RH-SSO レルムの管理者のユーザー名** (**SSO_USERNAME**) および **RH-SSO レルムの管理者のパスワード** (**SSO_PASSWORD**): Red Hat Decision Manager の RH-SSO レルムの管理者ユーザーに指定するユーザー名とパスワード必要なクライアントを作成するためにこのユーザー名およびパスワードを指定する必要があります。

次のステップ

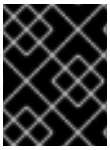
必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「追加の管理 Decision Server テンプレートデプロイの開始」 の手順に従います。

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

3.3.7. 追加の管理 Decision Server の LDAP 認証パラメーターの設定

LDAP 認証を使用する必要がある場合は、テンプレートを追加の管理 Decision Server をデプロイするように設定する際に追加の設定を実行します。



重要

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

前提条件

- LDAP システムに Red Hat Decision Manager のユーザー名およびパスワードを作成している。利用可能なロールの一覧については、*4章Red Hat Decision Manager ロールおよびユーザー* を参照してください。この環境のパラメーターを設定するために、少なくとも以下のユーザーを

作成している必要があります。

- **kie-server,rest-all,admin** ロールを持つ管理者ユーザー。このユーザーは環境を管理し、これを使用できます。
- **kie-server,rest-all,user** ロールを持つサーバーユーザー。このユーザーは、Decision Server に対する REST API 呼び出しを実行できます。

- 「追加の管理 Decision Server テンプレート設定の開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「追加の管理 Decision Server テンプレートデプロイの開始」 の手順に従います。

3.3.8. 追加の管理 Decision Server の Prometheus メトリクス収集の有効化

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

前提条件

- 「追加の管理 Decision Server テンプレート設定の開始」 に説明されているようにテンプレートの設定を開始している。

手順

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

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「追加の管理 Decision Server テンプレートデプロイの開始」 の手順に従います。

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

3.3.9. 追加の管理 Decision Server テンプレートデプロイの開始

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

手順

使用している方法に応じて、以下の手順を実行します。

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

3.4. (任意) LDAP ロールマッピングファイルの指定

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

手順

1. **my-role-map** など、ロールマッピングのプロパティー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ー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. 以下のコマンドを入力して、このファイルから OpenShift 設定ファイルのマッピングを作成します。

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

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

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

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。以下のデプロイメント設定は、この環境で影響を受ける可能性があります。

   - **myapp-rhdmcentr**: Business Central
   - **myapp-kieserver**: Decision Server

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

   すべてのデプロイメント設定について、以下のコマンドを実行します。

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

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

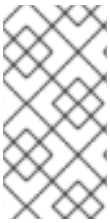
第4章 RED HAT DECISION MANAGER ロールおよびユーザー

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

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

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

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



注記

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

- **admin**: **admin** ロールを持つユーザーは Business Central 管理者です。管理者は、ユーザーの管理や、リポジトリーの作成、クローン作成、および管理ができます。アプリケーションで必要な変更をすべて利用できます。**admin** ロールを持つユーザーは、Red Hat Decision Manager の全領域にアクセスできます。

- **analyst**: **analyst** ロールを持つユーザーには、すべてのハイレベル機能へのアクセスがあります。プロジェクトのモデル化が可能です。ただし、このユーザーは、**Design → Projects** ビューでスペースに貢献者を追加したり、スペースを削除したりできません。**analyst** ロールを持つユーザーは、管理者向けの **Deploy → Execution Servers** ビューにアクセスできません。ただし、これらのユーザーは、ライブラリーパースペクティブにアクセスするときに **Deploy** ボタンを使用できます。

- **rest-all**: **rest-all** ロールを持つユーザーは、Business Central REST 機能にアクセスできます。

- **kie-server**: **kie-server** ロールを持つユーザーは Decision Server (KIE サーバー) REST 機能へのアクセスがあります。

第5章 OPENSHIFT 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-7.5.1-openshift-templates.zip** をダウンロードして展開します。

- **rhdm75-authoring.yaml** は Business Central と Business 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、「rhdm75-authoring.yaml テンプレート」 を参照してください。
- **rhdm75-authoring-ha.yaml** は高可用性 Business Central および Business 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、「rhdm75-authoring-ha.yaml template」 を参照してください。
- **rhdm75-kieserver.yaml** は Decision Server を提供します。Decision server を Business Central に接続するように設定できます。この方法で、Business 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、「rhdm75-kieserver.yaml template」 を参照してください。

5.1. RHDM75-AUTHORING.YAML テンプレート

Red Hat Decision Manager 7.5 の HA 以外の永続的な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 (非推奨)

5.1.1. パラメーター

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

変数名	イメージの環境変数	説明	値の例	必須
APPLICATION_NAME	–	アプリケーションの名前。	myapp	True
KIE_ADMIN_USER	**KIE_ADMIN_USER**	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PWD	**KIE_ADMIN_PWD**	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
KIE_SERVER_CONTROLLER_USER	**KIE_SERVER_CONTROLLER_USER**	KIE サーバー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する)	controllerUser	False
KIE_SERVER_CONTROLLER_PWD	**KIE_SERVER_CONTROLLER_PWD**	KIE サーバー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する)	–	False
KIE_SERVER_CONTROLLER_TOKEN	**KIE_SERVER_CONTROLLER_TOKEN**	ベアラー認証用の KIE Server コントローラートークン。(org.kie.server.controller.token システムプロパティーを設定)	–	False
KIE_SERVER_USER	**KIE_SERVER_USER**	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	executionUser	False
KIE_SERVER_PWD	**KIE_SERVER_PWD**	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	–	False
KIE_SERVER_BYPASS_AUTH_USER	**KIE_SERVER_BYPASS_AUTH_USER**	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。(org.kie.server.bypass.auth.user システムプロパティーを設定)	false	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_MODE	**KIE_SERVER_MODE**	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナーでアーティファクトのバージョンを変更することはできません。(org.kie.server.mode システムプロパティーを設定)	**DEVELOPMENT**	False
KIE_MBEANS	**KIE_MBEANS**	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
DROOLS_SERVER_FILTER_CLASSES	**DROOLS_SERVER_FILTER_CLASSES**	KIE Server のクラスフィルター (org.drools.server.filter.classes システムプロパティーを設定)	true	False
PROMETHEUS_SERVER_EXT_DISABLED	**PROMETHEUS_SERVER_EXT_DISABLED**	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	false	False

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_HOSTNAME_HTTP	**HOSTNAME_HTTP**	Decision Central の 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は空白にします (例: insecure-<application-name>-rhdmcentr-<project>.<default-domain-suffix>)。	–	False
DECISION_CENTRAL_HOSTNAME_HTTPS	**HOSTNAME_HTTPS**	Decision Central の https 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
KIE_SERVER_HOSTNAME_HTTP	**HOSTNAME_HTTP**	KIE Server の http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>)。	–	False
KIE_SERVER_HOSTNAME_HTTPS	**HOSTNAME_HTTPS**	KIE Server の https 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
DECISION_CENTRAL_HTTPS_SECRET	–	Decision Central のキーストアファイルが含まれるシークレットの名前。	decisioncentral-app-secret	True
DECISION_CENTRAL_HTTPS_KEYSTORE	**HTTPS_KEYSTORE**	シークレット内のキーストアファイルの名前。	keystore.jks	False
DECISION_CENTRAL_HTTPS_NAME	**HTTPS_NAME**	サーバー証明書に関連付けられている名前	jboss	False
DECISION_CENTRAL_HTTPS_PASSWORD	**HTTPS_PASSWORD**	キーストアおよび証明書のパスワード。	mykeystorepass	False
KIE_SERVER_HTTPS_SECRET	–	キーストアファイルを含むシークレット名	kieserver-app-secret	True
KIE_SERVER_HTTPS_KEYSTORE	**HTTPS_KEYSTORE**	シークレット内のキーストアファイルの名前。	keystore.jks	False
KIE_SERVER_HTTPS_NAME	**HTTPS_NAME**	サーバー証明書に関連付けられている名前	jboss	False
KIE_SERVER_HTTPS_PASSWORD	**HTTPS_PASSWORD**	キーストアおよび証明書のパスワード。	mykeystorepass	False
KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED	**KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED**	true に設定すると、KIE Server のグローバル検出機能はオンになります (org.kie.server.controller.openshift.global.discovery.enabled システムプロパティーを設定)。	false	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE	**KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE**	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。(org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティーを設定します)	true	False
KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL	**KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL**	KIE ServerTemplate Cache TTL (ミリ秒単位)。(org.kie.server.controller.template.cache.ttl システムプロパティーを設定)	60000	False
IMAGE_STREAM_NAMESPACE	–	Red Hat Decision Manager イメージの ImageStream がインストールされている名前空間。これらの ImageStreams は通常 OpenShift の名前空間にインストールされています。ImageStreams を別の namespace/プロジェクトにインストールしている場合には、これを変更するだけで結構です。	openshift	True

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_IMAGE_STREAM_NAME	–	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm-kieserver-rhel8 です。	rhdm-kieserver-rhel8	True
IMAGE_STREAM_TAG	–	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 7.5.0 です。	7.5.0	True
MAVEN_MIRROR_URL	**MAVEN_MIRROR_URL**	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	–	False
MAVEN_MIRROR_OF	**MAVEN_MIRROR_OF**	KIE Server の Maven ミラー設定。	external:*,!repo-rhdmcentr	False

変数名	イメージの環境変数	説明	値の例	必須
MAVEN_REPO_ID	**MAVEN_REPO_ID**	Maven リポジトリーに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	repo-custom	False
MAVEN_REPO_URL	**MAVEN_REPO_URL**	Maven リポジトリーまたはサービスへの完全修飾 URL。	http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/	False
MAVEN_REPO_USERNAME	**MAVEN_REPO_USERNAME**	Maven リポジトリーにアクセスするユーザー名 (必要な場合)	–	False
MAVEN_REPO_PASSWORD	**MAVEN_REPO_PASSWORD**	Maven リポジトリーにアクセスするパスワード (必要な場合)。	–	False
DECISION_CENTRAL_MAVEN_USERNAME	**KIE_MAVEN_USER**	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

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_MAVEN_PASSWORD	**KIE_MAVEN_PWD**	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
GIT_HOOKS_DIR	**GIT_HOOKS_DIR**	git フックに使用するディレクトリー (必要な場合)。	**/opt/kie/data/git/hooks**	False
DECISION_CENTRAL_VOLUME_CAPACITY	–	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
DECISION_CENTRAL_MEMORY_LIMIT	–	Decision Central コンテナーのメモリー制限。	2Gi	False
KIE_SERVER_MEMORY_LIMIT	–	KIE Server のコンテナーのメモリー制限。	1Gi	False
SSO_URL	**SSO_URL**	RH-SSO URL。	https://rh-sso.example.com/auth	False
SSO_REALM	**SSO_REALM**	RH-SSO レルム名。	–	False
DECISION_CENTRAL_SSO_CLIENT	**SSO_CLIENT**	Decision Central RH-SSO クライアント名。	–	False
DECISION_CENTRAL_SSO_SECRET	**SSO_SECRET**	Decision Central RH-SSO クライアントシークレット。	252793ed-7118-4ca8-8dab-5622fa97d892	False
KIE_SERVER_SSO_CLIENT	**SSO_CLIENT**	KIE Server の RH-SSO クライアント名。	–	False
KIE_SERVER_SSO_SECRET	**SSO_SECRET**	KIE Server の RH-SSO クライアントシークレット。	252793ed-7118-4ca8-8dab-5622fa97d892	False

変数名	イメージの環境変数	説明	値の例	必須
SSO_USERNAME	**SSO_USERNAME**	クライアント作成に使用する RH-SSO レルムの管理者のユーザー名 (存在しない場合)	–	False
SSO_PASSWORD	**SSO_PASSWORD**	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	**SSO_DISABLE_SSL_CERTIFICATE_VALIDATION**	RH-SSO が無効な SSL 証明書の検証。	false	False
SSO_PRINCIPAL_ATTRIBUTE	**SSO_PRINCIPAL_ATTRIBUTE**	ユーザー名として使用する RH-SSO プリンシパル属性	preferred_username	False
AUTH_LDAP_URL	**AUTH_LDAP_URL**	認証用に接続する LDAP エンドポイント。	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	**AUTH_LDAP_BIND_DN**	認証に使用するバインド DN	uid=admin,ou=users,ou=exmample,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	**AUTH_LDAP_BIND_CREDENTIAL**	認証に使用する LDAP の認証情報	パスワード	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	**AUTH_LDAP_JAAS_SECURITY_DOMAIN**	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	–	False
AUTH_LDAP_BASE_CTX_DN	**AUTH_LDAP_BASE_CTX_DN**	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	ou=users,ou=example,ou=com	False

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

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

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

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

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

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

5.1.2. オブジェクト

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

5.1.2.1. サービス

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

サービス	ポート	名前	説明
${APPLICATION_NAME}-rhdmcentr	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
${APPLICATION_NAME}-kieserver	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	

5.1.2.2. ルート

ルートとは、**www.example.com** など、外部から到達可能なホスト名を指定して、サービスを公開する手段です。ルーターは、定義したルートや、サービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセレクター、セキュリティー設定 (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	セキュリティー	ホスト名
insecure-${APPLICATION_NAME}-rhdmcentr-http	なし	**${DECISION_CENTRAL_HOSTNAME_HTTP}**
${APPLICATION_NAME}-rhdmcentr-https	TLS パススルー	**${DECISION_CENTRAL_HOSTNAME_HTTPS}**
insecure-${APPLICATION_NAME}-kieserver-http	なし	**${KIE_SERVER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-kieserver-https	TLS パススルー	**${KIE_SERVER_HOSTNAME_HTTPS}**

5.1.2.3. デプロイメント設定

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

5.1.2.3.1. 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
${APPLICATION_NAME}-rhdmcentr	ImageChange
${APPLICATION_NAME}-kieserver	ImageChange

5.1.2.3.2. 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、コンテナー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
${APPLICATION_NAME}-rhdmcentr	1
${APPLICATION_NAME}-kieserver	1

5.1.2.3.3. Pod テンプレート

5.1.2.3.3.1. 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
${APPLICATION_NAME}-rhdmcentr	**${APPLICATION_NAME}-rhdmsvc**
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-rhdmsvc**

5.1.2.3.3.2. イメージ

デプロイメント	イメージ
${APPLICATION_NAME}-rhdmcentr	rhdm-decisioncentral-rhel8
${APPLICATION_NAME}-kieserver	**${KIE_SERVER_IMAGE_STREAM_NAME}**

5.1.2.3.3.3. Readiness Probe

${APPLICATION_NAME}-rhdmcentr

> Http Get on http://localhost:8080/rest/ready

${APPLICATION_NAME}-kieserver

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

5.1.2.3.3.4. Liveness Probe

${APPLICATION_NAME}-rhdmcentr

> Http Get on http://localhost:8080/rest/healthy

- ${APPLICATION_NAME}-kieserver

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

5.1.2.3.3.5. 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
${APPLICATION_NAME}-rhdmcentr	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
${APPLICATION_NAME}-kieserver	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**

5.1.2.3.3.6. イメージの環境変数

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

デプロイメント	変数名	説明	値の例
	KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED	true に設定すると、KIE Server のグローバル検出機能はオンになります (org.kie.server.controller.openshift.global.discovery.enabled システムプロパティーを設定)。	**${KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED}**
	KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。(org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティーを設定します)	**${KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE}**
	KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL	KIE ServerTemplate Cache TTL (ミリ秒単位)。(org.kie.server.controller.template.cache.ttl システムプロパティーを設定)	**${KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL}**
	KIE_WORKBENCH_CONTROLLER_OPENSHIFT_ENABLED	–	true
	KIE_SERVER_CONTROLLER_USER	KIE サーバーコントローラーのユーザー名。(org.kie.server.controller.user システムプロパティーを設定する)	**${KIE_SERVER_CONTROLLER_USER}**
	KIE_SERVER_CONTROLLER_PWD	KIE サーバー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する)	**${KIE_SERVER_CONTROLLER_PWD}**

デプロイメント	変数名	説明	値の例
	KIE_SERVER_CONTROLLER_TOKEN	ベアラー認証用の KIE Server コントローラートークン。(org.kie.server.controller.token システムプロパティーを設定)	**${KIE_SERVER_CONTROLLER_TOKEN}**
	KIE_SERVER_USER	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	**${KIE_SERVER_USER}**
	KIE_SERVER_PWD	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	**${KIE_SERVER_PWD}**
	WORKBENCH_ROUTE_NAME	–	**${APPLICATION_NAME}-rhdmcentr**
	MAVEN_MIRROR_URL	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	**${MAVEN_MIRROR_URL}**
	MAVEN_REPO_ID	Maven リポジトリーに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	**${MAVEN_REPO_ID}**

デプロイメント	変数名	説明	値の例
	MAVEN_REPO_URL	Maven リポジトリーまたはサービスへの完全修飾 URL。	**${MAVEN_REPO_URL}**
	MAVEN_REPO_USERNAME	Maven リポジトリーにアクセスするユーザー名 (必要な場合)	**${MAVEN_REPO_USERNAME}**
	MAVEN_REPO_PASSWORD	Maven リポジトリーにアクセスするパスワード (必要な場合)。	**${MAVEN_REPO_PASSWORD}**
	KIE_MAVEN_USER	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	**${DECISION_CENTRAL_MAVEN_USERNAME}**
	KIE_MAVEN_PWD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	**${DECISION_CENTRAL_MAVEN_PASSWORD}**
	GIT_HOOKS_DIR	git フックに使用するディレクトリー (必要な場合)。	**${GIT_HOOKS_DIR}**
	HTTPS_KEYSTORE_DIR	–	**/etc/decisioncentral-secret-volume**
	HTTPS_KEYSTORE	シークレット内のキーストアファイル名	**${DECISION_CENTRAL_HTTPS_KEYSTORE}**
	HTTPS_NAME	サーバー証明書に関連付けられている名前	**${DECISION_CENTRAL_HTTPS_NAME}**
	HTTPS_PASSWORD	キーストアおよび証明書のパスワード	**${DECISION_CENTRAL_HTTPS_PASSWORD}**
	SSO_URL	RH-SSO URL。	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war

デプロイメント	変数名	説明	値の例
	SSO_REALM	RH-SSO レルム名。	**${SSO_REALM}**
	SSO_SECRET	Decision Central RH-SSO クライアントシークレット。	**${DECISION_CENTRAL_SSO_SECRET}**
	SSO_CLIENT	Decision Central RH-SSO クライアント名。	**${DECISION_CENTRAL_SSO_CLIENT}**
	SSO_USERNAME	クライアント作成に使用する RH-SSO レルムの管理者のユーザー名 (存在しない場合)	**${SSO_USERNAME}**
	SSO_PASSWORD	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO が無効な SSL 証明書の検証。	**${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}**
	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	**${SSO_PRINCIPAL_ATTRIBUTE}**
	HOSTNAME_HTTP	Decision Central の http サービスルートのカスタムホスト名。デフォルトホスト名は空白にします (例: insecure-<application-name>-rhdmcentr-<project>.<default-domain-suffix>)。	**${DECISION_CENTRAL_HOSTNAME_HTTP}**
	HOSTNAME_HTTPS	Decision Central の https 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>)。	**${DECISION_CENTRAL_HOSTNAME_HTTPS}**
	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント。	**${AUTH_LDAP_URL}**

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

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_PARSE_USERNAME	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、 DN はユーザー名に対して解析されます。false に設定した場合には、 DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	**${AUTH_LDAP_PARSE_USERNAME}**
	AUTH_LDAP_USERNAME_BEGIN_STRING	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	**${AUTH_LDAP_USERNAME_BEGIN_STRING}**
	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	**${AUTH_LDAP_USERNAME_END_STRING}**
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前。	**${AUTH_LDAP_ROLE_ATTRIBUTE_ID}**
	AUTH_LDAP_ROLES_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	**${AUTH_LDAP_ROLES_CTX_DN}**

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

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

デプロイメント	変数名	説明	値の例
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping のログインモジュールで、指定したファイルを使用するように設定します。このパラメーターは、ロールを置換ロールに対してマップするプロパティーファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	**${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}**
	AUTH_ROLE_MAPPER_REPLACE_ROLE	現在のロールを追加するか、マップされたロールに現在のロールを置き換えるか。true に設定した場合は、置き換えられます。	**${AUTH_ROLE_MAPPER_REPLACE_ROLE}**
${APPLICATION_NAME}-kieserver	**WORKBENCH_SERVICE_NAME**	–	**${APPLICATION_NAME}-rhdmcentr**
	KIE_ADMIN_USER	KIE 管理者のユーザー名	**${KIE_ADMIN_USER}**
	KIE_ADMIN_PWD	KIE 管理者のパスワード	**${KIE_ADMIN_PWD}**
	KIE_SERVER_MODE	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナーでアーティファクトのバージョンを変更することはできません。(org.kie.server.mode システムプロパティーを設定)	**${KIE_SERVER_MODE}**

デプロイメント	変数名	説明	値の例
	KIE_MBEANS	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)。	**${KIE_MBEANS}**
	DROOLS_SERVER_FILTER_CLASSES	KIE Server のクラスフィルター (org.drools.server.filter.classes システムプロパティーを設定)	**${DROOLS_SERVER_FILTER_CLASSES}**
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	**${PROMETHEUS_SERVER_EXT_DISABLED}**
	KIE_SERVER_BYPASS_AUTH_USER	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。(org.kie.server.bypass.auth.user システムプロパティーを設定)	**${KIE_SERVER_BYPASS_AUTH_USER}**
	KIE_SERVER_ID	–	–
	KIE_SERVER_ROUTE_NAME	–	**${APPLICATION_NAME}-kieserver**
	KIE_SERVER_STARTUP_STRATEGY	–	OpenShiftStartupStrategy
	KIE_SERVER_USER	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	**${KIE_SERVER_USER}**
	KIE_SERVER_PWD	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	**${KIE_SERVER_PWD}**

デプロイメント	変数名	説明	値の例
	MAVEN_MIRROR_URL	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	**${MAVEN_MIRROR_URL}**
	MAVEN_MIRROR_OF	KIE Server の Maven ミラー設定。	**${MAVEN_MIRROR_OF}**
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_ID	–	repo-rhdmcentr
	RHDMCENTR_MAVEN_REPO_SERVICE	–	**${APPLICATION_NAME}-rhdmcentr**
	RHDMCENTR_MAVEN_REPO_PATH	–	**/maven2/**
	RHDMCENTR_MAVEN_REPO_USERNAME	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	**${DECISION_CENTRAL_MAVEN_USERNAME}**
	RHDMCENTR_MAVEN_REPO_PASSWORD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	**${DECISION_CENTRAL_MAVEN_PASSWORD}**

デプロイメント	変数名	説明	値の例
	EXTERNAL_MAVEN_REPO_ID	Maven リポジトリーに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Maven リポジトリーまたはサービスへの完全修飾 URL。	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Maven リポジトリーにアクセスするユーザー名 (必要な場合)	**${MAVEN_REPO_USERNAME}**
	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリーにアクセスするパスワード (必要な場合)。	**${MAVEN_REPO_PASSWORD}**
	HTTPS_KEYSTORE_DIR	–	**/etc/kieserver-secret-volume**
	HTTPS_KEYSTORE	シークレット内のキーストアファイルの名前。	**${KIE_SERVER_HTTPS_KEYSTORE}**
	HTTPS_NAME	サーバー証明書に関連付けられている名前	**${KIE_SERVER_HTTPS_NAME}**
	HTTPS_PASSWORD	キーストアおよび証明書のパスワード。	**${KIE_SERVER_HTTPS_PASSWORD}**
	SSO_URL	RH-SSO URL。	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war

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

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

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

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

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

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

5.1.2.3.3.7. ボリューム

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

5.1.2.4. 外部の依存関係

5.1.2.4.1. 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
${APPLICATION_NAME}-rhdmcentr-claim	ReadWriteOnce

5.1.2.4.2. 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

5.2. RHDM75-AUTHORING-HA.YAML TEMPLATE

Red Hat Decision Manager 7.5 の HA の永続的な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 (非推奨)

5.2.1. パラメーター

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

変数名	イメージの環境変数	説明	値の例	必須
APPLICATION_NAME	–	アプリケーションの名前。	myapp	True

変数名	イメージの環境変数	説明	値の例	必須
KIE_ADMIN_USER	**KIE_ADMIN_USER**	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PWD	**KIE_ADMIN_PWD**	KIE 管理者のパスワード	–	False
KIE_SERVER_CONTROLLER_USER	**KIE_SERVER_CONTROLLER_USER**	KIE サーバー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する)	controllerUser	False
KIE_SERVER_CONTROLLER_PWD	**KIE_SERVER_CONTROLLER_PWD**	KIE サーバー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する)	–	False
KIE_SERVER_CONTROLLER_TOKEN	**KIE_SERVER_CONTROLLER_TOKEN**	ベアラー認証用の KIE Server コントローラートークン。(org.kie.server.controller.token システムプロパティーを設定)	–	False
KIE_SERVER_USER	**KIE_SERVER_USER**	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	executionUser	False
KIE_SERVER_PWD	**KIE_SERVER_PWD**	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	–	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_BYPASS_AUTH_USER	**KIE_SERVER_BYPASS_AUTH_USER**	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。(org.kie.server.bypass.auth.user システムプロパティーを設定)	false	False
KIE_SERVER_MODE	**KIE_SERVER_MODE**	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナーでアーティファクトのバージョンを変更することはできません。(org.kie.server.mode システムプロパティーを設定)	**DEVELOPMENT**	False
KIE_MBEANS	**KIE_MBEANS**	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	enabled	False
DROOLS_SERVER_FILTER_CLASSES	**DROOLS_SERVER_FILTER_CLASSES**	KIE Server クラスのフィルターリング。(org.drools.server.filter.classes システムプロパティーを設定)	true	False

変数名	イメージの環境変数	説明	値の例	必須
PROMETHEUS_SERVER_EXT_DISABLED	**PROMETHEUS_SERVER_EXT_DISABLED**	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	false	False
DECISION_CENTRAL_HOSTNAME_HTTP	**HOSTNAME_HTTP**	Decision Central の 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は空白にします (例: insecure-<application-name>-rhdmcentr-<project>.<default-domain-suffix>)。	–	False
DECISION_CENTRAL_HOSTNAME_HTTPS	**HOSTNAME_HTTPS**	Decision Central の https 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
KIE_SERVER_HOSTNAME_HTTP	**HOSTNAME_HTTP**	KIE Server の http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>)。	–	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_HOSTNAME_HTTPS	**HOSTNAME_HTTPS**	KIE Server の https 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
DECISION_CENTRAL_HTTPS_SECRET	–	Decision Central のキーストアファイルが含まれるシークレットの名前。	decisioncentral-app-secret	True
DECISION_CENTRAL_HTTPS_KEYSTORE	**HTTPS_KEYSTORE**	Decision Central のシークレット内のキーストアファイルの名前。	keystore.jks	False
DECISION_CENTRAL_HTTPS_NAME	**HTTPS_NAME**	Decision Central のサーバー証明書に関連付けられている名前。	jboss	False
DECISION_CENTRAL_HTTPS_PASSWORD	**HTTPS_PASSWORD**	Decision Central のキーストアおよび証明書のパスワード。	mykeystorepass	False
KIE_SERVER_HTTPS_SECRET	–	KIE Server のキーストアファイルが含まれるシークレットの名前。	kieserver-app-secret	True
KIE_SERVER_HTTPS_KEYSTORE	**HTTPS_KEYSTORE**	KIE Server のシークレット内のキーストアファイルの名前。	keystore.jks	False
KIE_SERVER_HTTPS_NAME	**HTTPS_NAME**	KIE Server のサーバー証明書に関連付けられている名前。	jboss	False
KIE_SERVER_HTTPS_PASSWORD	**HTTPS_PASSWORD**	KIE Server のキーストアおよび証明書のパスワード。	mykeystorepass	False

変数名	イメージの環境変数	説明	値の例	必須
APPFORMER_JMS_BROKER_USER	**APPFORMER_JMS_BROKER_USER**	JMS ブローカーに接続するためのユーザー名	jmsBrokerUser	True
APPFORMER_JMS_BROKER_PASSWORD	**APPFORMER_JMS_BROKER_PASSWORD**	JMS ブローカーに接続するためのパスワード。	–	True
DATAGRID_IMAGE	–	DataGrid イメージ。	registry.redhat.io/jboss-datagrid-7/datagrid73-openshift:1.2	True
DATAGRID_CPU_LIMIT	–	DataGrid Container の CPU の制限	1000 m	True
DATAGRID_MEMORY_LIMIT	–	DataGrid コンテナーのメモリー制限。	2Gi	True
DATAGRID_VOLUME_CAPACITY	–	DataGrid のランタイムデータの永続ストレージのサイズ。	1Gi	True
AMQ_BROKER_IMAGE	–	AMQ ブローカーイメージ。	registry.redhat.io/amq7/amq-broker:7.4	True
AMQ_ROLE	–	標準ブローカーユーザーのユーザーロール。	admin	True
AMQ_NAME	–	ブローカーの名前。	broker	True
AMQ_GLOBAL_MAX_SIZE	–	メッセージデータが使用可能な最大メモリー量を指定します。値が指定されていない場合は、システムのメモリーの半分が割り当てられます。	10 gb	False

変数名	イメージの環境変数	説明	値の例	必須
AMQ_VOLUME_CAPACITY	–	AMQ ブローカーボリュームの永続ストレージのサイズ。	1Gi	True
AMQ_REPLICAS	–	クラスターのブローカーレプリカ数。	2	True
KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED	**KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED**	true に設定すると、KIE Server のグローバル検出機能はオンになります (org.kie.server.controller.openshift.global.discovery.enabled システムプロパティーを設定)。	false	False
KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE	**KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE**	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。 (org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティーを設定します)	true	False
KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL	**KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL**	KIE ServerTemplate Cache TTL (ミリ秒単位)。 (org.kie.server.controller.template.cache.ttl システムプロパティーを設定)	60000	False

変数名	イメージの環境変数	説明	値の例	必須
IMAGE_STREAM_NAMESPACE	–	Red Hat Decision Manager イメージの ImageStream がインストールされている名前空間。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
DECISION_CENTRAL_IMAGE_STREAM_NAME	–	Decision Central に使用するイメージストリームの名前。デフォルトは rhdm-decisioncentral-rhel8 です。	rhdm-decisioncentral-rhel8	True
KIE_SERVER_IMAGE_STREAM_NAME	–	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm-kieserver-rhel8 です。	rhdm-kieserver-rhel8	True
IMAGE_STREAM_TAG	–	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 7.5.0 です。	7.5.0	True

変数名	イメージの環境変数	説明	値の例	必須
MAVEN_MIRROR_URL	**MAVEN_MIRROR_URL**	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	–	False
MAVEN_MIRROR_OF	**MAVEN_MIRROR_OF**	KIE Server の Maven ミラー設定。	external:*,!repo-rhdmcentr	False
MAVEN_REPO_ID	**MAVEN_REPO_ID**	Maven リポジトリーに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	repo-custom	False
MAVEN_REPO_URL	**MAVEN_REPO_URL**	Maven リポジトリーまたはサービスへの完全修飾 URL。	http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/	False

変数名	イメージの環境変数	説明	値の例	必須
MAVEN_REPO_USERNAME	**MAVEN_REPO_USERNAME**	Maven リポジトリーにアクセスするユーザー名 (必要な場合)	–	False
MAVEN_REPO_PASSWORD	**MAVEN_REPO_PASSWORD**	Maven リポジトリーにアクセスするパスワード (必要な場合)。	–	False
DECISION_CENTRAL_MAVEN_USERNAME	**KIE_MAVEN_USER**	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
DECISION_CENTRAL_MAVEN_PASSWORD	**KIE_MAVEN_PWD**	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
GIT_HOOKS_DIR	**GIT_HOOKS_DIR**	git フックに使用するディレクトリー (必要な場合)。	**/opt/kie/data/git/hooks**	False
DECISION_CENTRAL_VOLUME_CAPACITY	–	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
DECISION_CENTRAL_MEMORY_LIMIT	–	Decision Central コンテナーのメモリー制限。	2Gi	False
KIE_SERVER_MEMORY_LIMIT	–	KIE Server のコンテナーのメモリー制限。	1Gi	False
SSO_URL	**SSO_URL**	RH-SSO URL。	https://rh-sso.example.com/auth	False
SSO_REALM	**SSO_REALM**	RH-SSO レルム名。	–	False

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

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

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	**AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE**	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されます。	distinguishedName	False
AUTH_LDAP_PARSE_USERNAME	**AUTH_LDAP_PARSE_USERNAME**	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、DN はユーザー名に対して解析されます。false に設定した場合には、DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	true	False
AUTH_LDAP_USERNAME_BEGIN_STRING	**AUTH_LDAP_USERNAME_BEGIN_STRING**	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	–	False

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

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

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

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

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

5.2.2. オブジェクト

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

5.2.2.1. サービス

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

サービス	ポート	名前	説明
${APPLICATION_NAME}-rhdmcentr	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
${APPLICATION_NAME}-rhdmcentr-ping	8888	ping	rhdmcentr クラスターリングの JGroups ping ポート。
${APPLICATION_NAME}-datagrid-ping	8888	ping	クラスター化されたアプリケーションの ping サービスを提供します。
${APPLICATION_NAME}-datagrid	11222	hotrod	Hot Rod プロトコルでアプリケーションにアクセスするためのサービスを提供します。
${APPLICATION_NAME}-kieserver	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	
${APPLICATION_NAME}-amq-tcp	61616	–	ブローカーの OpenWire ポート。
ping	8888	–	amq クラスターリングの JGroups ping ポート。

5.2.2.2. ルート

ルートとは、**www.example.com** など、外部から到達可能なホスト名を指定して、サービスを公開する手段です。ルーターは、定義したルートや、サービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセレクター、セキュリティー設定 (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	セキュリティー	ホスト名
insecure-${APPLICATION_NAME}-rhdmcentr-http	なし	**${DECISION_CENTRAL_HOSTNAME_HTTP}**
${APPLICATION_NAME}-rhdmcentr-https	TLS パススルー	**${DECISION_CENTRAL_HOSTNAME_HTTPS}**
insecure-${APPLICATION_NAME}-kieserver-http	なし	**${KIE_SERVER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-kieserver-https	TLS パススルー	**${KIE_SERVER_HOSTNAME_HTTPS}**

5.2.2.3. 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。

5.2.2.3.1. 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
${APPLICATION_NAME}-rhdmcentr	ImageChange
${APPLICATION_NAME}-kieserver	ImageChange

5.2.2.3.2. 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、コンテナー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
${APPLICATION_NAME}-rhdmcentr	2
${APPLICATION_NAME}-kieserver	2

5.2.2.3.3. Pod テンプレート

5.2.2.3.3.1. 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
${APPLICATION_NAME}-rhdmcentr	**${APPLICATION_NAME}-rhdmsvc**
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-rhdmsvc**

5.2.2.3.3.2. イメージ

デプロイメント	イメージ
${APPLICATION_NAME}-rhdmcentr	**${DECISION_CENTRAL_IMAGE_STREAM_NAME}**
${APPLICATION_NAME}-kieserver	**${KIE_SERVER_IMAGE_STREAM_NAME}**

5.2.2.3.3.3. Readiness Probe

${APPLICATION_NAME}-rhdmcentr

> Http Get on http://localhost:8080/rest/ready

${APPLICATION_NAME}-kieserver

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

5.2.2.3.3.4. Liveness Probe

${APPLICATION_NAME}-rhdmcentr

> Http Get on http://localhost:8080/rest/healthy

${APPLICATION_NAME}-kieserver

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

5.2.2.3.3.5. 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
${APPLICATION_NAME}-rhdmcentr	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
	ping	8888	**TCP**
${APPLICATION_NAME}-kieserver	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**

5.2.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
${APPLICATION_NAME}-rhdmcentr	**APPLICATION_USERS_PROPERTIES**	–	**/opt/kie/data/configuration/application-users.properties**
	APPLICATION_ROLES_PROPERTIES	–	**/opt/kie/data/configuration/application-roles.properties**
	KIE_ADMIN_USER	KIE 管理者のユーザー名	**${KIE_ADMIN_USER}**
	KIE_ADMIN_PWD	KIE 管理者のパスワード	**${KIE_ADMIN_PWD}**
	KIE_MBEANS	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	**${KIE_MBEANS}**
	KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED	true に設定すると、KIE Server のグローバル検出機能はオンになります (org.kie.server.controller.openshift.global.discovery.enabled システムプロパティーを設定)。	**${KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED}**
	KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。(org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティーを設定します)	**${KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE}**
	KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL	KIE ServerTemplate Cache TTL (ミリ秒単位)。(org.kie.server.controller.template.cache.ttl システムプロパティーを設定)	**${KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL}**

デプロイメント	変数名	説明	値の例
	KIE_WORKBENCH_CONTROLLER_OPENSHIFT_ENABLED	–	true
	KIE_SERVER_CONTROLLER_USER	KIE サーバー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する)	**${KIE_SERVER_CONTROLLER_USER}**
	KIE_SERVER_CONTROLLER_PWD	KIE サーバーコントローラーのパスワード。(org.kie.server.controller.pwd システムプロパティーを設定する)	**${KIE_SERVER_CONTROLLER_PWD}**
	KIE_SERVER_CONTROLLER_TOKEN	ベアラー認証用の KIE Server コントローラートークン。(org.kie.server.controller.token システムプロパティーを設定)	**${KIE_SERVER_CONTROLLER_TOKEN}**
	KIE_SERVER_USER	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	**${KIE_SERVER_USER}**
	KIE_SERVER_PWD	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	**${KIE_SERVER_PWD}**
	WORKBENCH_ROUTE_NAME	–	**${APPLICATION_NAME}-rhdmcentr**
	MAVEN_MIRROR_URL	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	**${MAVEN_MIRROR_URL}**

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

デプロイメント	変数名	説明	値の例
	HTTPS_KEYSTORE	Decision Central のシークレット内のキーストアファイルの名前。	**${DECISION_CENTRAL_HTTPS_KEYSTORE}**
	HTTPS_NAME	Decision Central のサーバー証明書に関連付けられている名前。	**${DECISION_CENTRAL_HTTPS_NAME}**
	HTTPS_PASSWORD	Decision Central のキーストアおよび証明書のパスワード。	**${DECISION_CENTRAL_HTTPS_PASSWORD}**
	JGROUPS_PING_PROTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PING_SERVICE_NAME	–	**${APPLICATION_NAME}-rhdmcentr-ping**
	OPENSHIFT_DNS_PING_SERVICE_PORT	–	8888
	APPFORMER_INFINISPAN_SERVICE_NAME	–	**${APPLICATION_NAME}-datagrid**
	APPFORMER_INFINISPAN_PORT	–	11222
	APPFORMER_JMS_BROKER_ADDRESS	–	**${APPLICATION_NAME}-amq-tcp**
	APPFORMER_JMS_BROKER_PORT	–	61616
	APPFORMER_JMS_BROKER_USER	JMS ブローカーに接続するためのユーザー名	**${APPFORMER_JMS_BROKER_USER}**
	APPFORMER_JMS_BROKER_PASSWORD	JMS ブローカーに接続するためのパスワード。	**${APPFORMER_JMS_BROKER_PASSWORD}**
	SSO_URL	RH-SSO URL。	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO レルム名。	**${SSO_REALM}**

デプロイメント	変数名	説明	値の例
	SSO_SECRET	Decision Central RH-SSO クライアントシークレット。	**${DECISION_CENTRAL_SSO_SECRET}**
	SSO_CLIENT	Decision Central RH-SSO クライアント名。	**${DECISION_CENTRAL_SSO_CLIENT}**
	SSO_USERNAME	クライアント作成に使用する RH-SSO レルムの管理者のユーザー名 (存在しない場合)	**${SSO_USERNAME}**
	SSO_PASSWORD	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO が無効な SSL 証明書の検証。	**${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}**
	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	**${SSO_PRINCIPAL_ATTRIBUTE}**
	HOSTNAME_HTTP	Decision Central の 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は空白にします (例: insecure-<application-name>-rhdmcentr-<project>.<default-domain-suffix>)。	**${DECISION_CENTRAL_HOSTNAME_HTTP}**
	HOSTNAME_HTTPS	Decision Central の https サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr-<project>.<default-domain-suffix>)。	**${DECISION_CENTRAL_HOSTNAME_HTTPS}**

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

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

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

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

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

デプロイメント	変数名	説明	値の例
	KIE_SERVER_MODE	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナーでアーティファクトのバージョンを変更することはできません。(org.kie.server.mode システムプロパティーを設定)	**${KIE_SERVER_MODE}**
	KIE_MBEANS	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	**${KIE_MBEANS}**
	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスのフィルターリング。(org.drools.server.filter.classes システムプロパティーを設定)	**${DROOLS_SERVER_FILTER_CLASSES}**
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	**${PROMETHEUS_SERVER_EXT_DISABLED}**
	KIE_SERVER_BYPASS_AUTH_USER	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。(org.kie.server.bypass.auth.user システムプロパティーを設定)	**${KIE_SERVER_BYPASS_AUTH_USER}**
	KIE_SERVER_ID	–	–

デプロイメント	変数名	説明	値の例
	KIE_SERVER_ROUTE_NAME	–	**${APPLICATION_NAME}-kieserver**
	KIE_SERVER_STARTUP_STRATEGY	–	OpenShiftStartupStrategy
	KIE_SERVER_PWD	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	**${KIE_SERVER_PWD}**
	KIE_SERVER_USER	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	**${KIE_SERVER_USER}**
	MAVEN_MIRROR_URL	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	**${MAVEN_MIRROR_URL}**
	MAVEN_MIRROR_OF	KIE Server の Maven ミラー設定。	**${MAVEN_MIRROR_OF}**
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_ID	–	repo-rhdmcentr
	RHDMCENTR_MAVEN_REPO_SERVICE	–	**${APPLICATION_NAME}-rhdmcentr**
	RHDMCENTR_MAVEN_REPO_PATH	–	**/maven2/**
	RHDMCENTR_MAVEN_REPO_USERNAME	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	**${DECISION_CENTRAL_MAVEN_USERNAME}**

デプロイメント	変数名	説明	値の例
	RHDMCENTR_MAVEN_REPO_PASSWORD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	**${DECISION_CENTRAL_MAVEN_PASSWORD}**
	EXTERNAL_MAVEN_REPO_ID	Maven リポジトリーに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Maven リポジトリーまたはサービスへの完全修飾 URL。	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Maven リポジトリーにアクセスするユーザー名 (必要な場合)	**${MAVEN_REPO_USERNAME}**
	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリーにアクセスするパスワード (必要な場合)。	**${MAVEN_REPO_PASSWORD}**
	HTTPS_KEYSTORE_DIR	–	**/etc/kieserver-secret-volume**
	HTTPS_KEYSTORE	KIE Server のシークレット内のキーストアファイルの名前。	**${KIE_SERVER_HTTPS_KEYSTORE}**
	HTTPS_NAME	KIE Server のサーバー証明書に関連付けられている名前。	**${KIE_SERVER_HTTPS_NAME}**

デプロイメント	変数名	説明	値の例
	HTTPS_PASSWORD	KIE Server のキーストアおよび証明書のパスワード。	**${KIE_SERVER_HTTPS_PASSWORD}**
	SSO_URL	RH-SSO URL。	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO レルム名。	**${SSO_REALM}**
	SSO_SECRET	KIE Server の RH-SSO クライアントシークレット。	**${KIE_SERVER_SSO_SECRET}**
	SSO_CLIENT	KIE Server の RH-SSO クライアント名。	**${KIE_SERVER_SSO_CLIENT}**
	SSO_USERNAME	クライアント作成に使用する RH-SSO レルムの管理者のユーザー名 (存在しない場合)	**${SSO_USERNAME}**
	SSO_PASSWORD	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO が無効な SSL 証明書の検証。	**${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}**
	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	**${SSO_PRINCIPAL_ATTRIBUTE}**
	HOSTNAME_HTTP	KIE Server の http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>)。	**${KIE_SERVER_HOSTNAME_HTTP}**

デプロイメント	変数名	説明	値の例
	HOSTNAME_HTTPS	KIE Server の https 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>。	**${KIE_SERVER_HOSTNAME_HTTPS}**
	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント。	**${AUTH_LDAP_URL}**
	AUTH_LDAP_BIND_DN	認証に使用するバインド DN	**${AUTH_LDAP_BIND_DN}**
	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP の認証情報	**${AUTH_LDAP_BIND_CREDENTIAL}**
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	**${AUTH_LDAP_JAAS_SECURITY_DOMAIN}**
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	**${AUTH_LDAP_BASE_CTX_DN}**
	AUTH_LDAP_BASE_FILTER	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	**${AUTH_LDAP_BASE_FILTER}**
	AUTH_LDAP_SEARCH_SCOPE	使用する検索範囲。	**${AUTH_LDAP_SEARCH_SCOPE}**
	AUTH_LDAP_SEARCH_TIME_LIMIT	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	**${AUTH_LDAP_SEARCH_TIME_LIMIT}**

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されます。	**${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}**
	AUTH_LDAP_PARSE_USERNAME	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、 DN はユーザー名に対して解析されます。false に設定した場合には、 DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	**${AUTH_LDAP_PARSE_USERNAME}**
	AUTH_LDAP_USERNAME_BEGIN_STRING	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	**${AUTH_LDAP_USERNAME_BEGIN_STRING}**
	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	**${AUTH_LDAP_USERNAME_END_STRING}**
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前。	**${AUTH_LDAP_ROLE_ATTRIBUTE_ID}**

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

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

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

5.2.2.3.3.7. ボリューム

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

5.2.2.4. 外部の依存関係

5.2.2.4.1. 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
${APPLICATION_NAME}-rhdmcentr-claim	ReadWriteMany

5.2.2.4.2. 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

5.2.2.4.3. 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. **OPENSHIFT_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. **OPENSHIFT_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、(起動後でないと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. **OPENSHIFT_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. **OPENSHIFT_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5.1 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
```

5.3. RHDM75-KIESERVER.YAML TEMPLATE

Red Hat Decision Manager 7.5 での管理 KIE Server 向けのアプリケーションテンプレート (非推奨)

5.3.1. 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
APPLICATION_NAME	–	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
MAVEN_MIRROR_URL	**MAVEN_MIRROR_URL**	KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合には、このミラーにはサービスのデプロイに必要なすべてのアーティファクトを含める必要があります。	–	False
MAVEN_MIRROR_OF	**MAVEN_MIRROR_OF**	KIE Server の Maven ミラー設定。	external:*	False
MAVEN_REPO_ID	**EXTERNAL_MAVEN_REPO_ID**	Maven リポジトリーに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	repo-custom	False
MAVEN_REPO_URL	**EXTERNAL_MAVEN_REPO_URL**	Maven リポジトリーまたはサービスへの完全修飾 URL。	http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/	True

変数名	イメージの環境変数	説明	値の例	必須
MAVEN_REPO_USERNAME	**EXTERNAL_MAVEN_REPO_USERNAME**	Maven リポジトリーにアクセスするユーザー名 (必要な場合)	–	False
MAVEN_REPO_PASSWORD	**EXTERNAL_MAVEN_REPO_PASSWORD**	Maven リポジトリーにアクセスするパスワード (必要な場合)。	–	False
DECISION_CENTRAL_SERVICE	**WORKBENCH_SERVICE_NAME**	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリーの使用など) を許可するのに使用される任意の Decision Central のサービス名。	myapp-rhdmcentr	False
DECISION_CENTRAL_MAVEN_USERNAME	**RHDMCENTR_MAVEN_REPO_USERNAME**	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのユーザー名	mavenUser	False
DECISION_CENTRAL_MAVEN_PASSWORD	**RHDMCENTR_MAVEN_REPO_PASSWORD**	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	maven1!	False
KIE_ADMIN_USER	**KIE_ADMIN_USER**	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PWD	**KIE_ADMIN_PWD**	KIE 管理者のパスワード	–	False
KIE_SERVER_USER	**KIE_SERVER_USER**	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	executionUser	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_PWD	**KIE_SERVER_PWD**	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	–	False
IMAGE_STREAM_NAMESPACE	–	Red Hat Decision Manager イメージの ImageStream がインストールされている名前空間。これらの ImageStreams は通常 OpenShift の名前空間にインストールされています。ImageStreams を別の namespace/プロジェクトにインストールしている場合には、これを変更するだけで結構です。	openshift	True
KIE_SERVER_IMAGE_STREAM_NAME	–	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm-kieserver-rhel8 です。	rhdm-kieserver-rhel8	True
IMAGE_STREAM_TAG	–	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 7.5.0 です。	7.5.0	True

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_MODE	**KIE_SERVER_MODE**	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナーでアーティファクトのバージョンを変更することはできません。(org.kie.server.mode システムプロパティーを設定)	**PRODUCTION**	False
KIE_MBEANS	**KIE_MBEANS**	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	enabled	False
DROOLS_SERVER_FILTER_CLASSES	**DROOLS_SERVER_FILTER_CLASSES**	KIE Server クラスのフィルターリング。(org.drools.server.filter.classes システムプロパティーを設定)	true	False
PROMETHEUS_SERVER_EXT_DISABLED	**PROMETHEUS_SERVER_EXT_DISABLED**	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	false	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_HOSTNAME_HTTP	**HOSTNAME_HTTP**	http サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>)。	–	False
KIE_SERVER_HOSTNAME_HTTPS	**HOSTNAME_HTTPS**	https サービスルートのカスタムのホスト名。デフォルトホスト名の場合は空白にします (例: <application-name>-kieserver-<project>.<default-domain-suffix>。	–	False
KIE_SERVER_HTTPS_SECRET	–	キーストアファイルを含むシークレット名	kieserver-app-secret	True
KIE_SERVER_HTTPS_KEYSTORE	**HTTPS_KEYSTORE**	シークレット内のキーストアファイルの名前。	keystore.jks	False
KIE_SERVER_HTTPS_NAME	**HTTPS_NAME**	サーバー証明書に関連付けられている名前	jboss	False
KIE_SERVER_HTTPS_PASSWORD	**HTTPS_PASSWORD**	キーストアおよび証明書のパスワード。	mykeystorepass	False
KIE_SERVER_BYPASS_AUTH_USER	**KIE_SERVER_BYPASS_AUTH_USER**	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。(org.kie.server.bypass.auth.user システムプロパティーを設定)	false	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_MEMORY_LIMIT	–	KIE Server のコンテナーのメモリー制限。	1Gi	False
KIE_SERVER_CONTAINER_DEPLOYMENT	**KIE_SERVER_CONTAINER_DEPLOYMENT**	KIE Server コンテナーのデプロイメント設定。任意でエイリアスあり。形式: containerId=groupId:artifactId:version|c2(alias2)=g2:a2:v2	rhdm-kieserver-library=org.openshift.quickstarts:rhdm-kieserver-library:1.5.0-SNAPSHOT	False
KIE_SERVER_MGMT_DISABLED	**KIE_SERVER_MGMT_DISABLED**	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。org.kie.server.mgmt.api.disabled プロパティーを true に、org.kie.server.startup.strategy プロパティー を LocalContainersStartupStrategy に設定します。	true	False
SSO_URL	**SSO_URL**	RH-SSO URL。	https://rh-sso.example.com/auth	False
SSO_REALM	**SSO_REALM**	RH-SSO レルム名。	–	False
KIE_SERVER_SSO_CLIENT	**SSO_CLIENT**	KIE Server の RH-SSO クライアント名。	–	False
KIE_SERVER_SSO_SECRET	**SSO_SECRET**	KIE Server の RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False

変数名	イメージの環境変数	説明	値の例	必須
SSO_USERNAME	**SSO_USERNAME**	クライアント作成に使用する RH-SSO レルムの管理者のユーザー名 (存在しない場合)	–	False
SSO_PASSWORD	**SSO_PASSWORD**	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	**SSO_DISABLE_SSL_CERTIFICATE_VALIDATION**	RH-SSO が無効な SSL 証明書の検証。	false	False
SSO_PRINCIPAL_ATTRIBUTE	**SSO_PRINCIPAL_ATTRIBUTE**	ユーザー名として使用する RH-SSO プリンシパル属性	preferred_username	False
AUTH_LDAP_URL	**AUTH_LDAP_URL**	認証用に接続する LDAP エンドポイント。	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	**AUTH_LDAP_BIND_DN**	認証に使用するバインド DN	uid=admin,ou=users,ou=exmample,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	**AUTH_LDAP_BIND_CREDENTIAL**	認証に使用する LDAP の認証情報	パスワード	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	**AUTH_LDAP_JAAS_SECURITY_DOMAIN**	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	–	False
AUTH_LDAP_BASE_CTX_DN	**AUTH_LDAP_BASE_CTX_DN**	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	ou=users,ou=example,ou=com	False

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

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

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

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

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

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

5.3.2. 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。

5.3.2.1. 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、コンテナーエンジンのドキュメント を参照してください。

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

5.3.2.2. 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、サービスセレクター、セキュリティー設定 (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	セキュリティー	ホスト名
insecure-${APPLICATION_NAME}-kieserver-http	なし	**${KIE_SERVER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-kieserver-https	TLS パススルー	**${KIE_SERVER_HOSTNAME_HTTPS}**

5.3.2.3. 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。

5.3.2.3.1. 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
${APPLICATION_NAME}-kieserver	ImageChange

5.3.2.3.2. 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、コンテナー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
${APPLICATION_NAME}-kieserver	1

5.3.2.3.3. Pod テンプレート

5.3.2.3.3.1. 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
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**

5.3.2.3.3.2. イメージ

デプロイメント	イメージ
${APPLICATION_NAME}-kieserver	**${KIE_SERVER_IMAGE_STREAM_NAME}**

5.3.2.3.3.3. Readiness Probe

${APPLICATION_NAME}-kieserver

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

5.3.2.3.3.4. Liveness Probe

${APPLICATION_NAME}-kieserver

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

5.3.2.3.3.5. 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
${APPLICATION_NAME}-kieserver	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
	ping	8888	**TCP**

5.3.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
${APPLICATION_NAME}-kieserver	**WORKBENCH_SERVICE_NAME**	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリーの使用など) を許可するのに使用される任意の Decision Central のサービス名。	**${DECISION_CENTRAL_SERVICE}**

デプロイメント	変数名	説明	値の例
	KIE_ADMIN_USER	KIE 管理者のユーザー名	**${KIE_ADMIN_USER}**
	KIE_ADMIN_PWD	KIE 管理者のパスワード	**${KIE_ADMIN_PWD}**
	KIE_SERVER_MODE	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナーでアーティファクトのバージョンを変更することはできません。(org.kie.server.mode システムプロパティーを設定)	**${KIE_SERVER_MODE}**
	KIE_MBEANS	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	**${KIE_MBEANS}**
	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスのフィルターリング。(org.drools.server.filter.classes システムプロパティーを設定)	**${DROOLS_SERVER_FILTER_CLASSES}**
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定すると、prometheus サーバー拡張が有効になります。(org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	**${PROMETHEUS_SERVER_EXT_DISABLED}**
	KIE_SERVER_BYPASS_AUTH_USER	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。(org.kie.server.bypass.auth.user システムプロパティーを設定)	**${KIE_SERVER_BYPASS_AUTH_USER}**
	KIE_SERVER_ID	–	–

デプロイメント	変数名	説明	値の例
	KIE_SERVER_ROUTE_NAME	–	**${APPLICATION_NAME}-kieserver**
	KIE_SERVER_USER	KIE サーバーのユーザー名。(org.kie.server.user システムプロパティーを設定する)	**${KIE_SERVER_USER}**
	KIE_SERVER_PWD	KIE サーバーのパスワード。(org.kie.server.pwd システムプロパティーを設定する)	**${KIE_SERVER_PWD}**
	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE Server コンテナーのデプロイメント設定。任意でエイリアスあり。形式: containerId=groupId:artifactId:version|c2(alias2)=g2:a2:v2	**${KIE_SERVER_CONTAINER_DEPLOYMENT}**
	MAVEN_MIRROR_URL	KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合には、このミラーにはサービスのデプロイに必要なすべてのアーティファクトを含める必要があります。	**${MAVEN_MIRROR_URL}**
	MAVEN_MIRROR_OF	KIE Server の Maven ミラー設定。	**${MAVEN_MIRROR_OF}**
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_ID	–	repo-rhdmcentr
	RHDMCENTR_MAVEN_REPO_SERVICE	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリーの使用など) を許可するのに使用される任意の Decision Central のサービス名。	**${DECISION_CENTRAL_SERVICE}**
	RHDMCENTR_MAVEN_REPO_PATH	–	**/maven2/**

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

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

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

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

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_PARSE_USERNAME	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定した場合には、 DN はユーザー名に対して解析されます。false に設定した場合には、 DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	**${AUTH_LDAP_PARSE_USERNAME}**
	AUTH_LDAP_USERNAME_BEGIN_STRING	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	**${AUTH_LDAP_USERNAME_BEGIN_STRING}**
	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	**${AUTH_LDAP_USERNAME_END_STRING}**
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前。	**${AUTH_LDAP_ROLE_ATTRIBUTE_ID}**
	AUTH_LDAP_ROLES_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	**${AUTH_LDAP_ROLES_CTX_DN}**

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

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

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

5.3.2.3.3.7. ボリューム

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

5.3.2.4. 外部の依存関係

5.3.2.4.1. 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

5.4. OPENSHIFT の使用に関するクイックリファレンス

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

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

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

- プロジェクトを作成するには、以下のコマンドを使用します。

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

詳細は、CLI を使用したプロジェクトの作成 を参照してください。

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

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

詳細は、CLI を使用したアプリケーションの作成 を参照してください。

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

```
$ oc get pods
```

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

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

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

- Pod のログを表示するには、以下のコマンドを使用します。

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

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

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

詳細は、デプロイメントログの表示 を参照してください。

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

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

詳細は、ビルドログのアクセス を参照してください。

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

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

詳細は、手動スケーリング を参照してください。

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

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

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

付録A バージョン情報

本書の最終更新日: 2021 年 11 月 15 日 (月)