



Red Hat Decision Manager 7.6

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

Red Hat Decision Manager 7.6 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

Red Hat Customer Content Services

brms-docs@redhat.com

法律上の通知

Copyright © 2020 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

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

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

概要

本書では、Red Hat Decision Manager 7.6 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

前書き	4
第1章 RED HAT OPENSIFT CONTAINER PLATFORM における RED HAT DECISION MANAGER の概要	6
第2章 OPENSIFT 環境への RED HAT DECISION MANAGER のデプロイの準備	8
2.1. イメージストリームとイメージレジストリーが利用可能であることの確認	8
2.2. DECISION SERVER のシークレットの作成	9
2.3. BUSINESS CENTRAL へのシークレットの作成	10
2.4. オフラインで使用する MAVEN ミラーリポジトリーの準備	10
2.5. GLUSTERFS 設定の変更	12
2.6. NFS を使用した READWRITEMANY アクセスモードの永続ボリュームのプロビジョニング	13
第3章 オーサリングまたは管理サーバー環境	15
3.1. オーサリング環境のデプロイメント	16
3.1.1. オーサリング環境用のテンプレートの設定を開始する	16
3.1.2. オーサリング環境に必要なパラメーターの設定	17
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	18
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	18
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	19
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	20
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	20
3.1.8. 高可用性デプロイメントのリソース使用状況の設定	21
3.1.9. オーサリング環境用の RH-SSO 認証パラメーターの設定	21
3.1.10. オーサリング環境用の LDAP 認証パラメーターの設定	23
3.1.11. オーサリング環境用の Prometheus メトリクス収集の有効化	24
3.1.12. オーサリング環境用テンプレートのデプロイの実行	25
3.2. (オプション) GIT フックディレクトリーの指定	25
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	27
3.3.1. 追加の管理 Decision Server テンプレート設定の開始	27
3.3.2. 追加の管理 Decision Server に必要なパラメーターの設定	28
3.3.3. 追加の管理 Decision Server のイメージストリーム namespace の設定	29
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	29
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	30
3.3.6. 追加の管理 Decision Server の RH-SSO 認証パラメーターの設定	31
3.3.7. 追加の管理 Decision Server の LDAP 認証パラメーターの設定	33
3.3.8. 追加の管理 Decision Server の Prometheus メトリクス収集の有効化	34
3.3.9. 追加の管理 Decision Server テンプレートデプロイの開始	34
3.4. (オプション) LDAP ロールマッピングファイルの指定	34
第4章 RED HAT DECISION MANAGER ロールおよびユーザー	36
第5章 OPENSIFT テンプレートの参考資料	37
5.1. RHDM76-AUTHORING.YAML テンプレート	37
5.1.1. パラメーター	37
5.1.2. オブジェクト	52
5.1.2.1. サービス	52
5.1.2.2. ルート	53
5.1.2.3. デプロイメント設定	53
5.1.2.3.1. トリガー	53
5.1.2.3.2. レプリカ	53
5.1.2.3.3. Pod テンプレート	54

5.1.2.3.3.1. サービスアカウント	54
5.1.2.3.3.2. イメージ	54
5.1.2.3.3.3. Readiness プローブ	54
5.1.2.3.3.4. Liveness プローブ	54
5.1.2.3.3.5. 公開されたポート	55
5.1.2.3.3.6. イメージの環境変数	55
5.1.2.3.3.7. ボリューム	73
5.1.2.4. 外部の依存関係	74
5.1.2.4.1. ボリューム要求	74
5.1.2.4.2. シークレット	74
5.2. RHDM76-AUTHORING-HA.YAML テンプレート	74
5.2.1. パラメーター	74
5.2.2. オブジェクト	91
5.2.2.1. サービス	91
5.2.2.2. ルート	92
5.2.2.3. デプロイメント設定	92
5.2.2.3.1. トリガー	93
5.2.2.3.2. レプリカ	93
5.2.2.3.3. Pod テンプレート	93
5.2.2.3.3.1. サービスアカウント	93
5.2.2.3.3.2. イメージ	93
5.2.2.3.3.3. Readiness プローブ	94
5.2.2.3.3.4. Liveness プローブ	94
5.2.2.3.3.5. 公開されたポート	94
5.2.2.3.3.6. イメージの環境変数	94
5.2.2.3.3.7. ボリューム	113
5.2.2.4. 外部の依存関係	113
5.2.2.4.1. ボリューム要求	113
5.2.2.4.2. シークレット	114
5.2.2.4.3. クラスタリング	114
5.3. RHDM76-KIESERVER.YAML テンプレート	115
5.3.1. パラメーター	115
5.3.2. オブジェクト	128
5.3.2.1. サービス	128
5.3.2.2. ルート	129
5.3.2.3. デプロイメント設定	129
5.3.2.3.1. トリガー	129
5.3.2.3.2. レプリカ	129
5.3.2.3.3. Pod テンプレート	129
5.3.2.3.3.1. サービスアカウント	129
5.3.2.3.3.2. イメージ	130
5.3.2.3.3.3. Readiness プローブ	130
5.3.2.3.3.4. Liveness プローブ	130
5.3.2.3.3.5. 公開されたポート	130
5.3.2.3.3.6. イメージの環境変数	130
5.3.2.3.3.7. ボリューム	140
5.3.2.4. 外部の依存関係	140
5.3.2.4.1. シークレット	140
5.4. OPENSIFT の使用に関するクイックリファレンス	140
付録A バージョン情報	143

前書き

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

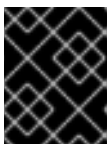
- Red Hat OpenShift Container Platform バージョン 3.11 がデプロイされている。
- OpenShift クラスター/namespace で 4 ギガバイト以上のメモリーが利用可能である。
- 高可用性のデプロイメントでは、以下のリソースが OpenShift クラスターで利用可能である。
 - Business Central で複製された Pod の場合、8 ギガバイトのメモリーと 2 CPU コアが各レプリカに必要です。デフォルトで 2 つのレプリカが作成されます。
 - Decision Server で複製された Pod の場合、1 ギガバイトのメモリーと 1 CPU コアが各レプリカに必要です。デフォルトで 2 つのレプリカが作成されます。
 - Red Hat Data Grid で複製された Pod の場合、2 ギガバイトのメモリーと 1 CPU コアが各レプリカに必要です。デフォルトで 2 つのレプリカが作成されます。
 - Red Hat AMQ で複製された Pod は、クラスターに設定されたデフォルトのリソース制限を使用します。



注記

クラスターの容量を確認する方法については、Red Hat OpenShift Container Platform 3.11 製品ドキュメントの「[クラスター容量の分析](#)」を参照してください。

- デプロイメントする 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 [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を有効にしている。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 サイズを変更できます。
- 高可用性 Business Central を含む高可用性オーサリング環境をデプロイする場合、OpenShift 環境は **ReadWriteMany** モードの永続ボリュームをサポートします。ご使用の環境がこのモードに対応していない場合、NFS を使用してボリュームをプロビジョニングできます。ただし、パフォーマンスと信頼性を最大化するには、GlusterFS を使用して、高可用性オーサリング環境用に永続ボリュームをプロビジョニングします。OpenShift Online ボリュームプラグインにおけるアクセスモードのサポートについては、「[アクセスモード](#)」を参照してください。



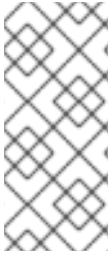
重要

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、Red Hat OpenShift Container Platform 3.x のサポートは非推奨となっています。これには、Red Hat Decision Manager のインストールに使用するテンプレートも含まれます。この機能は今後のリリースで削除されます。



注記

Red Hat Decision Manager テンプレートを Red Hat OpenShift Container Platform 4.x と共に使用しないでください。Red Hat Decision Manager を Red Hat OpenShift Container Platform 4.x にデプロイするには、『[Deploying a Red Hat Decision Manager environment on Red Hat OpenShift Container Platform using Operators](#)』の説明を参照してください。

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

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

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

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

- **Decision Server (実行サーバー (Execution Server) または KIE Server と呼ばれる)** は、デジジョンサービスおよびその他のデプロイ可能なアセット (サービス と総称される) を実行するインフラストラクチャー要素です。サービスの全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 をスケールアップまたはスケールダウンすると、そのコピーはすべて同じサービスを実行します。OpenShift には負荷分散機能があり、要求はいずれかの Pod で処理されます。

Decision Server Pod を個別にデプロイし、サービスの異なる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使用される Web ベースのインタラクティブな環境です。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 は一元化されたアプリケーションですが、複数の Pod を実行して同一データを共有する、高可用性の設定が可能です。

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

これらのコンポーネントおよびその他のコンポーネントを OpenShift 内の各種の環境設定に配置できます。

以下は、通常的环境タイプです。

- **オーサリングまたは管理環境:** Business Central を使用してサービスを作成および変更し、サービスを Decision Server で実行するために使用できる環境アーキテクチャーです。この環境は、オーサリング用の Business Central を提供する Pod と、サービス実行用の 1 つ以上の Decision Server を提供する Pod で構成されます。それぞれの Decision Server が 1 つの Pod となり、Pod はスケールアップまたはスケールダウンを随時実行して複製できます。Business Central を使用して、それぞれの Decision Server で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、『[Deploying a Red Hat Decision Manager authoring or managed server environment on Red Hat OpenShift Container Platform](#)』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、Decision Server Pod のデプロイ時に、サービスまたはサービスのグループをロードし、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 Pod のように実行されるので、任意のコンテナベースの統合ワークフローを使用することができ、他のツールを使用して Pod を管理する必要はありません。この環境のデプロイメント手順については、『[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、『[Deploying a Red Hat Decision Manager trial environment on Red Hat OpenShift Container Platform](#)』を参照してください。

Red Hat Decision Manager 環境を OpenShift にデプロイするには、Red Hat Decision Manager で提供される OpenShift テンプレートを使用できます。

第2章 OPENSIFT 環境への RED HAT DECISION MANAGER のデプロイの準備

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、または他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が利用可能であることの確認

Red Hat Decision Manager コンポーネントを Red Hat OpenShift Container Platform にデプロイするには、OpenShift が Red Hat レジストリーから適切なイメージをダウンロードできることを確認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 レジストリーで認証でき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には、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のユーザー名とパスワードで設定されているかどうかを判別します。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 Online サブスクリプションを使用している場合は、Red Hat レジストリーへのアクセス用の設定はすでに行われています。
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 rhdm76-decisioncentral-openshift
$ oc get imagestreamtag -n openshift | grep rhdm76-kieserver-openshift
```

両方のコマンドの出力が空でない場合、必要なイメージストリームは **openshift** namespace で利用可能な状態であるため、追加の操作は必要ありません。

3. コマンドのいずれかまたは両方の出力が空の場合や、OpenShift 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ない場合には、以下の手順を実行してください。
 - a. **oc** コマンドで OpenShift にログインしており、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](#)」に記載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:** エントリーに一覧表示されている名前をメモします。
- 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の名前に、<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-7.6.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードし、**rhdm76-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 rhdm76-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プロジェクトの namespace にインストールします。この場合、テンプレートをデプロイする際に **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 の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 暗号化向けの秘密鍵と公開鍵で 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. **keystore.jks** という名前のファイルにキーストアを保存します。
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の値は **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. Decision Server の SSL 暗号化向けの秘密鍵と公開鍵で 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 Business Central の URL と一致する、有効な署名済み証明書を生成します。

2. **keystore.jks** という名前のファイルにキーストアを保存します。
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の値は **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 **decisioncentral-app-secret** という名前のシークレットを生成します。

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

2.4. オフラインで使用する MAVEN ミラーリポジトリの準備

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



注記

Red Hat OpenShift Container Platform 環境がインターネットに接続されている場合にはこの手順を実行する必要はありません。

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可能であること。

手順

1. 書き込み可能な Maven リリースリポジトリを準備します。このリポジトリは、認証なしに読み込みアクセスができるようにする必要があります。OpenShift 環境は、このリポジトリへのアクセスが必要です。OpenShift 環境に、Nexus リポジトリマネージャーをデプロイできます。OpenShift への Nexus の設定方法は、「[Nexus の設定](#)」を参照してください。このリポジトリを別個のミラーリポジトリとして使用します。または、サービスにカスタムの外部リポジトリ (Nexus など) を使用する場合、同じリポジトリをミラーリポジトリ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、以下の手順を実行します。

- a. 最新版の [Offliner ツール](#) 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-7.6.0-offliner.txt** の製品配信可能ファイルをダウンロードします。
- c. 以下のコマンドを入力して Offliner ツールを使用し、必要なアーティファクトをダウンロードします。

```
java -jar offliner-<version>.jar -r https://maven.repository.redhat.com/ga/ -r  
https://repo1.maven.org/maven2/ -d /home/user/temp rhdm-7.6.0-offliner.txt
```

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

- d. 一時ディレクトリーから作成した Maven ミラーリポジトリにすべてのアーティファクトをアップロードします。アーティファクトのアップロードには、[Maven Repository Provisioner](#) 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には、ミラーリポジトリにその依存関係を追加します。サービスを Maven プロジェクトとして作成している場合には、以下の手順を使用すると、これらの依存関係を自動的に準備できます。公開インターネットへの送信接続のあ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について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 Repository Provisioner](#) 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
```

結果で、**(default)** マーカーが、**glusterfs** を一覧表示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、以下の出力では、デフォルトのストレージクラスは **gluster-container** であり、**glusterfs** を一覧表示します。

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

結果に **glusterfs** を一覧表示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、変更する必要はありません。変更しない場合は、以下の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。以下は、例になります。

```
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、高可用性設定なしの、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
```

以下は例になります。

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
```

以下は例になります。

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。以下は、例になります。

```
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
```

2.6. NFS を使用した READWRITEMANY アクセスモードの永続ボリュームのプロビジョニング

高可用性 Business Central をデプロイする場合には、ご使用の環境は **ReadWriteMany** アクセスモードで永続ボリュームをプロビジョニングする必要があります。



注記

高可用性オーサリング環境をデプロイする場合、パフォーマンスと信頼性を最大化するには、GlusterFS を使用して永続ボリュームをプロビジョニングします。「[GlusterFS 設定の変更](#)」の説明に従って GlusterFS ストレージクラスを設定します。

お使いの設定で **ReadWriteMany** アクセスモードの永続ボリュームのプロビジョニングが必要であるものの、環境がそのようなプロビジョニングに対応しない場合、NFS を使用してボリュームをプロビジョニングします。それ以外の場合は、この手順は省略します。

手順

NFS サーバーをデプロイし、NFS を使用して永続ボリュームをプロビジョニングします。NFS を使用して永続ボリュームをプロビジョニングする方法については、『[クラスターの設定](#)』の「NFS を使用した永続ストレージ」を参照してください。

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環境をデプロイできます。この環境は、Business Central と1つまたは複数の Decision Server で構成されます。

Business Central を使用するとサービスの開発や Decision Server へのデプロイを実行できます。複数の Decision Server を Business Central に接続して、各サーバーへのサービスのデプロイを管理することができます。

必要な場合は、別個の環境を作成して Business Central の1つのデプロイメントを使用してサービスのオーサリングを行い (オーサリング環境)、Business Central のもう1つのデプロイメントを使用して複数 Decision Server のステージングまたは実稼働サーバーのデプロイメントを管理できます (管理サーバー環境)。通常は、1つの専用オーサリング環境には1つの Decision Server があれば十分です。外部 Maven リポジトリを使用してオーサリング環境のサービスを保存し、それらを別個の管理サーバー環境にデプロイできます。

Red Hat Decision Manager では、オーサリング環境と管理サーバー環境のデプロイの手順は同じです。最初に、Business Central と1つの Decision Server で構成されるオーサリング環境テンプレートをデプロイする必要があります。

必要な場合は、追加の Decision Server テンプレートを同じ namespace にデプロイし、複数の Decision Server を含む環境を作成できます。この環境は、サービスのステージングおよび実稼働のデプロイメント用に管理サーバー環境にすることができます。

必要に応じて、単一のオーサリング環境テンプレートまたは高可用性 (HA) オーサリング環境テンプレートのいずれかをデプロイできます。

単一のオーサリング環境には2つの Pod が含まれます。それらの Pod の1つは Business Central であり、もう1つは Decision Server を実行します。この環境は、単一ユーザーのオーサリングや、OpenShift インフラストラクチャーのリソースが制限されている場合に最も適しています。

HA オーサリング環境では、Business Central および Decision Server の両方がスケーラブルな Pod で提供されます。Pod をスケーリングすると、永続ストレージはコピー間で共有されます。Business Central で高可用性機能を有効にするには、AMQ および Data Grid を含む追加の Pod が必要です。これらの Pod は高可用性オーサリングテンプレートで設定され、デプロイされます。高可用性オーサリング環境を使用すると、複数のユーザーが同時にオーサリングを行っている場合などはとくに、信頼性と応答性を最大化できます。

Red Hat Decision Manager の現行バージョンでは、HA オーサリング環境は特定の制限付きでサポートされています。

- Business Central Pod がユーザーがそれを使用している間にクラッシュする場合、ユーザーにはエラーメッセージが送られ、ユーザーは別の Pod にリダイレクトされます。この場合、再度ログインする必要はありません。
- ユーザーの操作時に Business Central Pod がクラッシュする場合、コミット (保存) されていないデータが失われる可能性があります。
- プロジェクトの作成時に Business Central Pod がクラッシュする場合、使用できないプロジェクトが作成される可能性があります。
- アセットの作成時に Business Central Pod がクラッシュする場合、アセットは作成されるものの、インデックス化されず使用できない可能性があります。ユーザーは Business Central でアセットを開き、再度保存してインデックス化することができます。

もう1つの制限も、すべてのオーサリングおよび管理環境デプロイメントに適用されます。ユーザーがサービスを Decision Server にデプロイする場合、初回のデプロイメントが完了するまで別のサービスを同じ Decision Server にデプロイすることはできません。

必要な場合には、追加の管理またはイミュータブル Decision Server をデプロイすることもできます。Business Central は、イミュータブル Decision Server および管理 Decision Server を含む Decision Server を同じ namespace で自動的に検出できます。この機能には、デフォルトですべての Decision Server に有効にされる **OpenShiftStartupStrategy** 設定が必要です。管理 Decision Server のデプロイメント方法については、「[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](#)」を参照してください。イミュータブル Decision Server のデプロイメント方法については、『[Deploying a Red Hat Decision Manager immutable server environment on Red Hat OpenShift Container Platform](#)』を参照してください。

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 で構成されます。

3.1.1. オーサリング環境用のテンプレートの設定を開始する

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、**rhdm76-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、**rhdm76-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での [Software Downloads](#) ページから利用可能な **rhdm-7.6.0-openshift-templates.zip** の製品配信可能ファイル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>/<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、テンプレートファイルの名前に置き換えます。
- 必要なパラメーターを設定するために必要な数の **-p PARAMETER = value** のペアを使用します。

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](#)」の手順を実行し、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、すべてのパラメーターの説明を参照できます。

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、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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

1. 以下のパラメーターを設定します。
 - **Business Central Server Keystore Secret Name (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 Keystore Secret Name (KIE_SERVER_HTTPS_SECRET):** 「[Decision Server の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 Server Certificate Name (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 Server Keystore Password (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 の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 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。
 - **Application Name (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 で使用されません。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別個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 namespace (IMAGE_STREAM_NAMESPACE):** イメージストリームが利用可能な namespace。OpenShift 環境でイメージストリームがすでに利用可能な場合（「[イメージストリームとイメージレジストリーが利用可能であることの確認](#)」を参照）、

namespace は **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、namespace が OpenShift プロジェクトの名前になります。

- 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 namespace でイメージストリームを作成した場合、テンプレートで namespace 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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

「[イメージストリームとイメージレジストリーが利用可能であることの確認](#)」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場合、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、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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

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 repository URL (MAVEN_REPO_URL)**: Maven リポジトリーの URL。

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

次のステップ

必要な場合は、追加のパラメーターを設定します。

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

3.1.5. オーサリング環境のビルドイン Maven リポジトリ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。

RH-SSO または LDAP 認証を設定する場合には、ビルトインの Maven リポジトリの認証情報は、RH-SSO または LDAP で指定したユーザー名とパスワードに、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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

ビルトイン Maven リポジトリ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。

- **Username for the Maven service hosted by Business Central (DECISION_CENTRAL_MAVEN_USERNAME)**: ビルトインの Maven リポジトリのユーザー名。
- **Password for the Maven service hosted by Business Central (DECISION_CENTRAL_MAVEN_PASSWORD)**: ビルトインの Maven リポジトリのパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[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 ミラーリポジトリの準備](#)」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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

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 mirror URL (MAVEN_MIRROR_URL)**: 「[オフラインで使用する Maven ミラーリポジトリの準備](#)」で設定した Maven ミラーリポジトリの URL。この URL は OpenShift 環境の Pod からアクセスできる必要があります。
- **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** 値の設定方法については、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 (**MAVEN_REPO_URL**) を設定するには、このリポジトリのアーティファクトを除外するように **MAVEN_MIRROR_OF** を変更します (例: **external:*,!repo-custom**)。 **repo-custom** を **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 リポジトリと外部 Git リポジトリの対話を容易にすることができます。

Git フックを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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

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 hooks directory (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指定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、マウントする方法については、「[\(オプション\) 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. 高可用性デプロイメントのリソース使用状況の設定

高可用性テンプレート (`rhdm76-authoring-ha.yaml`) をデプロイしている場合、要件に合わせてパフォーマンスを最適化するためにリソースの使用をオプションで設定することができます。

単一オーサリング環境テンプレート (`rhdm76-authoring.yaml`) をデプロイしている場合は、この手順を省略してください。

リソースのサイジングについての詳細は、Red Hat OpenShift Container Platform 3.11 の製品ドキュメントの以下のセクションを参照してください。

- [アプリケーションメモリーのサイジング](#)
- [コンピュータリソース](#)

前提条件

- 「[オーサリング環境用のテンプレートの設定を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

以下のパラメーターをテンプレートに設定します (該当する場合)。

- **Business Central Container Memory Limit(DECISION_CENTRAL_MEMORY_LIMIT):** Business Central コンテナについて OpenShift 環境で必要とされるメモリー量。デフォルト値は **8Gi** です。
- **Business Central JVM Max Memory Ratio (DECISION_CENTRAL_JAVA_MAX_MEM_RATIO):** Business Central の Java Virtual Machine に使用されるコンテナメモリーのパーセンテージ。残りのメモリーはオペレーティングシステムに使用されます。デフォルト値は 80% を制限値として **80** になります。
- **Business Central Container CPU Limit(DECISION_CENTRAL_CPU_LIMIT):** Business Central の CPU 使用の最大値。デフォルト値は **2000m** です。
- **KIE Server Container Memory Limit(KIE_SERVER_MEMORY_LIMIT):** Decision Server コンテナについて OpenShift 環境で必要とされるメモリー量。デフォルト値は **1Gi** です。
- **KIE Server Container CPU Limit(KIE_SERVER_CPU_LIMIT):** Decision Server の CPU 使用の最大値。デフォルト値は **1000m** です。
- **DataGrid Container Memory Limit(DATAGRID_MEMORY_LIMIT):** Red Hat Data Grid コンテナについて OpenShift 環境で必要とされるメモリー量。デフォルト値は **2Gi** です。
- **DataGrid Container CPU Limit(DATAGRID_CPU_LIMIT):** Red Hat Data Grid の CPU 使用の最大値。デフォルト値は **1000m** です。

3.1.9. 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لمムが RH-SSO 認証システムに作成されていること。
- 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こと。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、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。
- クライアントが、デプロイしている Red Hat Decision Manager 環境のすべてのコンポーネントについて RH-SSO 認証システムに作成されていること。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 デプロイメントは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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

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 Realm name (SSO_REALM)**: Red Hat Decision Manager の RH-SSO レلمム。
 - **RH-SSO Disable SSL Certificate Validation (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には **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 Client name (DECISION_CENTRAL_SSO_CLIENT)**

- **Business Central RH-SSO Client name(DECISION_CENTRAL_SSO_CLIENT):** Business Central の RH-SSO クライアント名。
 - **Business Central RH-SSO Client Secret(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 RH-SSO Client name(KIE_SERVER_SSO_CLIENT):** Decision Server の RH-SSO クライアント名。
 - **KIE Server RH-SSO Client Secret(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 Client name(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 Client Secret(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 RH-SSO Client name(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 RH-SSO Client Secret(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 Realm Admin Username(SSO_USERNAME) および RH-SSO Realm Admin Password (SSO_PASSWORD):** Red Hat Decision Manager の RH-SSO レルムのレルム管理者ユーザーのユーザー名およびパスワード。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

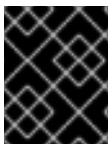
必要な場合は、追加のパラメーターを設定します。

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。

3.1.10. 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、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おく。利用可能なロールの一覧は、[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、最低でも以下のユーザーを作成します。

- **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を開始する](#)」 に説明されているテンプレートの設定を開始していること。

手順

- 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。
- 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。これらの設定の使用方法については、「[LdapExtended login module](#)」を参照してください。
LDAP サーバーでデプロイメントに必要なすべてのロールが定義されていない場合には、Red Hat Decision Manager ロールに LDAP グループをマップできます。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 file path (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、「[\(オプション\) 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 property (AUTH_ROLE_MAPPER_REPLACE_ROLE)**: **true** に設定されている場合には、LDAP サーバーに定義したロールは、マップされたロールに置き換えられます。**false** に設定されている場合、マップされたロールおよび LDAP サーバーに定義され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。

3.1.11. 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を開始する](#)」に説明されているテンプレートの設定を開始していること。

手順

Prometheus メトリクス収集のサポートを有効にするには、**Prometheus Server Extension Disabled (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、「[Managing and monitoring Decision Server](#)」を参照してください。

3.1.12. 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に必要なすべてのパラメーターを設定した後に、テンプレートのデプロイを実行します。

手順

使用している方法に応じて、以下の手順を実行します。

- OpenShift Web UI で、**Create** をクリックします。
 - 「**This will create resources that may have security or project behavior implications**」というポップアップメッセージが表示された場合には、**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する場合、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。

通常 Git フックはアップストリーム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. アップストリームリポジトリーにコミットをプッシュする必要がある場合には、以下の手順を実行して、リポジトリーへのアクセスを有効にします。
 - a. **id_rsa** という名前の秘密鍵と **id_rsa.pub** という名前の公開鍵のペアを作成します。アップストリームリポジトリーにアクセスできるメールアドレスを使用します。空のパスフレーズを設定します。これを実行する方法については、「[Generating a new SSH key](#)」を参照してください。
 - b. 公開鍵をアップストリームリポジトリーにアップロードします。
 - c. 秘密鍵から **rhdm-centr-gitkey** という名前の OpenShift シークレットを作成します。

```
oc create secret generic --from-file=id_rsa=id_rsa rhdm-centr-gitkey
```

- d. 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 rhdm-centr-gitkey --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。これを実行する方法については、[Git hooks reference ドキュメント](#)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から Business Central にインポートされた場合には、このリポジトリはアップストリームリポジトリ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には、設定マップを使用します。以下の手順を実行します。

- i. 作成した Git フックディレクトリーに切り替えます。

- ii. このディレクトリー内のファイルから OpenShift 設定マップを作成し、以下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。以下は例になります。

```
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構成されているか、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、そのボリュームを要求に関連付けてから、ファイルをその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します (**myapp** は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については、「[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については、「[Transferring files in and out of containers](#)」を参照してください。

- 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ため、Decision Server は全く起動されない可能性があります。Decision 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、これを起動します。

```
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または外部リポジトリのいずれかを使用するように設定する必要があります。

サーバーはロードされるサービスが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、**rhdm76-kieserver.yaml** テンプレートファイルを使用します。

手順

- Red Hat カスタマーポータルでの [Software Downloads](#) ページから利用可能な **rhdm-7.6.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードします。
- rhdm76-kieserver.yaml** テンプレートファイルを展開します。
- 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、**rhdm76-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>/rhdm76-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を設定するために必要な数の **-p PARAMETER = value** のペアを使用します。

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](#)」の手順を実行し、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参照できます。

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こと。

手順

1. 以下のパラメーターを設定します。

- **KIE Server Keystore Secret Name(KIE_SERVER_HTTPS_SECRET)**: 「[Decision Server の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 の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 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。
- **Application Name (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できます。別々のアプリケーション名を使用する限り、同じテンプレートを使用して複数のアプリケーションを同じプロジェクトにデプロイできます。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 をデプロイしている場合、それぞれのサーバーに異なるアプリケーション名があることを確認する必要があります。
- **KIE Server Mode(KIE_SERVER_MODE)**: `rhdm76-kieserver.yaml` テンプレートで、デフォルト値は **PRODUCTION** です。**PRODUCTION** モードでは、**SNAPSHOT** バージョンの KJAR アーティファクトは Decision Server にデプロイできず、既存のコンテナでアーティファクトのバージョンを変更することはできません。**PRODUCTION** モードで新規バージョンをデプロイするには、同じ Decision Server で新規コンテナを作成します。**SNAPSHOT** バージョンをデプロイするか、または既存コンテナのアーティファクトのバージョンを変更するには、このパラメーターを **DEVELOPMENT** に設定します。
- **ImageStream namespace (IMAGE_STREAM_NAMESPACE)**: イメージストリームが利用可能な namespace。OpenShift 環境でイメージストリームがすでに利用可能な場合 (「[イメージストリームとイメージレジストリーが利用可能であることの確認](#)」を参照)、namespace は **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、namespace が OpenShift プロジェクトの名前になります。

- 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 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](#)」に記載の手順を実行します。

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 namespace でイメージストリームを作成した場合、テンプレートで namespace 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こと。

手順

「[イメージストリームとイメージレジストリーが利用可能であることの確認](#)」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こと。

手順

- 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。

- **Name of the Business Central service(DECISION_CENTRAL_SERVICE):** Business Central の OpenShift サービス名。
2. サーバーがサービスのロードに使用する Maven リポジトリ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を使用する場合、以下のパラメーターを設定します。
 - **Name of the Maven service hosted by Business Central (DECISION_CENTRAL_MAVEN_SERVICE):** Business Central の OpenShift サービス名。
 - **Username for the Maven service hosted by Business Central (DECISION_CENTRAL_MAVEN_USERNAME):** Business Central のビルドイン Maven リポジトリのユーザー名。Business Central に **DECISION_CENTRAL_MAVEN_USERNAME** として設定したユーザー名を入力します。
 - **Password to access the Maven service hosted by Business Central (DECISION_CENTRAL_MAVEN_PASSWORD):** Business Central のビルドイン Maven リポジトリのパスワード。Business Central に **DECISION_CENTRAL_MAVEN_PASSWORD** として設定したパスワードを入力します。
 - Business Central を外部 Maven リポジトリ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 repository URL (MAVEN_REPO_URL):** Business Central が使用する外部 Maven リポジトリの URL。
 - **Maven repository ID (MAVEN_REPO_ID):** Maven リポジトリの ID。デフォルト値は **repo-custom** です。
 - **Maven リポジトリのユーザー名 (MAVEN_REPO_USERNAME):** Maven リポジトリのユーザー名。
 - **Maven repository password (MAVEN_REPO_PASSWORD):** Maven リポジトリのパスワード。

次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[追加の管理 Decision Server テンプレートデプロイの開始](#)」に記載の手順を実行します。

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 ミラーリポジトリの準備](#)」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こと。

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 mirror 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準備」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** の値を設定する方法は、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。この値で、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**) を設定する場合には、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。
 - ビルトイン Business Central Maven リポジトリー (**BUSINESS_CENTRAL_MAVEN_SERVICE**) を設定する場合には、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**)。
 - 両方のリポジトリーを設定している場合には、ミラーからそれらのリポジトリーを除外するように **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」に記載の手順を実行します。

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لمムが RH-SSO 認証システムに作成されていること。
- 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こと。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の管理および使用が可能です。

- クライアントが、デプロイしている Red Hat Decision Manager 環境のすべてのコンポーネントについて RH-SSO 認証システムに作成されていること。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 デプロイメントは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こと。

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 Realm name (SSO_REALM)**: Red Hat Decision Manager の RH-SSO レルム。
 - **RH-SSO Disable SSL Certificate Validation (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には **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 Client name(DECISION_CENTRAL_SSO_CLIENT)**: Business Central の RH-SSO クライアント名。
 - **KIE Server RH-SSO Client name(KIE_SERVER_SSO_CLIENT)**: Decision Server の RH-SSO クライアント名。
 - **KIE Server RH-SSO Client Secret(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 RH-SSO Client name(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 RH-SSO Client Secret(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 Realm Admin Username(SSO_USERNAME)** および **RH-SSO Realm Admin Password (SSO_PASSWORD)**: Red Hat Decision Manager の RH-SSO レルムのレルム管理者ユーザーのユーザー名およびパスワード。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」に記載の手順を実行します。

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おく。利用可能なロールの一覧は、[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、最低でも以下のユーザーを作成します。
 - **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こと。

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。これらの設定の使用方法については、「[LdapExtended login module](#)」を参照してください。LDAP サーバーでデプロイメントに必要なすべてのロールが定義されていない場合には、Red Hat Decision Manager ロールに LDAP グループをマップできます。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 file path (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、「[\(オプション\) 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 property (AUTH_ROLE_MAPPER_REPLACE_ROLE): true** に設定されている場合には、LDAP サーバーに定義したロールは、マップされたロールに置き換えられます。**false** に設定されている場合、マップされたロールおよび LDAP サーバーに定義され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](#)」に記載の手順を実行します。

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こと。

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 Extension Disabled (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](#)」に記載の手順を実行します。

Prometheus メトリクス収集の方法については、「[Managing and monitoring Decision Server](#)」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 で、**Create** をクリックします。
 - 「**This will create resources that may have security or project behavior implications**」というポップアップメッセージが表示された場合には、**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. (オプション) 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には、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。このファイルを影響を受けるすべてのデプロイメント設定にマウントします。

手順

1. **my-role-map** などのロールマッピングのプロパティファイルを作成します。このファイルには、以下の形式のエントリーを含める必要があります。

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

以下は例になります。

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

2. 以下のコマンドを実行して、このファイルから OpenShift 設定ファイルのマップを作成します。

```
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、**<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設定されたすべての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 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場合があります。

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これらのユーザーに適切なロールを割り当てる必要があります。本セクションでは、利用可能な Red Hat Decision Manager のユーザーロールについて説明します。



注記

admin、**analyst** および **rest-all** 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。これらのユーザーはユーザーの管理や、リポジトリの作成、クローン作成および管理を実行でき、アプリケーションで必要な変更を行うためのフルアクセスがあります。**admin** ロールを持つユーザーは、Red Hat Decision Manager 内のすべての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、プロジェクトをモデル化できます。ただし、これらのユーザーは **Design → Projects** ビューで共同作成者 (contributor) をスペースに追加したり、スペースを削除したりできません。**Deploy → Execution Servers** ビューへのアクセスは管理者を対象にしており、**analyst** ロールを持つユーザーは利用できません。ただし、**Deploy** ボタンは、これらのユーザーが Library パースペクティブにアクセスする際に利用できます。
- **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** ロールが割り当てられたユーザーは、Decision Server (KIE Server) REST のケイパビリティを使用できます。

第5章 OPENSIFT テンプレートの参考資料

Red Hat Decision Manager は以下の OpenShift テンプレートを提供します。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、**rhdm-7.6.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードし、これを展開します。

- **rhdm76-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、それらをステージングや実稼働環境で実行することができます。このテンプレートについての詳細は、「[rhdm76-authoring.yaml テンプレート](#)」を参照してください。
- **rhdm76-authoring-ha.yaml** は高可用性 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、それらをステージングや実稼働環境で実行することができます。このテンプレートについての詳細は、「[rhdm76-authoring-ha.yaml テンプレート](#)」を参照してください。
- **rhdm76-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。これにより、1つの Business Central が複数の別個の Decision Server を管理するステージングまたは実稼働環境をセットアップできます。このテンプレートについての詳細は、「[rhdm76-kieserver.yaml テンプレート](#)」を参照してください。

5.1. RHDM76-AUTHORING.YAML テンプレート

Red Hat Decision Manager 7.6 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、値を取るパラメーターを定義できます。この値は、パラメーターが参照される際に置き換えられます。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。詳細情報は、[Openshift ドキュメント](#)を参照してください。

変数名	イメージの環境変数	説明	値の例	必須
APPLICATION_NAME	–	アプリケーションの名前	myapp	True
KIE_ADMIN_USER	KIE_ADMIN_USER	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PASSWORD	KIE_ADMIN_PASSWORD	KIE 管理者のパスワード	–	False
KIE_SERVER_CONTROLLER_USER	KIE_SERVER_CONTROLLER_USER	KIE Server コントローラーのユーザー名 (org.kie.server.controller.user システムプロパティーを設定します)	controllerUser	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_CONTROLLER_PWD	KIE_SERVER_CONTROLLER_PWD	KIE Server コントローラーのパスワード (org.kie.server.controller.pwd システムプロパティーを設定します)	–	False
KIE_SERVER_CONTROLLER_TOKEN	KIE_SERVER_CONTROLLER_TOKEN	Bearer 認証用の KIE Server コントローラーのトークン (org.kie.server.controller.token システムプロパティーを設定します)	–	False
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します)	executionUser	False
KIE_SERVER_PASSWORD	KIE_SERVER_PASSWORD	KIE Server のパスワード (org.kie.server.pwd システムプロパティーを設定します)	–	False
KIE_SERVER_BYPASS_AUTH_USER	KIE_SERVER_BYPASS_AUTH_USER	KIE Server による、クエリーなどのタスク関連の操作についての認証済みユーザーのバイパスを許可 (org.kie.server.bypass.auth.user システムプロパティーを設定します)	false	False

変数名	イメージの環境変数	説明	値の例	必須
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、アーティファクトの SNAPSHOT バージョンを KIE サーバーにデプロイできず、既存コンテナでアーティファクトのバージョンを変更することはできません (org.kie.server.mode システムプロパティを設定します)。	DEVELOPMENT	False
KIE_MBEANS	KIE_MBEANS	KIE Server mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティを設定します)	有効	False
DROOLS_SERVER_FILTER_CLASSES	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスフィルター (org.drools.server.filter.classes システムプロパティを設定します)	true	False
PROMETHEUS_SERVER_EXT_DISABLED	PROMETHEUS_SERVER_EXT_DISABLED	false に設定されている場合には、Prometheus サーバーの拡張は有効にされます (org.kie.prometheus.server.ext.disabled システムプロパティを設定します)。	false	False

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_HOSTNAME_HTTP	HOSTNAME_HTTP	Decision Central の http サービス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。デフォルトホスト名は空白にします (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
DECISION_CENTRAL_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	decisioncentral-app-secret	True

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_HTTPS_KEYSTORE	HTTPS_KEYSTORE	シークレット内のキーストアファイル名	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名	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を設定します)。	false	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVICE_SERVICE	KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVICE_SERVICE	Business Central の OpenShift 統合がオンの場合、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.kieservice.service システムプロパティを設定します)。	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を設定します)。	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 namespace。これらの ImageStreams は通常 OpenShift の namespace 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のポインター。デフォルトは「7.6.0」です。	7.6.0	True
MAVEN_MIRROR_URL	MAVEN_MIRROR_URL	Decision Central および KIE サーバー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 リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*,!repo-rhdmcentr,!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、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 リポジトリにアクセスするためのユーザー名 (必要な場合)。	–	False
MAVEN_REPO_PASSWORD	MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	–	False
DECISION_CENTRAL_MAVEN_USERNAME	KIE_MAVEN_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パスワード	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_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	–	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 コンテナのメモリー制限	2Gi	False
KIE_SERVER_MEMORY_LIMIT	–	KIE Server コンテナのメモリー制限	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 RH-SSO クライアント名	–	False
KIE_SERVER_SSO_SECRET	SSO_SECRET	KIE Server RH-SSO クライアント名	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 レルムの管理者パスワード	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable SSL 証明書の検証	false	False
SSO_PRINCIPAL_ATTRIBUTE	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	preferred_username	False
AUTH_LDAP_URL	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	AUTH_LDAP_BIND_DN	認証に使用するバインド DN	uid=admin,ou=users,ou=example,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP 認証情報	Password	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	–	False
AUTH_LDAP_BASE_CTX_DN	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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される 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 が使用されません。	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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、DN はユーザー名に対して解析されません。このオプションは <code>usernameBeginString</code> および <code>usernameEndString</code> と共に使用されます。	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 <code>usernameEndString</code> と併用され、 <code>parseUsername</code> 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 <code>usernameEndString</code> と合わせて使用し、 <code>parseUsername</code> が true に設定されている場合にのみ考慮されます。	–	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。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される userDN は、{0} 式が使用されたフィルターに置換されます。認証済み userDN は {1} が使用されたフィルターに置換されます。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

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_DEFAULT_ROLE	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	user	False
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。 roleAttributelsDN プロパティが true に設定されている場合には、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。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 属性の値からロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	false	False
AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	-	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 ログインモジュールが指定したファイルを使用するように設定されます。このパラメーターは、ロールを置換ロールにマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたは名前を定義します。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マップを置き換えるか。true に設定されている場合は、置き換えられます。	–	False

5.1.2. オブジェクト

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

5.1.2.1. サービス

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

サービス	ポート	名前	説明
\${APPLICATION_NAME}-rhdmcentr	8080	http	全 Decision Central の Web サーバーのポート
	8443	https	
\${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

ルートは、**www.example.com** などの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1つの手段です。ルーターは、定義したルートやサービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセクター、セキュリティ設定 (オプション) で構成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

サービス	セキュリティ	ホスト名
insecure- \${APPLICATION_NAME}- rhdmcenr-http	なし	\${DECISION_CENTRAL_HOS TNAME_HTTP}
\${APPLICATION_NAME}- rhdmcenr-https	TLS パススルー	\${DECISION_CENTRAL_HOS TNAME_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ベースと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、またはトリガーされるイベントに対応して作成されます。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。

デプロイメント	トリガー
\${APPLICATION_NAME}-rhdmcenr	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は、指定した数の Pod の「レプリカ」が一度に実行されるようになります。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 の一部を強制終了します。レプリカが足りない場合には、追加で起動します。詳細は、[コンテナエンジンのドキュメント](#) を参照してください。

デプロイメント	レプリカ
<code>\${APPLICATION_NAME}-rhdmcentr</code>	1
<code>\${APPLICATION_NAME}-kieserver</code>	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。

デプロイメント	サービスアカウント
<code>\${APPLICATION_NAME}-rhdmcentr</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>

5.1.2.3.3.2. イメージ

デプロイメント	イメージ
<code>\${APPLICATION_NAME}-rhdmcentr</code>	rhdm-decisioncentral-rhel8
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${KIE_SERVER_IMAGE_STREAM_NAME}</code>

5.1.2.3.3.3. Readiness プローブ

`${APPLICATION_NAME}-rhdmcentr`

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

`${APPLICATION_NAME}-kieserver`

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

5.1.2.3.3.4. Liveness プローブ

`${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_USE RS_PROPERTIES	–	/opt/kie/data/configuration/application- users.properties
	APPLICATION_ROL ES_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 mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティを設定します)	\${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を設定します)。	`\${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、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を設定します)。	`\${KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL}`
	KIE_WORKBENCH_CONTROLLER_OPENSHIFT_ENABLED	–	true
	KIE_SERVER_CONTROLLER_USER	KIE Server コントローラーのユーザー名 (org.kie.server.controller.user システムプロパティを設定します)	`\${KIE_SERVER_CONTROLLER_USER}`
	KIE_SERVER_CONTROLLER_PWD	KIE Server コントローラーのパスワード (org.kie.server.controller.pwd システムプロパティを設定します)	`\${KIE_SERVER_CONTROLLER_PWD}`

デプロイメント	変数名	説明	値の例
	KIE_SERVER_CONTROLLER_TOKEN	Bearer 認証用の KIE Server コントローラーのトークン (org.kie.server.controller.token システムプロパティを設定します)	`\${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を設定します)	`\${KIE_SERVER_USER}`
	KIE_SERVER_PWD	KIE Server のパスワード (org.kie.server.pwd システムプロパティを設定します)	`\${KIE_SERVER_PWD}`
	WORKBENCH_ROUTE_NAME	–	`\${APPLICATION_NAME}-rhdmcenr`
	MAVEN_MIRROR_URL	Decision Central および KIE サーバー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 リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*,!repo-rhdmcenr,!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、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 リポジトリにアクセスするためのユーザー名 (必要な場合)。	\${MAVEN_REPO_USERNAME}
	MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	\${MAVEN_REPO_PASSWORD}
	KIE_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パスワード	\${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 (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 レルムの管理者パスワード	`\${SSO_PASSWORD}`
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable 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 サービスの custom 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 custom ホスト名。デフォルトホスト名は空白にします (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 認証情報	`\${AUTH_LDAP_BIND_CREDENTIAL}`
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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される 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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、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 と共に使用されます。	`\${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 と併用され、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USERNAME_BEGIN_STRING}`
	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USERNAME_END_STRING}`
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前	`\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_ROLE_S_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	`\${AUTH_LDAP_ROLE_S_CTX_DN}`
	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。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される userDN は、 <code>{0}</code> 式が使用されたフィルターに置換されます。認証済み userDN は <code>{1}</code> が使用されたフィルターに置換されます。入力ユーザー名に一致する検索フィルター例は <code>(member={0})</code> です。認証済み userDN に一致する他の例は <code>(member={1})</code> です。	`\${AUTH_LDAP_ROLE_FILTER}`
	AUTH_LDAP_ROLE_RECURSION	ロール検索が一致するコンテキストで行われる再帰のレベル数。再帰を無効にするには、これを 0 に設定します。	`\${AUTH_LDAP_ROLE_RECURSION}`
	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	`\${AUTH_LDAP_DEFAULT_ROLE}`
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。roleAttributesDN プロパティーが true に設定されている場合には、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 に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。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	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	<code>\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}</code>
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping ログインモジュールが指定したファイルを使用するように設定されます。このパラメーターは、ロールを置換ロールにマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたは名前を定義します。形式は <code>original_role=role1,role2,role3</code> になります。	<code>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</code>
	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マップを置き換えるか。true に設定されている場合は、置き換えられます。	<code>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</code>
<code>\${APPLICATION_NAME}</code>-kieserver	WORKBENCH_SERVICE_NAME	–	<code>\${APPLICATION_NAME}</code>-rhdmcenr
	KIE_ADMIN_USER	KIE 管理者のユーザー名	<code>\${KIE_ADMIN_USER}</code>
	KIE_ADMIN_PWD	KIE 管理者のパスワード	<code>\${KIE_ADMIN_PWD}</code>

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、アーティファクトの SNAPSHOT バージョンを KIE サーバーにデプロイできず、既存コンテナでアーティファクトのバージョンを変更することはできません (org.kie.server.mode システムプロパティーを設定します)。	\${KIE_SERVER_MODE}
	KIE_MBEANS	KIE Server mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティーを設定します)	\${KIE_MBEANS}
	DROOLS_SERVER_FILTER_CLASSES	KIE Server 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します)	\${DROOLS_SERVER_FILTER_CLASSES}
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定されている場合には、Prometheus サーバーの拡張は有効にされます (org.kie.prometheus.server.ext.disabled システムプロパティーを設定します)。	\${PROMETHEUS_SERVER_EXT_DISABLED}
	KIE_SERVER_BYPASS_AUTH_USER	KIE Server による、クエリーなどのタスク関連の操作についての認証済みユーザーのバイパスを許可 (org.kie.server.bypass.auth.user システムプロパティーを設定します)	\${KIE_SERVER_BYPASS_AUTH_USER}
	KIE_SERVER_ID	—	—

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_USER	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティを設定します)	`\${KIE_SERVER_USER}`
	KIE_SERVER_PWD	KIE Server のパスワード (org.kie.server.pwd システムプロパティを設定します)	`\${KIE_SERVER_PWD}`
	MAVEN_MIRROR_URL	Decision Central および KIE サーバーが使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	`\${MAVEN_MIRROR_URL}`
	MAVEN_MIRROR_OFF	KIE Server の Maven ミラー設定	`\${MAVEN_MIRROR_OFF}`
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_ID	–	repo-rhdmcentr
	RHDMCENTR_MAVEN_REPO_SERVICE	–	`\${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パスワード	`\${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 リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*,!repo-rhdmcentr,!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、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 リポジトリにアクセスするためのユーザー名 (必要な場合)。	`\${MAVEN_REPO_USERNAME}`
	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	`\${MAVEN_REPO_PASSWORD}`
	HTTPS_KEYSTORE_DIR	–	/etc/kieserver-secret-volume
	HTTPS_KEYSTORE	シークレット内のキーストアファイル名	`\${KIE_SERVER_HTTPS_KEYSTORE}`
	HTTPS_NAME	サーバー証明書に関連付けられている名前	`\${KIE_SERVER_HTTPS_NAME}`
	HTTPS_PASSWORD	キーストアおよび証明書のパスワード	`\${KIE_SERVER_HTTPS_PASSWORD}`

デプロイメント	変数名	説明	値の例
	SSO_URL	RH-SSO URL	`\${SSO_URL}`
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO レalm名	`\${SSO_REALM}`
	SSO_SECRET	KIE Server RH-SSO クライアント名	`\${KIE_SERVER_SSO_SECRET}`
	SSO_CLIENT	KIE Server RH-SSO クライアント名	`\${KIE_SERVER_SSO_CLIENT}`
	SSO_USERNAME	クライアント作成に使用する RH-SSO レalmの管理者ユーザー名 (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almの管理者パスワード	`\${SSO_PASSWORD}`
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable 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}`

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 認証情報	\${AUTH_LDAP_BIND_CREDENTIAL}
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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される 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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、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 と共に使用されます。	`\${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 と併用され、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}`

デプロイメント	変数名	説明	値の例
	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_ROLE_S_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	`\${AUTH_LDAP_ROLE_S_CTX_DN}`
	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。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される userDN は、 <code>{0}</code> 式が使用されたフィルターに置換されません。認証済み userDN は <code>{1}</code> が使用されたフィルターに置換されます。入力ユーザー名に一致する検索フィルター例は <code>(member={0})</code> です。認証済み userDN に一致する他の例は <code>(member={1})</code> 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	<p>ロール名を含む roleCtxDN コンテキスト内の属性の名前。</p> <p>roleAttributesDN プロパティが true に設定されている場合には、このプロパティはロールオブジェクトの名前属性の検索に使用されます。</p>	`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`
	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	<p>クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。このフラグは LDAP クエリーのパフォーマンスを向上できます。</p>	`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`
	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	<p>roleAttributeID にロールオブジェクトの完全修飾 DN が含まれるかどうか。false の場合は、コンテキスト名の roleNameAttributeID 属性の値から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。</p>	`\${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	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	<code>\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}</code>
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping ログインモジュールが指定したファイルを使用するように設定されます。このパラメーターは、ロールを置換ロールにマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたは名前を定義します。形式は <code>original_role=role1,role2,role3</code> になります。	<code>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</code>
	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マップを置き換えるか。true に設定されている場合は、置き換えられます。	<code>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</code>

5.1.2.3.3.7. ボリューム

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

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

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) および 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。詳細情報は、[OpenShift ドキュメント](#) を参照してください。

名前	アクセスモード
<code>\${APPLICATION_NAME}-rhdmcentr-claim</code>	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. RHDM76-AUTHORING-HA.YAML テンプレート

Red Hat Decision Manager 7.6 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、値を取るパラメーターを定義できます。この値は、パラメーターが参照される際に置き換えられます。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。詳細情報は、[OpenShift ドキュメント](#) を参照してください。

変数名	イメージの環境変数	説明	値の例	必須
APPLICATION_NAME	–	アプリケーションの名前	myapp	True
KIE_ADMIN_USER	KIE_ADMIN_USER	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PASSWORD	KIE_ADMIN_PASSWORD	KIE 管理者のパスワード	–	False

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 Server コントローラーのユーザー名 (org.kie.server.controller.user システムプロパティを設定します)	controllerUser	False
KIE_SERVER_CONTROLLER_PWD	KIE_SERVER_CONTROLLER_PWD	KIE Server コントローラーのパスワード (org.kie.server.controller.pwd システムプロパティを設定します)	—	False
KIE_SERVER_CONTROLLER_TOKEN	KIE_SERVER_CONTROLLER_TOKEN	Bearer 認証用の KIE Server コントローラーのトークン (org.kie.server.controller.token システムプロパティを設定します)	—	False
KIE_SERVER_USER	KIE_SERVER_USER	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティを設定します)	executionUser	False
KIE_SERVER_PWD	KIE_SERVER_PWD	KIE Server のパスワード (org.kie.server.pwd システムプロパティを設定します)	—	False

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 による、クエリーなどのタスク関連の操作についての認証済みユーザーのバイパスを許可 (org.kie.server.bypass.auth.user システムプロパティを設定します)	false	False
KIE_SERVER_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、アーティファクトの SNAPSHOT バージョンを KIE サーバーにデプロイできず、既存コンテナでアーティファクトのバージョンを変更することはできません (org.kie.server.mode システムプロパティを設定します)。	DEVELOPMENT	False
KIE_MBEANS	KIE_MBEANS	KIE Server mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティを設定します)	有効	False
DROOLS_SERVER_FILTER_CLASSES	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスフィルター (org.drools.server.filter.classes システムプロパティを設定します)	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 に設定されている場合には、Prometheus サーバーの拡張は有効にされます (org.kie.prometheus.server.ext.disabled システムプロパティを設定します)。	false	False
DECISION_CENTRAL_HOSTNAME_HTTP	HOSTNAME_HTTP	Decision Central の http サービス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。デフォルトホスト名は空白にします (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	–	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	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:1.3	True
DATAGRID_CPU_LIMIT	–	DataGrid Container の CPU 制限	1000m	True
DATAGRID_MEMORY_LIMIT	–	DataGrid コンテナのメモリー制限	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:7.5	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	ブローカー	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には、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を設定します)。	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、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を設定します)。	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 namespace。これらの ImageStreams は通常 OpenShift の namespace 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のポインター。デフォルトは「7.6.0」です。	7.6.0	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 サーバー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 リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*;!repo-rhdmcentr;!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、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 リポジトリにアクセスするためのユーザー名 (必要な場合)。	–	False
MAVEN_REPO_PASSWORD	MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	–	False
DECISION_CENTRAL_MAVEN_USERNAME	KIE_MAVEN_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パスワード	mavenUser	True
DECISION_CENTRAL_MAVEN_PASSWORD	KIE_MAVEN_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	–	True
GIT_HOOKS_DIRECTORY	GIT_HOOKS_DIRECTORY	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 コンテナのメモリー制限	8Gi	True

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_JAVA_MAX_MEM_RATIO	JAVA_MAX_MEM_RATIO	Decision Central Container JVM の最大メモリ比率。-Xmx がコンテナで利用可能なメモリの比率に設定されます。デフォルトは 80 です。これは、利用可能なメモリについての範囲の上限が 80% であることを意味します。-Xmx オプションの追加を省略するには、この値を 0 に設定します。	80	True
DECISION_CENTRAL_CPU_LIMIT	–	Decision Central コンテナの CPU 制限	2000m	True
KIE_SERVER_MEMORY_LIMIT	–	KIE Server コンテナのメモリ制限	1Gi	True
KIE_SERVER_CPU_LIMIT	–	KIE Server コンテナの CPU 制限	1000m	True
SSO_URL	SSO_URL	RH-SSO URL	https://rh-sso.example.com/auth	False
SSO_REALM	SSO_REALM	RH-SSO レalm 名	–	False
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 RH-SSO クライアント名	–	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_SSO_SECRET	SSO_SECRET	KIE Server RH-SSO クライアント名	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 レルムの管理者パスワード	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable SSL 証明書の検証	false	False
SSO_PRINCIPAL_ATTRIBUTE	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	preferred_username	False
AUTH_LDAP_URL	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	AUTH_LDAP_BIND_DN	認証に使用するバインド DN	uid=admin,ou=users,ou=example,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP 認証情報	Password	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	–	False
AUTH_LDAP_BASE_CTX_DN	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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される 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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、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 と共に使用されます。	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 と併用され、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。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される userDN は、{0} 式が使用されたフィルターに置換されます。認証済み userDN は {1} が使用されたフィルターに置換されます。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

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_DEFAULT_ROLE	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	user	False
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。 roleAttributelsDN プロパティが true に設定されている場合には、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。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 属性の値からロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	false	False
AUTH_LDAP_REFERRAL_USE_ROLE_ATTRIBUTE_ID_TO_CHECK	AUTH_LDAP_REFERRAL_USE_ROLE_ATTRIBUTE_ID_TO_CHECK	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	-	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 ログインモジュールが指定したファイルを使用するように設定されます。このパラメーターは、ロールを置換ロールにマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたは名前を定義します。形式は <code>original_role=role1,role2,role3</code> 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マップを置き換えるか。true に設定されている場合は、置き換えられます。	–	False

5.2.2. オブジェクト

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

5.2.2.1. サービス

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

サービス	ポート	名前	説明
\${APPLICATION_NAME}-rhdmcentr	8080	http	全 Decision Central の Web サーバーのポート
	8443	https	
\${APPLICATION_NAME}-rhdmcentr-ping	8888	ping	rhdmcentr クラスタリングの JGroups ping ポート

サービス	ポート	名前	説明
\${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 クラスタリングの JGroups ping ポート

5.2.2.2. ルート

ルートは、**www.example.com** などの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1つの手段です。ルーターは、定義したルートやサービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセレクター、セキュリティ設定 (オプション) で構成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

サービス	セキュリティ	ホスト名
insecure- \${APPLICATION_NAME}- 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ベースと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、またはトリガーされるイベントに対応して作成されます。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。

デプロイメント	トリガー
<code>\${APPLICATION_NAME}-rhdmcentr</code>	ImageChange
<code>\${APPLICATION_NAME}-kieserver</code>	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は、指定した数の Pod の「レプリカ」が一度に実行されるようにします。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 の一部を強制終了します。レプリカが足りない場合には、追加で起動します。詳細は、[コンテナエンジンのドキュメント](#)を参照してください。

デプロイメント	レプリカ
<code>\${APPLICATION_NAME}-rhdmcentr</code>	2
<code>\${APPLICATION_NAME}-kieserver</code>	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。

デプロイメント	サービスアカウント
<code>\${APPLICATION_NAME}-rhdmcentr</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-rhdmsvc</code>

5.2.2.3.3.2. イメージ

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

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

5.2.2.3.3.3. Readiness プローブ

`${APPLICATION_NAME}-rhdmcenr`

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 プローブ

`${APPLICATION_NAME}-rhdmcenr`

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
<code>\${APPLICATION_NAME}-rhdmcenr</code>	jolokia	8778	TCP
	http	8080	TCP
	https	8443	TCP
	ping	8888	TCP
<code>\${APPLICATION_NAME}-kieserver</code>	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 mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティを設定します)	\${KIE_MBEANS}
	KIE_SERVER_CONTROLLER_OPENSIFT_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を設定します)。	\${KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED}
	KIE_SERVER_CONTROLLER_OPENSIFT_PREFER_KIESERVER_SERVICE	Business Central の OpenShift 統合がオンの場合、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を設定します)。	\${KIE_SERVER_CONTROLLER_OPENSIFT_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を設定します)。	\${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 Server コントローラーのユーザー名 (org.kie.server.controller.user システムプロパティを設定します)	\${KIE_SERVER_CONTROLLER_USER}
	KIE_SERVER_CONTROLLER_PWD	KIE Server コントローラーのパスワード (org.kie.server.controller.pwd システムプロパティを設定します)	\${KIE_SERVER_CONTROLLER_PWD}
	KIE_SERVER_CONTROLLER_TOKEN	Bearer 認証用の KIE Server コントローラーのトークン (org.kie.server.controller.token システムプロパティを設定します)	\${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を設定します)	\${KIE_SERVER_USER}
	KIE_SERVER_PWD	KIE Server のパスワード (org.kie.server.pwd システムプロパティを設定します)	\${KIE_SERVER_PWD}
	WORKBENCH_ROUTE_NAME	–	\${APPLICATION_NAME}-rhdmcentr
	MAVEN_MIRROR_URL	Decision Central および KIE サーバー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 リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*,!repo-rhdmcentr,!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、MAVEN_MIRROR_OF では使用できません。	\${MAVEN_REPO_ID}
	MAVEN_REPO_URL	Maven リポジトリまたはサービスへの完全修飾 URL	\${MAVEN_REPO_URL}
	MAVEN_REPO_USE RNAME	Maven リポジトリにアクセスするためのユーザー名 (必要な場合)。	\${MAVEN_REPO_US ERNAME}
	MAVEN_REPO_PAS SWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	\${MAVEN_REPO_PA SSWORD}
	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パスワード	\${DECISION_CENTR AL_MAVEN_USERN AME}
	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_CENTR AL_MAVEN_PASSW ORD}
	GIT_HOOKS_DIR	git フックに使用するディレクトリ (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
	OPENSIFT_DNS_PING_SERVICE_NAME	–	`\${APPLICATION_NAME}-rdmcentr-ping`
	OPENSIFT_DNS_PING_SERVICE_PORT	–	8888
	APPFORMER_INFINSPIAN_SERVICE_NAME	–	`\${APPLICATION_NAME}-datagrid`
	APPFORMER_INFINSPIAN_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}`

デプロイメント	変数名	説明	値の例
	JAVA_MAX_MEM_RATIO	Decision Central Container JVM の最大メモリー比率。-Xmx がコンテナで利用可能なメモリーの比率に設定されます。デフォルトは 80 です。これは、利用可能なメモリーについての範囲の上限が 80% であることを意味します。-Xmx オプションの追加を省略するには、この値を 0 に設定します。	`\${DECISION_CENTRAL_JAVA_MAX_MEM_RATIO}`
	SSO_URL	RH-SSO URL	`\${SSO_URL}`
	SSO_OPENIDCONNECT_DEPLOYMENTS	-	ROOT.war
	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 レルムの管理者パスワード	`\${SSO_PASSWORD}`
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable 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}`

デプロイメント	変数名	説明	値の例
	HOSTNAME_HTTP	Decision Central の http サービス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。デフォルトホスト名は空白にします (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}`
	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 認証情報	`\${AUTH_LDAP_BIND_CREDENTIAL}`
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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される 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}`

デプロイメント	変数名	説明	値の例
	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検索のタイムアウト (ミリ秒単位)。	`\${AUTH_LDAP_SEARCH_TIME_LIMIT}
	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されません。	`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}
	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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、DN はユーザー名に対して解析されません。このオプションは <code>usernameBeginString</code> および <code>usernameEndString</code> と共に使用されます。	`\${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 <code>usernameEndString</code> と併用され、 <code>parseUsername</code> 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}

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_USER_NAME_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_ROLE_S_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	`\${AUTH_LDAP_ROLE_S_CTX_DN}
	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。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される userDN は、 <code>{0}</code> 式が使用されたフィルターに置換されます。認証済み userDN は <code>{1}</code> が使用されたフィルターに置換されます。入力ユーザー名に一致する検索フィルター例は <code>(member={0})</code> です。認証済み userDN に一致する他の例は <code>(member={1})</code> です。	`\${AUTH_LDAP_ROLE_FILTER}

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_ROLE_RECURSION	ロール検索が一致するコンテキストで行われる再帰のレベル数。再帰を無効にするには、これを 0 に設定します。	`\${AUTH_LDAP_ROLE_RECURSION}`
	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	`\${AUTH_LDAP_DEFAULT_ROLE}`
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。roleAttributesDN プロパティが true に設定されている場合には、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`
	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 に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。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	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping ログインモジュールが指定したファイルを使用するように設定されます。このパラメーターは、ロールを置換ロールにマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたは名前を定義します。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マップを置き換えるか。true に設定されている場合は、置き換えられます。	`\${AUTH_ROLE_MAPPER_REPLACE_ROLE}`
`\${APPLICATION_NAME}`-kieserver	WORKBENCH_SERVICE_NAME	–	`\${APPLICATION_NAME}`-rhdmcen
	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、アーティファクトの SNAPSHOT バージョンを KIE サーバーにデプロイできず、既存コンテナでアーティファクトのバージョンを変更することはできません (org.kie.server.mode システムプロパティを設定します)。	`\${KIE_SERVER_MODE}`
	KIE_MBEANS	KIE Server mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティを設定します)	`\${KIE_MBEANS}`
	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスフィルター (org.drools.server.filter.classes システムプロパティを設定します)	`\${DROOLS_SERVER_FILTER_CLASSES}`
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定されている場合には、Prometheus サーバーの拡張は有効にされます (org.kie.prometheus.server.ext.disabled システムプロパティを設定します)。	`\${PROMETHEUS_SERVER_EXT_DISABLED}`
	KIE_SERVER_BYPASS_AUTH_USER	KIE Server による、クエリーなどのタスク関連の操作についての認証済みユーザーのバイパスを許可 (org.kie.server.bypass.auth.user システムプロパティを設定します)	`\${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 Server のパスワード (org.kie.server.pwd システムプロパティを設定します)	\${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を設定します)	\${KIE_SERVER_USER}
	MAVEN_MIRROR_URL	Decision Central および KIE サーバーが使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	\${MAVEN_MIRROR_URL}
	MAVEN_MIRROR_OFF	KIE Server の Maven ミラー設定	\${MAVEN_MIRROR_OFF}
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_ID	–	repo-rhdmcentr
	RHDMCENTR_MAVEN_REPO_SERVICE	–	\${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パスワード	\${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 リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*,!repo-rhdmcentr,!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、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 リポジトリにアクセスするためのユーザー名 (必要な場合)。	`\${MAVEN_REPO_USERNAME}`
	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	`\${MAVEN_REPO_PASSWORD}`
	HTTPS_KEYSTORE_DIR	–	/etc/kieserver-secret-volume
	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 RH-SSO クライアント名	`\${KIE_SERVER_SSO_SECRET}`
	SSO_CLIENT	KIE Server 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 レルムの管理者パスワード	`\${SSO_PASSWORD}`
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable 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 認証情報	`\${AUTH_LDAP_BIND_CREDENTIAL}`
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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される 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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、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 と共に使用されます。	`\${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 と併用され、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USERNAME_BEGIN_STRING}`
	AUTH_LDAP_USERNAME_END_STRING	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	`\${AUTH_LDAP_USERNAME_END_STRING}`
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	ユーザーロールを含む属性の名前	`\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}`

デプロイメント	変数名	説明	値の例
	AUTH_LDAP_ROLE_S_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	`\${AUTH_LDAP_ROLE_S_CTX_DN}`
	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。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される userDN は、 <code>{0}</code> 式が使用されたフィルターに置換されます。認証済み userDN は <code>{1}</code> が使用されたフィルターに置換されます。入力ユーザー名に一致する検索フィルター例は <code>(member={0})</code> です。認証済み userDN に一致する他の例は <code>(member={1})</code> です。	`\${AUTH_LDAP_ROLE_FILTER}`
	AUTH_LDAP_ROLE_RECURSION	ロール検索が一致するコンテキストで行われる再帰のレベル数。再帰を無効にするには、これを 0 に設定します。	`\${AUTH_LDAP_ROLE_RECURSION}`
	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	`\${AUTH_LDAP_DEFAULT_ROLE}`
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。roleAttributesDN プロパティーが true に設定されている場合には、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 に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。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 属性の値からロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`
	AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`

デプロイメント	変数名	説明	値の例
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	このパラメーターがある場合には、RoleMapping ログインモジュールが指定したファイルを使用するように設定されます。このパラメーターは、ロールを置換ロールにマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたは名前を定義します。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マップを置き換えるか。true に設定されている場合は、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}-rhdmcen	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) および 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。詳細情報は、[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}-rhdmcen-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リングを実現できます。これには、standalone-openshift.xml で `<openshift.KUBE_PING/>` 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。

使用する検出メカニズムは、`JGROUPS_PING_PROTOCOL` 環境変数で指定します。この環境変数は `openshift.DNS_PING` または `openshift.KUBE_PING` のいずれかに設定できます。`JGROUPS_PING_PROTOCOL` に何も値が指定されていない場合には、イメージで使用するデフォルト値は、`openshift.KUBE_PING` となります。

`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 (ノードが 1 つのクラスタ) 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」が形成され、(起動後でない他のノードが検出されない) 起動後にこのクラスタが他のノードのクラスタにマージされます。

DNS_PING で使用する ping サービスの例

```
kind: Service
apiVersion: v1
spec:
  clusterIP: None
  ports:
  - name: ping
    port: 8888
  selector:
    deploymentConfig: eap-app
metadata:
  name: eap-app-ping
  annotations:
    service.alpha.kubernetes.io/tolerate-unready-endpoints: "true"
    description: "The JGroups ping port for clustering."
```

KUBE_PING を機能させるには以下の手順を実行する必要があります。

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

例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. RHDM76-KIESERVER.YAML テンプレート

Red Hat Decision Manager 7.6 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、値を取るパラメーターを定義できます。この値は、パラメーターが参照される際に置き換えられます。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。詳細情報は、[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
MAVEN_MIRROR_URL	MAVEN_MIRROR_URL	KIE Server が使用する必要がある 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

変数名	イメージの環境変数	説明	値の例	必須
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 リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*,!repo-rhdmcentr,!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、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
MAVEN_REPO_USERNAME	EXTERNAL_MAVEN_REPO_USERNAME	Maven リポジトリにアクセスするためのユーザー名 (必要な場合)。	–	False
MAVEN_REPO_PASSWORD	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	–	False

変数名	イメージの環境変数	説明	値の例	必須
DECISION_CENTRAL_SERVICE	WORKBENCH_SERVICE_NAME	必要な場合かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するために使用されるオプションの 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パスワード	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	maven!!	False
KIE_ADMIN_USER	KIE_ADMIN_USER	KIE 管理者のユーザー名	adminUser	False
KIE_ADMIN_PASSWORD	KIE_ADMIN_PASSWORD	KIE 管理者のパスワード	–	False
KIE_SERVER_USER	KIE_SERVER_USER	KIE サーバーのユーザー名 (org.kie.server.user システムプロパティを設定します)	executionUser	False
KIE_SERVER_PASSWORD	KIE_SERVER_PASSWORD	KIE Server のパスワード (org.kie.server.pwd システムプロパティを設定します)	–	False

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 namespace。これらの ImageStreams は通常 OpenShift の namespace 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のポインター。デフォルトは「7.6.0」です。	7.6.0	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、アーティファクトの SNAPSHOT バージョンを KIE サーバーにデプロイできず、既存コンテナでアーティファクトのバージョンを変更することはできません (org.kie.server.mode システムプロパティを設定します)。	PRODUCTION	False
KIE_MBEANS	KIE_MBEANS	KIE Server mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティを設定します)	有効	False
DROOLS_SERVER_FILTER_CLASSES	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスフィルター (org.drools.server.filter.classes システムプロパティを設定します)	true	False
PROMETHEUS_SERVER_EXT_DISABLED	PROMETHEUS_SERVER_EXT_DISABLED	false に設定されている場合には、Prometheus サーバーの拡張は有効にされます (org.kie.prometheus.server.ext.disabled システムプロパティを設定します)。	false	False

変数名	イメージの環境変数	説明	値の例	必須
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のままにします (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。デフォルトのホスト名を使用する場合には空白にします。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名	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 による、クエリーなどのタスク関連の操作についての認証済みユーザーのバイパスを許可 (org.kie.server.bypass.auth.user システムプロパティを設定します)	false	False

変数名	イメージの環境変数	説明	値の例	必須
KIE_SERVER_MEMORY_LIMIT	–	KIE Server コンテナのメモリー制限	1Gi	False
KIE_SERVER_CONTAINER_DEPLOYMENT	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE Server コンテナのデプロイメント設定。オプションでエイリアスあり (形式: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2)	rhdm-kieserver-library=org.openshift.quickstarts:rhdm-kieserver-library:1.6.0-SNAPSHOT	False
KIE_SERVER_MGMT_DISABLE	KIE_SERVER_MGMT_DISABLE	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.mgmt.api.disabled プロパティを true に、 org.kie.server.startup.strategy プロパティを LocalContainersStartupStrategy に設定します。	true	False
SSO_URL	SSO_URL	RH-SSO URL	https://rh-sso.example.com/auth	False
SSO_REALM	SSO_REALM	RH-SSO レalm名	–	False
KIE_SERVER_SSO_CLIENT	SSO_CLIENT	KIE Server RH-SSO クライアント名	–	False
KIE_SERVER_SSO_SECRET	SSO_SECRET	KIE Server 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 レルムの管理者パスワード	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable SSL 証明書の検証	false	False
SSO_PRINCIPAL_ATTRIBUTE	SSO_PRINCIPAL_ATTRIBUTE	ユーザー名として使用する RH-SSO プリンシパル属性	preferred_username	False
AUTH_LDAP_URL	AUTH_LDAP_URL	認証用に接続する LDAP エンドポイント	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	AUTH_LDAP_BIND_DN	認証に使用するバインド DN	uid=admin,ou=users,ou=example,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	AUTH_LDAP_BIND_CREDENTIAL	認証に使用する LDAP 認証情報	Password	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	–	False
AUTH_LDAP_BASE_CTX_DN	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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_B ASE_FILTER	AUTH_LDAP_B ASE_FILTER	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名またはログインモジュールコールバックから取得される userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	(uid={0})	False
AUTH_LDAP_S EARCH_SCOPE	AUTH_LDAP_S EARCH_SCOPE	使用する検索範囲。	SUBTREE_SCO PE	False
AUTH_LDAP_S EARCH_TIME_L IMIT	AUTH_LDAP_S EARCH_TIME_L IMIT	ユーザーまたはロール検索のタイムアウト(ミリ秒単位)。	10000	False
AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE	AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字(バックスラッシュなど)が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されません。	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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、DN はユーザー名に対して解析されません。このオプションは <code>usernameBeginString</code> および <code>usernameEndString</code> と共に使用されます。	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 <code>usernameEndString</code> と併用され、 <code>parseUsername</code> 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 <code>usernameEndString</code> と合わせて使用し、 <code>parseUsername</code> が true に設定されている場合にのみ考慮されます。	–	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_ROLE_CTX_DN	AUTH_LDAP_ROLE_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	ou=groups,ou=example,ou=com	False
AUTH_LDAP_ROLE_FILTER	AUTH_LDAP_ROLE_FILTER	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。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される userDN は、{0} 式が使用されたフィルターに置換されます。認証済み userDN は {1} が使用されたフィルターに置換されます。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

変数名	イメージの環境変数	説明	値の例	必須
AUTH_LDAP_DEFAULT_ROLE	AUTH_LDAP_DEFAULT_ROLE	認証された全ユーザーに対して含まれるロール	user	False
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	ロール名を含む roleCtxDN コンテキスト内の属性の名前。 roleAttributelsDN プロパティが true に設定されている場合には、このプロパティはロールオブジェクトの名前属性の検索に使用されます。	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	クエリーによって返された DN に roleNameAttributeID が含まれるかどうかを示すフラグ。true に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。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 属性の値からロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	false	False
AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	—	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。このプロパティは、ロールを置換ロールに対してマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	–	False
AUTH_ROLE_MAPPER_REPLACE_ROLE	AUTH_ROLE_MAPPER_REPLACE_ROLE	現在のロールを追加するか、マップされたロールに現在のマップを置き換えるか。true に設定されている場合は、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	クラスタリング向けの JGroups ping ポート

5.3.2.2. ルート

ルートは、**www.example.com** などの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1つの手段です。ルーターは、定義したルートやサービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセクター、セキュリティ設定 (オプション) で構成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

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

5.3.2.3. 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ベースと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、またはトリガーされるイベントに対応して作成されます。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。

デプロイメント	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は、指定した数の Pod の「レプリカ」が一度に実行されるようにします。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 の一部を強制終了します。レプリカが足りない場合には、追加で起動します。詳細は、[コンテナエンジンのドキュメント](#) を参照してください。

デプロイメント	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。

デプロイメント	サービスアカウント
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>

5.3.2.3.3.2. イメージ

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

5.3.2.3.3.3. Readiness プローブ

`${APPLICATION_NAME}-kieserver`

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

5.3.2.3.3.4. Liveness プローブ

`${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
<code>\${APPLICATION_NAME}-kieserver</code>	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
<code>\${APPLICATION_NAME}-kieserver</code>	<code>WORKBENCH_SERVICE_NAME</code>	必要な場合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) を許可するために使用されるオプションの Decision Central のサービス名	<code>\${DECISION_CENTRAL_SERVICE}</code>

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、アーティファクトの SNAPSHOT バージョンを KIE サーバーにデプロイできず、既存コンテナでアーティファクトのバージョンを変更することはできません (org.kie.server.mode システムプロパティを設定します)。	`\${KIE_SERVER_MODE}`
	KIE_MBEANS	KIE Server mbeans の有効化/無効化 (kie.mbeans and kie.scanner.mbeans システムプロパティを設定します)	`\${KIE_MBEANS}`
	DROOLS_SERVER_FILTER_CLASSES	KIE Server クラスフィルター (org.drools.server.filter.classes システムプロパティを設定します)	`\${DROOLS_SERVER_FILTER_CLASSES}`
	PROMETHEUS_SERVER_EXT_DISABLED	false に設定されている場合には、Prometheus サーバーの拡張は有効にされます (org.kie.prometheus.server.ext.disabled システムプロパティを設定します)。	`\${PROMETHEUS_SERVER_EXT_DISABLED}`
	KIE_SERVER_BYPASS_AUTH_USER	KIE Server による、クエリーなどのタスク関連の操作についての認証済みユーザーのバイパスを許可 (org.kie.server.bypass.auth.user システムプロパティを設定します)	`\${KIE_SERVER_BYPASS_AUTH_USER}`

デプロイメント	変数名	説明	値の例
	KIE_SERVER_ID	–	–
	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します)	\${KIE_SERVER_USER}
	KIE_SERVER_PWD	KIE Server のパスワード (org.kie.server.pwd システムプロパティーを設定します)	\${KIE_SERVER_PWD}
	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE Server コンテナのデプロイメント設定。オプションでエイリアスあり (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_OFF	KIE Server の Maven ミラー設定	\${MAVEN_MIRROR_OFF}
	MAVEN_REPOS	–	RHDMCENTR,EXTERNAL
	RHDMCENTR_MAVEN_REPO_ID	–	repo-rhdmcentr
	RHDMCENTR_MAVEN_REPO_SERVICE	必要な場合かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するために使用されるオプションの Decision Central のサービス名	\${DECISION_CENTRAL_SERVICE}

デプロイメント	変数名	説明	値の例
	RHDMCENTR_MAVEN_REPO_PATH	–	/maven2/
	RHDMCENTR_MAVEN_REPO_USERNAME	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	\${DECISION_CENTRAL_MAVEN_USERNAME}
	RHDMCENTR_MAVEN_REPO_PASSWORD	EAP 内の Decision Central がホストする Maven サービスにアクセスするためのパスワード	\${DECISION_CENTRAL_MAVEN_PASSWORD}
	EXTERNAL_MAVEN_REPO_ID	Maven リポジトリに使用する ID。これが設定されている場合には、MAVEN_MIRROR_OF に追加して、オプションで設定したミラーから除外できます (例: external:*,!repo-rhdmcentr,!repo-custom)。 MAVEN_MIRROR_URL が設定されているが MAVEN_MIRROR_ID が設定されていない場合には、ID は無作為に生成され、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 リポジトリにアクセスするためのユーザー名 (必要な場合)。	\${MAVEN_REPO_USERNAME}
	EXTERNAL_MAVEN_REPO_PASSWORD	Maven リポジトリにアクセスするパスワード (必要な場合)	\${MAVEN_REPO_PASSWORD}

デプロイメント	変数名	説明	値の例
	KIE_SERVER_MGMT_DISABLED	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.mgmt.api.disabled プロパティを true に、 org.kie.server.startup.strategy プロパティを LocalContainersStartupStrategy に設定します。	\${KIE_SERVER_MGMT_DISABLED}
	KIE_SERVER_STARTUP_STRATEGY	–	OpenShiftStartupStrategy
	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名	\${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
	OPENSIFT_DNS_PING_SERVICE_NAME	–	\${APPLICATION_NAME}-kieserver-ping
	OPENSIFT_DNS_PING_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL	\${SSO_URL}
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO レalm 名	\${SSO_REALM}

デプロイメント	変数名	説明	値の例
	SSO_SECRET	KIE Server RH-SSO クライアントシークレット	`\${KIE_SERVER_SSO_SECRET}`
	SSO_CLIENT	KIE Server 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 レルムの管理者パスワード	`\${SSO_PASSWORD}`
	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable 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のままにします (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。デフォルトのホスト名を使用する場合には空白にします。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 認証情報	`\${AUTH_LDAP_BIND_CREDENTIAL}`
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	パスワードの復号化に使用する JaasSecurityDomain の JMX ObjectName	`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`
	AUTH_LDAP_BASE_CTX_DN	ユーザー検索の開始に使用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される 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slash など) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されます。	`\${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 に設定されている場合には、DN はユーザー名に対して解析されます。false に設定されている場合には、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 と共に使用されます。	`\${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 と併用され、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_ROLE_S_CTX_DN	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールが存在する DN ではなく、ユーザーロールを含むオブジェクトが存在する DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	`\${AUTH_LDAP_ROLE_S_CTX_DN}`

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。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される userDN は、{0} 式が使用されたフィルターに置換されます。認証済み userDN は {1} が使用されたフィルターに置換されます。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。roleAttributelsDN プロパティーが true に設定されている場合には、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 に設定されている場合には、DN は roleNameAttributeID に対してチェックされます。false に設定されている場合、DN は roleNameAttributeID に対してチェックされません。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 属性の値からロール名が取得されます。Microsoft Active Directory などの特定のディレクトリースキーマでは、この属性を true に設定する必要があります。	\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}
	AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK	リファール (referral) を使用しない場合はこのオプションを無視してもかまいません。リファールを使用し、ロールオブジェクトがリファール内にある場合、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チェックされます。このオプションが設定されていないとチェックは常に失敗するため、ロールオブジェクトはリファールツリーに保存できません。	\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}

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

Red Hat OpenShift Container Platform で Red Hat Decision Manager テンプレートをデプロイし、モニターし、管理し、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。以下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、『[ビルドログへのアクセス](#)』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、『[手動のスケーリング](#)』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、「[アプリケーション変更操作](#)」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: 2019 年 10 月 31 日 (木)