



## Red Hat Decision Manager 7.8

Red Hat OpenShift Container Platform への  
Red Hat Decision Manager オーサリングまたは  
管理サーバー環境のデプロイメント

ガイド



# Red Hat Decision Manager 7.8 Red Hat OpenShift Container Platform への Red Hat Decision Manager オーサリングまたは管理サーバー環境のデプロイメント

---

ガイド

Enter your first name here. Enter your surname here.

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

Enter your email address here.

## 法律上の通知

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Deploying\_a\_Red\_Hat\_Decision\_Manager\_authoring\_or\_managed\_server\_environment\_on\_Red file |.

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

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

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

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

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

Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries.

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

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

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

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

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

All other trademarks are the property of their respective owners.

## 概要

本書では、Red Hat Decision Manager 7.8 オーサリングまたは管理サーバー環境を Red Hat OpenShift Container Platform にデプロイする方法について説明します。

## 目次

はじめに .....	4
第1章 RED HAT OPENSIFT CONTAINER PLATFORM における RED HAT DECISION MANAGER の概要 ....	6
第2章 オーサリング環境のアーキテクチャー .....	8
単一のオーサリング環境 .....	8
KIE Server のクラスターリングと複数の KIE Server の使用 .....	9
Smart Router .....	9
高可用性オーサリング環境 .....	9
第3章 OPENSIFT 環境に RED HAT DECISION MANAGER をデプロイする準備 .....	12
3.1. イメージストリームとイメージレジストリーの可用性確認 .....	12
3.2. KIE SERVER のシークレットの作成 .....	13
3.3. BUSINESS CENTRAL へのシークレットの作成 .....	14
3.4. 管理ユーザーのシークレットの作成 .....	14
3.5. オフラインで使用する MAVEN ミラーリポジトリの用意 .....	15
3.6. GLUSTERFS 設定の変更 .....	16
3.7. 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 .....	18
第4章 オーサリングまたは管理サーバー環境 .....	19
4.1. オーサリング環境のデプロイメント .....	20
4.1.1. オーサリング環境用のテンプレートの設定開始 .....	20
4.1.2. オーサリング環境に必要なパラメーターの設定 .....	21
4.1.3. オーサリング環境用のイメージストリーム namespace の設定 .....	22
4.1.4. オーサリング環境用のオプションの Maven リポジトリの設定 .....	22
4.1.5. 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 .....	23
4.1.6. 高可用性オーサリング環境用の Business Central と KIE Server のレプリカの設定 .....	23
4.1.7. オーサリング環境用の Git フックディレクトリーの指定 .....	24
4.1.8. 高可用性デプロイメントのリソース使用状況の設定 .....	24
4.1.9. オーサリング環境用の RH-SSO 認証パラメーターの設定 .....	25
4.1.10. オーサリング環境用の LDAP 認証パラメーターの設定 .....	27
4.1.11. オーサリング環境用の Prometheus メトリクス収集の有効化 .....	28
4.1.12. オーサリング環境用テンプレートのデプロイの実行 .....	28
4.2. (オプション) GIT フックディレクトリーの指定 .....	28
4.3. (オプション) 自己署名証明書で HTTPS サーバーにアクセスするためのトラストストアの提供 .....	30
4.4. (任意) LDAP ロールマッピングファイルの指定 .....	32
4.5. 追加の KIE SERVER を BUSINESS CENTRAL に接続するための OPENSIFTSTARTUPSTRATEGY 設定の有効化 .....	32
4.6. オーサリング環境または管理環境向けの追加の管理 KIE SERVER のデプロイ .....	34
4.6.1. 追加の管理 KIE Server テンプレート設定の開始 .....	34
4.6.2. 追加の管理 KIE Server に必要なパラメーターの設定 .....	35
4.6.3. 追加の管理 KIE Server のイメージストリーム namespace の設定 .....	36
4.6.4. 追加の管理 KIE Server 用の Business Central インスタンスについての情報の設定 .....	36
4.6.5. 追加の管理 KIE 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 .....	37
4.6.6. 追加の管理 KIE Server の RH-SSO 認証パラメーターの設定 .....	38
4.6.7. 追加の管理 KIE Server の LDAP 認証パラメーターの設定 .....	39
4.6.8. 追加の管理 KIE Server の Prometheus メトリクス収集の有効化 .....	40
4.6.9. 追加の管理 KIE Server テンプレートデプロイの実行 .....	40
第5章 RED HAT DECISION MANAGER ロールおよびユーザー .....	42

<b>第6章 OPENSIFT テンプレートの参考資料</b> .....	<b>43</b>
6.1. RHDM78-AUTHORING.YAML TEMPLATE	43
6.1.1. パラメーター	43
6.1.2. オブジェクト	57
6.1.2.1. サービス	57
6.1.2.2. ルート	58
6.1.2.3. デプロイメント設定	58
6.1.2.3.1. トリガー	58
6.1.2.3.2. レプリカ	59
6.1.2.3.3. Pod テンプレート	59
6.1.2.4. 外部の依存関係	78
6.1.2.4.1. ボリューム要求	78
6.1.2.4.2. シークレット	79
6.2. RHDM78-AUTHORING-HA.YAML テンプレート	79
6.2.1. パラメーター	79
6.2.2. オブジェクト	95
6.2.2.1. サービス	95
6.2.2.2. ルート	96
6.2.2.3. デプロイメント設定	97
6.2.2.3.1. トリガー	97
6.2.2.3.2. レプリカ	97
6.2.2.3.3. Pod テンプレート	97
6.2.2.4. 外部の依存関係	118
6.2.2.4.1. ボリューム要求	118
6.2.2.4.2. シークレット	118
6.2.2.4.3. クラスターリング	118
6.3. RHDM78-KIESERVER.YAML テンプレート	119
6.3.1. パラメーター	120
6.3.2. オブジェクト	132
6.3.2.1. サービス	132
6.3.2.2. ルート	133
6.3.2.3. デプロイメント設定	133
6.3.2.3.1. トリガー	133
6.3.2.3.2. レプリカ	133
6.3.2.3.3. Pod テンプレート	133
6.3.2.4. 外部の依存関係	144
6.3.2.4.1. シークレット	144
6.4. OPENSIFT の使用に関するクイックリファレンス	144
<b>付録A バージョン情報</b> .....	<b>147</b>



## はじめに

システムエンジニアは、Red Hat OpenShift Container Platform に Red Hat Decision Manager オーサリングまたは管理環境をデプロイして、サービスおよびその他のビジネスアセットを開発するプラットフォームを提供します。

### 前提条件

- 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。
  - KIE 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 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。
  - 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。



### 注記

クラスターの容量を確認する方法は、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 の [CLI リファレンス](#) を参照してください。OpenShift Web コンソールを使用してテンプレートをデプロイするには、Web コンソールを使用してログインしている必要もあります。
- 動的永続ボリューム (PV) のプロビジョニングが有効になっている。または、動的 PV プロビジョニングが有効でない場合には、十分な永続ボリュームが利用できる状態でなければなりません。デフォルトでは、Business Central は 1Gi 分の PV が必要です。テンプレートパラメーターで、Business Central 永続ストレージの PV サイズを変更することができます。
- 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は、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 のパブリックおよび専用クラウドでのアクセスモードのサポートに関する情報は、[アクセスモード](#) を参照してください。



## 注記

Red Hat Decision Manager バージョン 7.5 以降では、Red Hat OpenShift Container Platform 3.x 向けのイメージおよびテンプレートが非推奨になりました。上記のイメージとテンプレートには新機能が追加されませんが、Red Hat OpenShift Container Platform バージョン 3.x の完全サポートが終了するまでサポートは継続されます。Red Hat OpenShift Container Platform バージョン 3.x における完全なサポートライフサイクルフェーズに関する詳細は、[Red Hat OpenShift Container Platform のライフサイクルポリシー \(最新バージョン以外\)](#) を参照してください。



## 注記

Red Hat Decision Manager テンプレートを Red Hat OpenShift Container Platform 4.x と一緒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、[Operator を使用した Red Hat OpenShift Container Platform への Red Hat Decision Manager 環境のデプロイ](#) 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、別の OpenShift Pod としてデプロイされます。各 Pod のスケールアップおよびスケールダウンを個別に行い、特定のコンポーネントに必要な数だけコンテナを提供できます。標準の OpenShift の手法を使用して Pod を管理し、負荷を分散できます。

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

- **KIE Server (実行サーバー (Execution Server) と呼ばれる)** は、デシ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。サービスのすべてのロジックは実行サーバーで実行されます。  
一部のテンプレートでは、KIE Server Pod をスケールアップして、同一または異なるホストで実行するコピーを必要な数だけ提供できます。Pod のスケールアップまたはスケールダウンを行うと、そのコピーはすべて同じサービスを実行します。OpenShift は負荷分散を提供しているため、要求はどの Pod でも処理できます。

KIE 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 KIE Server Pod を必要な数だけ設定することができます。

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

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

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

以下の環境タイプが一般的です。

- **オーサリングまたは管理環境:** 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 KIE 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。これは、オーサリング作業用の Business Central を提供する Pod およびサービス実行用の 1 つ以上の KIE Server を提供する Pod で設定されます。それぞれの KIE 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 KIE 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、[Red Hat OpenShift Container Platform への Red Hat Decision Manager オーサリングまたは管理サーバー環境のデプロイ](#) を参照してください。
- **イミュータブルサーバーを使用するデプロイメント:** ステージングおよび実稼働目的で既存のサービスを実行するための代替の環境です。この環境では、KIE 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読み込み、起動するイメージをビルドします。この Pod でサービスを停止したり、新しいサービスを追加したりすることはできません。サービスの別のバージョンを使用したり、別の方法で設定を変更する必要がある場合は、新規のサーバーイ

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、KIE Server は OpenShift 環境の Pod のように実行されるため、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。このような環境のデプロイメント手順は、[Red Hat OpenShift Container Platform への Red Hat Decision Manager イミュータブルサーバー環境のデプロイメント](#) を参照してください。

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

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

## 第2章 オーサリング環境のアーキテクチャー

Red Hat Decision Manager では、Business Central のコンポーネントに、オーサリングサービス用の Web ベースの対話型ユーザーインターフェイスが含まれています。KIE Server のコンポーネントでこれらのサービスを実行します。

Business Central を使用して、KIE Server 上でサービスをデプロイすることもできます。複数の KIE Server を使用して異なるサービスを実行して同じ Business Central から複数のサーバーを制御できます。

### 単一のオーサリング環境

単一のオーサリング環境では、Business Central のインスタンスが1つだけ実行されます。複数のユーザーが同時に Web インターフェイスにアクセスできますが、パフォーマンスが制限される可能性があります。フェイルオーバー機能はありません。

Business Central には、開発したサービスの各種ビルドバージョン (KJAR ファイル/アーティファクト) を格納する、ビルトイン Maven リポジトリが含まれています。継続的インテグレーション/継続的デプロイメント (CI/CD) ツールを使用して、リポジトリからこのようなアーティファクトを取得し、必要に応じて移動できます。

Business Central は、ビルトインの Git リポジトリにソースコードを保存します (.niogit ディレクトリに保存)。組み込まれたインデックスメカニズムを使用して、サービス内でアセットをインデックス化します。

Business Central では、Maven リポジトリと Git リポジトリに永続ストレージを使用します。

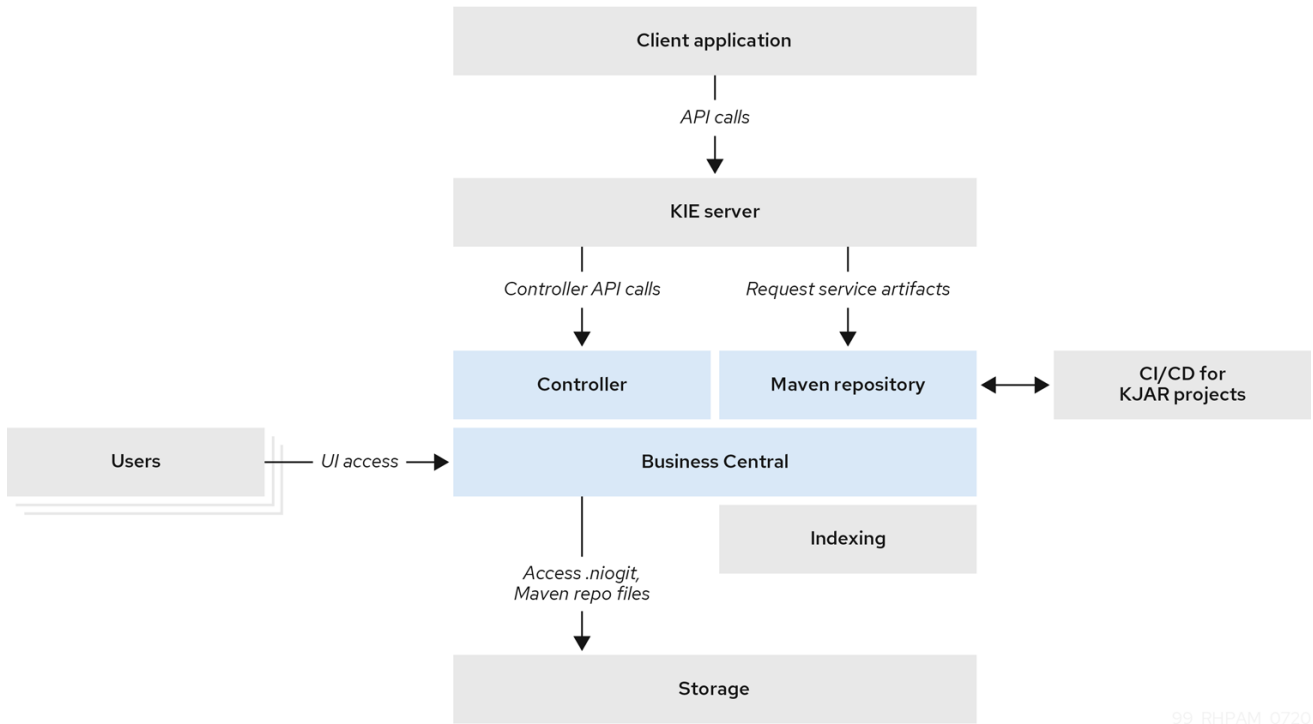
単一のオーサリング環境には、デフォルトで KIE Server が1台含まれています。

単一のオーサリング環境ではデフォルトで、**コントローラストラテジー** を使用します。Business Central には、KIE Server を管理できるコンポーネントである **コントローラー** が含まれています。Business Central に接続するように KIE Server を設定した場合、KIE Server は REST API を使用してコントローラーに接続します。この接続を使用すると、WebSocket が永続的に解放されます。コントローラストラテジーを使用する OpenShift デプロイメントでは、KIE Server はそれぞれ、Business Central コントローラーに接続するように初期設定されます。

Business Central ユーザーインターフェイスを使用して KIE Server でサービスをデプロイしたり管理したりする場合、KIE Server はコントローラー接続の WebSocket を使用して要求を受け取ります。サービスをデプロイする場合は、KIE Server が Business Central の一部である Maven リポジトリから必要なアーティファクトを要求します。

クライアントアプリケーションは、REST API 経由で、KIE Server で実行されるサービスを使用します。

図2.1 単一のオーサリング環境のアーキテクチャー図



99\_RHPAM\_0720

## KIE Server のクラスターリングと複数の KIE Server の使用

KIE Server Pod をスケーリングして、KIE Server のクラスター環境を実行できます。

クラスターデプロイメントでは、複数の KIE Server インスタンスが同じサービスを実行します。このようなサーバーは、Business Central コントローラーから同じ要求を受信できるように、同じサーバー ID を使用して Business Central コントローラーに接続します。Red Hat OpenShift Container Platform ではサーバー間の負荷分散が可能です。同じクライアントからの要求が別のインスタンスで処理される可能性があるため、クラスター化された KIE Server で実行するサービスは、ステートレスでなければなりません。

独立した KIE Server を複数デプロイして、異なるサービスを実行することも可能です。このような場合、サーバーは異なるサーバー ID 値を指定して Business Central コントローラーに接続します。各サーバーにサービスをデプロイする場合は、Business Central UI を使用できます。

## Smart Router

任意の Smart Router コンポーネントは、クライアントアプリケーションと KIE Server の間にレイヤーを提供します。独立した KIE Server を複数使用する場合に役立ちます。

クライアントアプリケーションは、異なる KIE Server で実行されるサービスを使用できますが、常に Smart Router に接続されます。Smart Router は自動的に、必要なサービスを実行する KIE Server に要求を渡します。また、Smart Router では、サービスのバージョン管理も可能で、追加の負荷分散レイヤーも提供されます。

## 高可用性オーサリング環境

高可用性 (HA) のオーサリング環境では Business Central Pod がスケーリングされるため、複数の Business Central インスタンスが実行されます。Red Hat OpenShift Container Platform は、ユーザー要求の負荷分散を提供します。この環境は、複数のユーザーに最適なパフォーマンスを提供し、フェイルオーバーをサポートします。

Business Central の各インスタンスには、構築されたアーティファクト用の Maven リポジトリが含まれており、ソースコードには **.niogit** の Git リポジトリを使用します。このインスタンスは、リポジトリ用に共有の永続ストレージを使用します。このストレージには、**ReadWriteMany** アクセス権の

ある永続ボリュームが必要です。

Red Hat DataGrid のインスタンスは、Business Central で開発されたすべてのプロジェクトとアセットをインデックス化します。

Red Hat AMQ インスタンスは、Business Central のすべてのインスタンス間に、Java CDI メッセージを伝播します。たとえば、新規プロジェクトが作成された場合、アセットがインスタンスの1つでロックまたは変更された場合に、その情報が即座に他の全インスタンスで反映されます。

コントローラストラテジーは、クラスターデプロイメントには適していません。OpenShift デプロイメントの場合は、高可用性の Business Central は **OpenShift スタートアップストラテジー** を使用して KIE Server を管理する必要があります。

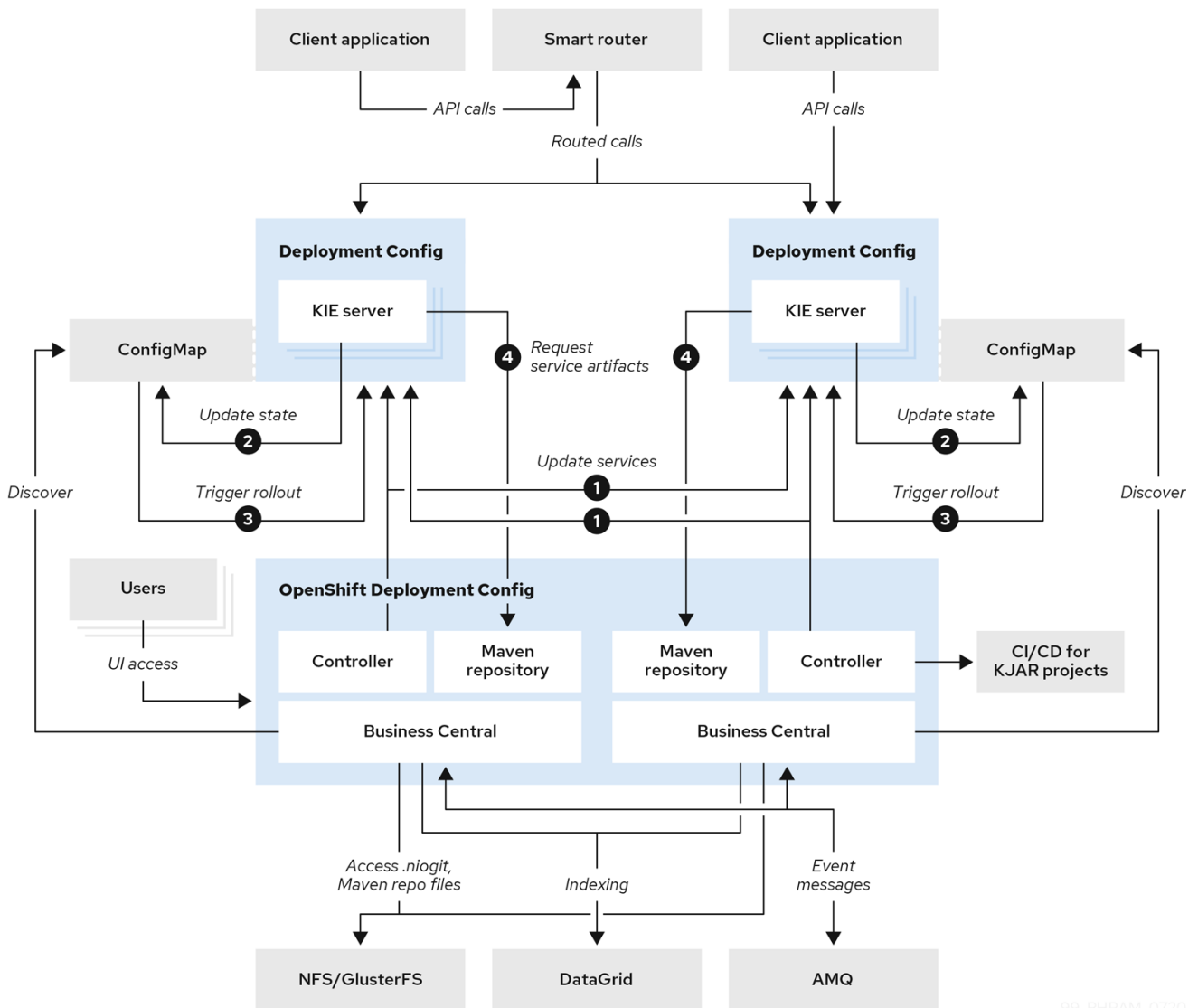
KIE Server デプロイメント (スケーリング可能) ごとに、現在の状態を反映する ConfigMap を作成します。Business Central は、ConfigMap を読み込むことで全 KIE Server を検出します。

ユーザーが KIE Server 設定 (例: サービスのデプロイまたはアンデプロイ) で変更を要求した場合に、Business Central は KIE Server への接続を開始し、REST API 要求を送信します。KIE Server は、全インスタンスが再デプロイされ、新規設定が反映されるように、ConfigMap を変更して新しい設定の状態を反映し、独自の再デプロイをトリガーします。

OpenShift 環境で、独立した KIE Server を複数デプロイできます。KIE Server にはそれぞれ、必要な設定が指定された個別の ConfigMap が設定されます。KIE Server は個別にスケーリングできます。

OpenShift デプロイメントに、Smart Router を追加できます。

図2.2 高可用性オーサリング環境のアーキテクチャー図



99\_RHPAM\_0720

## 第3章 OPENSIFT 環境に RED HAT DECISION MANAGER をデプロイする準備

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

### 3.1. イメージストリームとイメージレジストリーの可用性確認

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

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

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

#### 手順

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

```
$ oc get imagestreamtag -n openshift | grep -F rhdm78-decisioncentral-openshift
$ oc get imagestreamtag -n openshift | grep -F rhdm78-kieserver-openshift
```

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

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

- e. 以下のコマンドを実行します。

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

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

- f. **Software Downloads** ページから [rhdm-7.8.0-openshift-templates.zip](#) の製品配信可能ファイルをダウンロードし、**rhdm78-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 rhdm78-image-streams.yaml
```



#### 注記

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

## 3.2. KIE 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、Red Hat OpenShift Container Platform ドキュメントの [シークレット](#) の章を参照してください。

KIE 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. KIE 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 KIE Server の URL と一致する、有効な署名済み証明書を生成します。

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

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

### 3.3. 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 KIE Server に同じ証明書およびキーストアを使用しないでください。

#### 手順

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



#### 注記

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

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

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

### 3.4. 管理ユーザーのシークレットの作成

Red Hat Decision Manager 管理ユーザーアカウントのユーザー名とパスワードを含む汎用シークレットを作成する必要があります。このシークレットは、試行版テンプレート以外のテンプレートを使用して Red Hat Decision Manager をデプロイするのに必要です。

シークレットには、リテラルのユーザー名とパスワードが含まれている必要があります。ユーザー名のキー名は **KIE\_ADMIN\_USER** です。パスワードのキー名は **KIE\_ADMIN\_PWD** です。

複数のテンプレートを使用して Red Hat Decision Manager のコンポーネントをデプロイする場合は、これらのすべてのデプロイメントに同じシークレットを使用します。コンポーネントは、このユーザーアカウントを利用して相互に通信します。

このユーザーアカウントを使用して Business Central にログインすることもできます。



#### 重要

RH-SSO または LDAP 認証を使用する場合は、Red Hat Decision Manager の **kie-server,rest-all,admin** ロールを使用して、認証システムで同じパスワードを持つ同じユーザーを設定する必要があります。

## 手順

**oc** コマンドを使用し、ユーザー名およびパスワードの **kie-admin-user-secret** という汎用シークレットを生成します。

```
$ oc create secret generic rhpam-credentials --from-literal=KIE_ADMIN_USER=adminUser --from-literal=KIE_ADMIN_PWD=adminPassword
```

このコマンドで、**adminPassword** を管理ユーザーのパスワードに置き換えます。必要に応じて、**adminUser** を管理ユーザーの別のユーザー名に置き換えることができます。

## 3.5. オフラインで使用する MAVEN ミラーリポジトリの用意

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



### 注記

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

### 前提条件

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

### 手順

- 書き込みアクセス権がある Maven リリースリポジトリを設定します。リポジトリは認証なしで読み取りアクセスを許可する必要があり、OpenShift 環境にはこのリポジトリへのネットワーク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、Red Hat OpenShift Container Platform 3.11 ドキュメントの [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。

- 公開インターネットに送信アクセスができるコンピューターで、以下のアクションを実行します。
  - Red Hat Process Automation Manager 7.8.0 Offliner Content List** をクリックして、Red Hat カスタマーポータルの [Software Downloads](#) ページから製品配信ファイル **rhdm-7.8.0-offliner.zip** をダウンロードします。
  - rhdm-7.8.0-offliner.zip** ファイルの内容を任意のディレクトリに展開します。
  - ディレクトリに移動し、以下のコマンドを入力します。

```
./offline-repo-builder.sh offliner.txt
```

このコマンドは、**repository** サブディレクトリを作成し、必要なアーティファクトをこのサブディレクトリにダウンロードします。

一部のダウンロードが失敗したことを示すメッセージが表示された場合は、同じコマンドを再度実行してください。ダウンロードが再び失敗する場合は、Red Hat サポートに連絡してください。

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

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

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

- d. ローカルの Maven キャッシュディレクトリー (`~/.m2/repository`) から作成した Maven ミラーリポジトリにすべてのアーティファクトをアップロードします。アーティファクトをアップロードするには、Git リポジトリ [Maven repository tools](#) から利用できる Maven Repository Provisioner ユーティリティを使用できます。

### 3.6. GLUSTERFS 設定の変更

OpenShift 環境が GlusterFS を使用して永続ストレージボリュームを提供するかどうかを確認する必要があります。GlusterFS を使用している場合は、Business Central の最適なパフォーマンスを確保するために、ストレージクラスの設定を変更して GlusterFS ストレージをチューニングする必要があります。

#### 手順

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

```
oc get storageclass
```

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

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

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

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

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

**<class-name>** はデフォルトのストレージクラス名に置き換えます。以下に例を示します。

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

3. **storage\_config.yaml** ファイルを編集します。

- a. 以下のキーがある行を削除します。

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

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

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

以下に例を示します。

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

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

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

以下に例を示します。

**volumeoptions: client.ssl off, server.ssl off, features.cache-invalidation on, nfs.trusted-write on, nfs.trusted-sync on, performance.nl-cache on, performance.stat-**

**prefetch off, performance.read-ahead off, performance.write-behind off,  
performance.readdir-ahead off, performance.io-cache off, performance.quick-read off,  
performance.open-behind off, locks.mandatory-locking off, performance.strict-o-  
direct on**

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

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

**<class-name>** はデフォルトのストレージクラス名に置き換えます。以下に例を示します。

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

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

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

### 3.7. 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、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は、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、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、Red Hat OpenShift Container Platform 3.11 ドキュメントの [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4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 KIE 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 KIE Server で設定されます。

Business Central を使用するとサービスの開発や KIE Server へのデプロイを実行できます。複数の KIE 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 KIE 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 KIE 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 KIE Server で設定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 KIE Server テンプレートを同じ名前空間にデプロイし、複数の KIE 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の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 を実行し、もう1つは KIE 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。これには、**ReadWriteMany** アクセスモードをサポートする永続ボリュームは不要です。

単一のオーサリング環境では、Business Central をスケーリングすることはできません。KIE Server はスケーリングできます。

HA オーサリング環境では、Business Central と KIE Server の両方がスケーリング可能な 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して、特に複数のユーザーが同時にオーサリングに関与する場合に、信頼性と応答性を最大限提供します。

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と、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は、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は、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は、アセットが作成されるものの、インデックス化されないため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。
- サービスを KIE Server にデプロイすると、KIE Server デプロイメントが再度ロールアウトされます。ロールアウトが完了するまで、同じ KIE Server に別のサービスをデプロイできません。

高可用性オーサリング環境では、必要に応じて、別の管理対象またはイミュータブル KIE Server を追加でデプロイすることも可能です。Business Central は、イミュータブル KIE Server や管理対象 KIE Server など、同じ namespace 内の KIE Server を自動検出できます。

単一のオーサリング環境で管理対象またはイミュータブルな KIE Server を追加でデプロイする場合は、「[追加の KIE Server を Business Central に接続するための OpenShiftStartupStrategy 設定の有効化](#)」に記載されているように、環境内の **OpenShiftStartupStrategy** 設定を手作業で有効にする手順が別途必要になります。この設定により、他の KIE Server の検出が可能になります。

管理対象の KIE Server のデプロイ方法は、「[オーサリング環境または管理環境向けの追加の管理 KIE Server のデプロイ](#)」を参照してください。イミュータブル KIE Server のデプロイメント方法については、[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。

## 4.1. 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 KIE Server で設定されます。

### 4.1.1. オーサリング環境用のテンプレートの設定開始

単一オーサリング環境をデプロイする必要がある場合は、**rhdm78-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、**rhdm78-authoring-ha.yaml** テンプレートファイルを使用します。

#### 手順

1. Red Hat カスタマーポータル[の Software Downloads](#) ページから製品配信可能ファイル **rhdm-7.8.0-openshift-templates.zip** をダウンロードします。
2. 必要なテンプレートファイルを展開します。
3. 以下のいずれかの方法を使用してテンプレートのデプロイを開始します。
  - OpenShift Web UI を使用するには、OpenShift アプリケーションコンソールで **Add to Project → Import YAML / JSON** を選択してから **<template-file-name>.yaml** ファイルを選択または貼り付けます。Add Template ウィンドウで、**Process the template** が選択されていることを確認し、**Continue** をクリックします。
  - OpenShift コマンドラインコンソールを使用するには、以下のコマンドラインを準備します。

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

このコマンドラインで、以下のように変更します。

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

## 次のステップ

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

### 4.1.2. オーサリング環境に必要なパラメーターの設定

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

#### 前提条件

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

#### 手順

1. 以下のパラメーターを設定します。

- **Credentials secret (CREDENTIALS\_SECRET):** 「[管理ユーザーのシークレットの作成](#)」で作成される管理ユーザーの認証情報を含むシークレットの名前。
- **Business Central サーバーキーストアのシークレット名 (DECISION\_CENTRAL\_HTTPS\_SECRET):** 「[Business Central へのシークレットの作成](#)」で作成した Business Central のシークレットの名前。
- **KIE Server Keystore Secret Name (KIE\_SERVER\_HTTPS\_SECRET):** 「[KIE Server のシークレットの作成](#)」で作成した KIE Server のシークレットの名前。
- **Business Central サーバーの証明署名 (DECISION\_CENTRAL\_HTTPS\_NAME):** 「[Business Central へのシークレットの作成](#)」で作成したキーストアの証明書の名前。
- **Business Central サーバーキーストアのパスワード (DECISION\_CENTRAL\_HTTPS\_PASSWORD):** 「[Business Central へのシークレットの作成](#)」で作成したキーストアのパスワード。
- **KIE Server Certificate Name (KIE\_SERVER\_HTTPS\_NAME):** 「[KIE 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):** 「[KIE 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。
- **アプリケーション名 (APPLICATION\_NAME):** OpenShift アプリケーションの名前。これは、Business Central Monitoring および KIE Server のデフォルト URL で使用されます。OpenShift はアプリケーション名を使用して、デプロイメント設定、サービス、ルート、ラベル、およびアーティファクトの個別のセットを作成します。

- **ImageStream 名前空間 (IMAGE\_STREAM\_NAMESPACE)**: イメージストリームが利用可能な名前空間。OpenShift 環境でイメージストリームが利用可能な場合 ([「イメージストリームとイメージレジストリーの可用性確認」](#) を参照) は、namespace が **openshift** になります。イメージストリームファイルをインストールしている場合は、名前空間が OpenShift プロジェクトの名前になります。

## 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。

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

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

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

#### 前提条件

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

#### 手順

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

### 4.1.4. オーサリング環境用のオプションの Maven リポジトリの設定

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

#### 前提条件

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

#### 手順

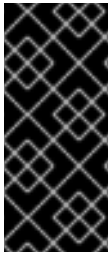
カスタム Maven リポジトリへのアクセスを設定するには、以下のパラメーターを設定します。

- **Maven リポジトリの URL (MAVEN\_REPO\_URL)**: Maven リポジトリの URL。
- **Maven リポジトリの ID (MAVEN\_REPO\_ID)**: Maven リポジトリの ID。デフォルト値は **repo-custom** です。
- **Maven リポジトリのユーザー名 (MAVEN\_REPO\_USERNAME)**: Maven リポジトリのユーザー名。
- **Maven リポジトリのパスワード (MAVEN\_REPO\_PASSWORD)**: Maven リポジトリのパスワード。

## 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。

## 4.1.5. 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用意](#)」に従って設定した Maven ミラーへのアクセスを設定する必要があります。

### 前提条件

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

### 手順

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

- Maven ミラー URL (MAVEN\_MIRROR\_URL):** 「[オフラインで使用する Maven ミラーリポジトリの用意](#)」で設定した Maven ミラーリポジトリの URL。この URL は、OpenShift 環境の Pod からアクセスできるようにする必要があります。
- Maven mirror of (MAVEN\_MIRROR\_OF):** ミラーから取得されるアーティファクトを定める値。**mirrorOf** 値の設定方法は、Apache Maven ドキュメントの [Mirror Settings](#) を参照してください。デフォルト値は **external:\*,!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**) を設定する場合は、このリポジトリ内のアーティファクトを除外するように **MAVEN\_MIRROR\_OF** を変更します (例: **external:\*,!repo-custom**)。 **repo-custom** は、**MAVEN\_REPO\_ID** で設定した ID に置き換えます。

## 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。

## 4.1.6. 高可用性オーサリング環境用の Business Central と KIE Server のレプリカの設定

高可用性オーサリング環境をデプロイする場合に、デフォルトでは、Business Central のレプリカと KIE Server のレプリカが 2 つずつ最初に作成されます。

必要に応じて、レプリカの数を変更できます。

単一のオーサリング環境では、この手順を飛ばして次に進んでください。

## 前提条件

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

## 手順

レプリカの数を変更するには、次のパラメーターを設定します。

- **Business Central Container レプリカ (DECISION\_CENTRAL\_CONTAINER\_REPLICAS)**: デプロイメントで Business Central に最初に作成するレプリカ数。
- **KIE Server コンテナのレプリカ (KIE\_SERVER\_CONTAINER\_REPLICAS)**: デプロイメントで KIE Server に最初に作成するレプリカ数。

## 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。

### 4.1.7. 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開始](#)」に説明されているようにテンプレートの設定を開始している。

## 手順

Git フックディレクトリーを設定するには、以下のパラメーターを設定します。

- **Git フックディレクトリー (GIT\_HOOKS\_DIR)**: Git フックディレクトリーへの完全修飾パス (例: `/opt/kie/data/git/hooks`)。ディレクトリーの内容を指定し、これを指定されたパスにマウントする必要があります。設定マップまたは永続ボリュームを使用して Git フックディレクトリーを指定し、マウントする方法は、「[\(オプション\) Git フックディレクトリーの指定](#)」を参照してください。

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

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

### 4.1.8. 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 (`rhdm78-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 (`rhdm78-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](#)
- [コンピュートリソース](#)

#### 前提条件

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

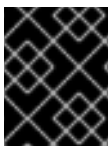
#### 手順

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 コンテナのメモリー制限(`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 の JVM 最大メモリー割合 (`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 コンテナの CPU 制限(`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 コンテナのメモリー制限(`KIE_SERVER_MEMORY_LIMIT`):** KIE 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 コンテナの CPU 制限(`KIE_SERVER_CPU_LIMIT`):** KIE Server の CPU 使用の最大値。デフォルト値は **1000m** です。
- **DataGrid Container のメモリー制限(`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 制限(`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。

#### 4.1.9. 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が RH-SSO 認証システムに作成されている。

- Red Hat Decision Manager のユーザー名およびパスワードが RH-SSO 認証システムに作成されている。利用可能なロールの一覧については、[5章Red Hat Decision Manager ロールおよびユーザー](#)を参照してください。  
「[管理ユーザーのシークレットの作成](#)」で説明されているように、管理ユーザーのシークレットで設定されたユーザー名およびパスワードを使用してユーザーを作成する必要があります。このユーザーには **kie-server,rest-all,admin** ロールが必要です。
- デプロイしている Red Hat Decision Manager 環境の全コンポーネントに対して、クライアントが RH-SSO 認証システムに作成されている。クライアントのセットアップには、コンポーネントの URL が含まれます。環境のデプロイ後に URL を確認し、編集できます。または、Red Hat Decision Manager のデプロイメントでクライアントを作成できます。ただし、このオプションの環境に対する制御の詳細度合はより低くなります。
- 「[オーサリング環境用のテンプレートの設定開始](#)」に説明されているようにテンプレートの設定を開始している。

## 手順

- 以下のパラメーターを設定します。
  - RH-SSO URL (SSO\_URL):** RH-SSO の URL。
  - RH-SSO レalm名 (SSO\_REALM):** Red Hat Decision Manager の RH-SSO レalm。
  - RH-SSO が無効な SSL 証明書の検証 (SSO\_DISABLE\_SSL\_CERTIFICATE\_VALIDATION):** RH-SSO インストールで有効な HTTPS 証明書を使用していない場合は **true** に設定します。
- 以下の手順のいずれかを実行します。
  - RH-SSO で Red Hat Decision Manager のクライアントを作成した場合は、テンプレートで以下のパラメーターを設定します。
    - Business Central RH-SSO クライアント名 (DECISION\_CENTRAL\_SSO\_CLIENT):** Business Central の RH-SSO クライアント名。
    - Business Central RH-SSO クライアントのシークレット (DECISION\_CENTRAL\_SSO\_SECRET):** Business Central のクライアント向けに RH-SSO で設定するシークレット文字列。
    - KIE Server RH-SSO クライアント名 (KIE\_SERVER\_SSO\_CLIENT):** KIE Server の RH-SSO クライアント名。
    - KIE Server RH-SSO クライアントのシークレット (KIE\_SERVER\_SSO\_SECRET):** KIE 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 に Red Hat Decision Manager のクライアントを作成する場合は、テンプレートで以下のパラメーターを設定します。
    - Business Central RH-SSO クライアント名 (DECISION\_CENTRAL\_SSO\_CLIENT):** Business Central 向けに RH-SSO に作成するクライアント名。
    - Business Central RH-SSO クライアントのシークレット (DECISION\_CENTRAL\_SSO\_SECRET):** Business Central のクライアント向けに RH-SSO で設定するシークレット文字列。
    - KIE Server RH-SSO クライアント名 (KIE\_SERVER\_SSO\_CLIENT):** KIE Server 向けに RH-SSO に作成するクライアント名。

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

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

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

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

### 4.1.10. 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は、テンプレートをオーサリング環境をデプロイするように設定する際に追加の設定を実行します。



#### 重要

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

## 前提条件

- LDAP システムに Red Hat Decision Manager のユーザー名およびパスワードを作成している。利用可能なロールの一覧については、[5章 Red Hat Decision Manager ロールおよびユーザー](#) を参照してください。  
「[管理ユーザーのシークレットの作成](#)」で説明されているように、管理ユーザーのシークレットで設定されたユーザー名およびパスワードを使用してユーザーを作成する必要があります。このユーザーには **kie-server,rest-all,admin** ロールが必要です。
- 「[オーサリング環境用のテンプレートの設定開始](#)」に説明されているようにテンプレートの設定を開始している。

## 手順

1. テンプレートの **AUTH\_LDAP\*** パラメーターを設定します。これらのパラメーターは、Red Hat JBoss EAP の **LdapExtended** ログインモジュールの設定に対応します。これらの設定に関する説明は、[LdapExtended ログインモジュール](#) を参照してください。  
LDAP サーバーがデプロイメントに必要な全ロールを定義していない場合は、LDAP グループを Red Hat Decision Manager ロールにマッピングしてください。LDAP のロールマッピングを有効にするには、以下のパラメーターを設定します。
  - RoleMapping rolesProperties ファイルパス (**AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES**):  
`/opt/eap/standalone/configuration/rolemapping/rolemapping.properties` など、ロールのマッピングを定義するファイルの完全修飾パス名。このファイルを指定して、該当するすべてのデプロイメント設定でこのパスにマウントする必要があります。これを実行する方法については、「[\(任意\) LDAP ロールマッピングファイルの指定](#)」を参照してください。

- **RoleMapping replaceRole プロパティ (AUTH\_ROLE\_MAPPER\_REPLACE\_ROLE):** **true** に設定した場合、マッピングしたロールは、LDAP サーバーに定義したロールに置き換えられます。**false** に設定した場合は、LDAP サーバーに定義したロールと、マッピングしたロールの両方がユーザーアプリケーションロールとして設定されます。デフォルトの設定は **false** です。

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[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。

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

KIE 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 KIE Server でこの機能のサポートを有効にします。

#### 前提条件

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

#### 手順

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

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

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

Prometheus メトリクス収集の設定手順は、[KIE Server の管理および監視](#)を参照してください。

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

## 4.2. (オプション) GIT フックディレクトリーの指定

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

Git フックは一般的に、アップストリームのリポジトリとの対話に使用します。Git フックを使用して、アップストリームのリポジトリにコミットをプッシュできるようにするには、アップストリームのリポジトリ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

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

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

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

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

<myapp> をテンプレートの設定時に設定したアプリケーション名に置き換えます。

- Git フックディレクトリを作成します。方法は、[Git hooks reference documentation](#) を参照してください。  
たとえば、単純な Git フックディレクトリで、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、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
```



### 注記

Business Central では **pre-commit** スクリプトはサポートされません。 **post-commit** スクリプトを使用してください。

- Git フックディレクトリを 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。
  - Git フックに1つまたは複数の固定スクリプトファイルが含まれる場合は、設定マップを使用します。以下の手順を実行してください。
    - 作成した Git フックディレクトリに移動します。
    - ディレクトリのファイルから OpenShift 設定マップを作成します。次のコマンドを実行します。

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

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

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

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

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

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

- b. Git フックが長いファイルで設定されているか、または実行可能なファイルや KJAR ファイルなどのバイナリーに依存する場合は、永続ボリュームを使用します。永続ボリュームを作成し、永続ボリューム要求を作成してボリュームを要求に関連付け、ファイルをボリュームに転送し、ボリュームを **myapp-rhdmcentr** デプロイメント設定にマウントする必要があります (**myapp** をアプリケーション名に置き換えます)。永続ボリュームの作成およびマウント方法は、[永続ボリュームの使用](#) を参照してください。永続ボリュームへのファイルのコピー方法は、[Transferring files in and out of containers](#) を参照してください。
4. 数分待機してから、プロジェクト内の Pod の一覧およびステータスを確認します。Business Central は Git フックディレクトリーが指定されるまで開始されないため、KIE Server は全く起動されない可能性があります。Process Server が起動しているかどうかを確認するには、以下のコマンドの出力で確認します。

```
oc get pods
```

稼働中の KIE 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。

### 4.3. (オプション) 自己署名証明書で HTTPS サーバーにアクセスするためのトラストストアの提供

Red Hat Decision Manager インフラストラクチャーのコンポーネントは、自己署名の HTTPS 証明書を使用するサーバーにアクセスするのに、HTTPS アクセスを使用する場合があります。たとえば、Business Central および KIE Server は、自己署名の HTTPS サーバー証明書を使用する内部の Nexus リポジトリと対話する必要がある場合があります。

このような場合は、HTTPS 接続が正常に完了するようにするには、トラストストアを使用してこれらのサービスのクライアント証明書を指定する必要があります。

Red Hat Decision Manager のコンポーネントが自己署名の HTTPS サーバー証明書を使用するサーバーと通信する必要がない場合は、この手順を飛ばして次に進んでください。

#### 手順

1. 対象の証明書を使用してトラストストアを準備します。次のコマンドを使用して、トラストストアを作成するか、証明書を既存のトラストストアに追加します。必要なすべての証明書を1つのトラストストアに追加します。

```
keytool -importcert -file certificate-file -alias alias -keyalg algorithm -keysize size -
trustcacerts -noprompt -storetype JKS -keypass truststore-password -storepass
truststore-password -keystore keystore-file
```

以下の値を置き換えます。

- **certificate-file**: トラストストアに追加する証明書のパス名。
- **alias**: トラストストアの証明書のエイリアス。トラストストアに複数の証明書を追加する場合は、全証明書に一意のエイリアスが必要です。
- **algorithm**: 証明書に使用する暗号化アルゴリズム。通常は **RSA** です。
- **size**: バイト単位での証明書キーの単位 (例: **2048**)。
- **truststore-password**: トラストストアのパスワード。
- **keystore-file**: トラストストアファイルのパス名。ファイルが存在しない場合には、このコマンドにより、新規トラストストアが作成されます。  
次のコマンド例は、**/var/certs/nexus.cer** ファイルから **/var/keystores/custom-truststore.jks** ファイルのトラストストアに証明書を追加します。トラストストアのパスワードは **mykeystorepass** です。

```
keytool -importcert -file /var/certs/nexus.cer -alias nexus-cert -keyalg RSA -keysize 2048
-trustcacerts -noprompt -storetype JKS -keypass mykeystorepass -storepass
mykeystorepass -keystore /var/keystores/custom-truststore.jks
```

2. 以下のように **oc** コマンドを使用して、トラストストアファイルでシークレットを作成します。

```
oc create secret generic truststore-secret --from-file=/var/keystores/custom-truststore.jks
```

3. お使いのインフラストラクチャーに必要なコンポーネントをデプロイする場合は、以下の例のように、シークレットをマウントしてから **JAVA\_OPTS\_APPEND** オプションを設定して Java アプリケーションのインフラストラクチャーがトラストストアを使用できるようにします。

```
oc set volume dc/myapp-rhdmcenr --add --overwrite --name=custom-truststore-volume --
mount-path /etc/custom-secret-volume --secret-name=custom-secret
```

```
oc set env dc/myapp-rhdmcenr JAVA_OPTS_APPEND='-
Djavax.net.ssl.trustStore=/etc/custom-secret-volume/custom-truststore.jks -
Djavax.net.ssl.trustStoreType=jks -Djavax.net.ssl.trustStorePassword=mykeystorepass'
```

```
oc set volume dc/myapp-kieserver --add --overwrite --name=custom-truststore-volume --
mount-path /etc/custom-secret-volume --secret-name=custom-secret
```

```
oc set env dc/myapp-kieserver JAVA_OPTS_APPEND='-
Djavax.net.ssl.trustStore=/etc/custom-secret-volume/custom-truststore.jks -
Djavax.net.ssl.trustStoreType=jks -Djavax.net.ssl.trustStorePassword=mykeystorepass'
```

**myapp** をテンプレートの設定時に指定したアプリケーション名に置き換えます。

## 4.4. (任意) LDAP ロールマッピングファイルの指定

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

### 手順

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

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

以下に例を示します。

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

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

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

**<new\_name>** は、Pod に指定するファイルの名前

(**AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES** ファイルで指定した名前と同じである必要があります) に置き換えます。また、**<existing\_name>** は、作成したファイル名に置き換えます。以下に例を示します。

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

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

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

**myapp** はアプリケーション名に置き換えます。複数の KIE 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。

## 4.5. 追加の KIE SERVER を BUSINESS CENTRAL に接続するための OPENSIFTSTARTUPSTRATEGY 設定の有効化

Red Hat Decision Manager オーサリングテンプレートを使用してデプロイされた環境では、Business Central は1つの KIE Server を管理します。KIE Server Pod をスケーリングすることができますが、すべてのコピーが同じサービスを実行します。

Business Central に追加で KIE Server を接続できます。ただし、**rhdm78-authoring.yaml** を使用して単一のオーサリング環境をデプロイした場合には、環境で **OpenShiftStartupStrategy** 設定を有効にする必要があります。**OpenShiftStartupStrategy** を有効にすると、Business Central は同じ名前空間にある KIE Server を検出し、これらの KIE Server は Business Central に接続するように設定できます。

**OpenShiftStartupStrategy** 設定では、KIE Server にサービスをデプロイすると、KIE Server デプロイメントが再度ロールアウトされます。ロールアウトが完了するまで、同じ KIE Server に別のサービスをデプロイできません。ロールアウトにはかなり時間が掛かる可能性があるため、**OpenShiftStartupStrategy** 設定によっては、オーサリング環境には適さない場合があります。

**rhdm78-authoring-ha.yaml** テンプレートを使用して高可用性オーサリング環境をデプロイした場合には、この手順を実行しないでください。この環境では、デフォルトで **OpenShiftStartupStrategy** 設定が有効です。

追加の KIE Server を Business Central に接続する場合を除き、この手順を実行しないでください。

### 前提条件

- **rhdm78-authoring.yaml** テンプレートを使用してオーサリング環境をデプロイしていること。
- **oc** ツールを使用して環境がデプロイされている OpenShift プロジェクトにログインしている。

### 手順

1. 以下のコマンドを入力して、プロジェクトにデプロイされているデプロイメント設定を表示します。

```
$ oc get dc
```

2. コマンドの出力で、Business Central Pod と KIE Server Pod のデプロイメント設定名を見つめます。
  - Business Central のデプロイメント設定の名前は、**myapp-rhdmcentr** です。**myapp** を、テンプレートの **APPLICATION\_NAME** パラメーターに設定される環境のアプリケーション名に置き換えます。
  - KIE Server のデプロイメント設定の名前は **myapp-kieserver** です。**myapp** をアプリケーション名に置き換えます。
3. 以下のコマンドを入力し、Pod で **OpenShiftStartupStrategy** 設定を有効にします。

```
$ oc env myapp-rhdmcentr KIE_SERVER_CONTROLLER_OPENSIFT_ENABLED=true
$ oc env myapp-kieserver
KIE_SERVER_STARTUP_STRATEGY=OpenShiftStartupStrategy
```

これらのコマンドで、**myapp-rhdmcentr** を Business Central デプロイメント設定名に、**myapp-kieserver** を KIE Server デプロイメント設定名に置き換えます。

4. **OpenShiftStartupStrategy** 設定を有効にする場合、デフォルトで Business Central は、オーサリングテンプレートと同じ値の **APPLICATION\_NAME** パラメーターでデプロイされる KIE Server のみを検出します。その他のアプリケーション名を持つ KIE Server を Business Central に接続する必要がある場合は、以下のコマンドを入力します。

```
$ oc env myapp-rhdmcentr
KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED=true
```

このコマンドで、**myapp-rhdmcentr** を Business Central デプロイメント設定名に置き換えます。

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

追加の管理 KIE 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。

**rhdm78-authoring.yaml** テンプレートを使用して単一のオーサリング環境をデプロイした場合には、環境内の **OpenShiftStartupStrategy** 設定を有効にして、Business Central が KIE Server に接続できるようにします。**OpenShiftStartupStrategy** 設定を有効にする方法は、「[追加の KIE Server を Business Central に接続するための OpenShiftStartupStrategy 設定の有効化](#)」を参照してください。高可用性オーサリング環境の場合は、この手順を実行する必要はありません。

KIE Server は、Maven リポジトリからサービスを読み込みます。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、サービスが読み込まれていない状態で起動します。Business Central または KIE 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。

### 4.6.1. 追加の管理 KIE Server テンプレート設定の開始

追加の管理 KIE Server をデプロイするには、**rhdm78-kieserver.yaml** テンプレートファイルを使用します。

#### 手順

1. Red Hat カスタマーポータルの [Software Downloads](#) ページから製品配信可能ファイル **rhdm-7.8.0-openshift-templates.zip** をダウンロードします。
2. **rhdm78-kieserver.yaml** テンプレートファイルを展開します。
3. 以下のいずれかの方法を使用してテンプレートのデプロイを開始します。
  - OpenShift Web UI を使用するには、OpenShift アプリケーションコンソールで **Add to Project → Import YAML / JSON** を選択してから、**rhdm78-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>/rhdm78-kieserver.yaml -p
KIE_SERVER_HTTPS_SECRET=kieserver-app-secret -p PARAMETER=value
```

このコマンドラインで、以下のように変更します。

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

## 次のステップ

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

### 4.6.2. 追加の管理 KIE 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 KIE 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 KIE Server テンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

#### 手順

1. 以下のパラメーターを設定します。
  - **Credentials secret (CREDENTIALS\_SECRET)**: 「[管理ユーザーのシークレットの作成](#)」で作成される管理ユーザーの認証情報を含むシークレットの名前。
  - **KIE Server Keystore Secret Name (KIE\_SERVER\_HTTPS\_SECRET)**: 「[KIE Server のシークレットの作成](#)」で作成した KIE Server のシークレットの名前。
  - **KIE Server Certificate Name (KIE\_SERVER\_HTTPS\_NAME)**: 「[KIE 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)**: 「[KIE 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。
  - **アプリケーション名 (APPLICATION\_NAME)**: OpenShift アプリケーションの名前。これは、Business Central Monitoring および KIE Server のデフォルト URL で使用されます。OpenShift はアプリケーション名を使用して、デプロイメント設定、サービス、ルート、ラベル、およびアーティファクトの個別のセットを作成します。同じテンプレートを同じプロジェクトで使用して複数のアプリケーションをデプロイすることもできますが、その場合はアプリケーション名を同じにすることはできません。また、アプリケーション名は、KIE 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 KIE Server をデプロイしている場合は、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)**: rhdm78-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 KIE 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 KIE Server で新規コンテナを作成します。**SNAPSHOT** バージョンをデプロイするか、または既存コンテナのアーティファクトのバージョンを変更するには、このパラメーターを **DEVELOPMENT** に設定します。
  - **ImageStream 名前空間 (IMAGE\_STREAM\_NAMESPACE)**: イメージストリームが利用可能な名前空間。OpenShift 環境でイメージストリームが利用可能な場合 (「[イメージストリームとイメージレジストリーの可用性確認](#)」を参照) は、namespace が **openshift** になります。イメージストリームファイルをインストールしている場合は、名前空間が OpenShift プロジェクトの名前になります。

## 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 KIE Server テンプレートデプロイの実行](#)」の手順に従います。

### 4.6.3. 追加の管理 KIE Server のイメージストリーム namespace の設定

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

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

#### 前提条件

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

#### 手順

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

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

同じ名前空間で Business Central インスタンスから KIE Server への接続を有効にする場合は、Business Central インスタンスに関する情報を設定する必要があります。

Business Central インスタンスは、KIE Server と同じ認証情報シークレット (**CREDENTIALS\_SECRET**) を使用して設定する必要があります。

#### 前提条件

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

#### 手順

1. 以下のパラメーターを設定します。
  - **Business Central サービスの名前 (DECISION\_CENTRAL\_SERVICE)**: Business Central の OpenShift サービス名。
2. サーバーがサービスを読み込むに使用する Maven リポジトリ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は、以下のパラメーターを設定します。
    - **Business Central の Maven サービスの名前 (DECISION\_CENTRAL\_MAVEN\_SERVICE)**: Business Central の OpenShift サービス名。

- Business Central 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 リポジトリの URL (MAVEN\_REPO\_URL)**: Business Central が使用する外部 Maven リポジトリの URL。
  - **Maven リポジトリの ID (MAVEN\_REPO\_ID)**: Maven リポジトリの ID。デフォルト値は **repo-custom** です。
  - **Maven リポジトリのユーザー名 (MAVEN\_REPO\_USERNAME)**: Maven リポジトリのユーザー名。
  - **Maven リポジトリのパスワード (MAVEN\_REPO\_PASSWORD)**: Maven リポジトリのパスワード。

## 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 KIE Server テンプレートデプロイの実行](#)」の手順に従います。

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

## 前提条件

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

## 手順

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

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

- 両リポジトリを設定した場合は、ミラーから両リポジトリのアーティファクトを除外するように **MAVEN\_MIRROR\_OF** を変更します (例: **external:\*,!repo-rhdmcentr,!repo-custom**)。 **repo-custom** は、 **MAVEN\_REPO\_ID** で設定した ID に置き換えます。

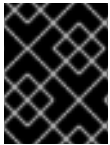
## 次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[追加の管理 KIE Server テンプレートデプロイの実行](#)」の手順に従います。

### 4.6.6. 追加の管理 KIE 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、管理 KIE Server をデプロイするようにテンプレートを設定する際に追加の設定を実行します。



#### 重要

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

## 前提条件

- Red Hat Decision Manager のレルムが RH-SSO 認証システムに作成されている。
- Red Hat Decision Manager のユーザー名およびパスワードが RH-SSO 認証システムに作成されている。利用可能なロールの一覧については、[5章 Red Hat Decision Manager ロールおよびユーザー](#)を参照してください。  
「[管理ユーザーのシークレットの作成](#)」で説明されているように、管理ユーザーのシークレットで設定されたユーザー名およびパスワードを使用してユーザーを作成する必要があります。このユーザーには **kie-server,rest-all,admin** ロールが必要です。
- デプロイしている Red Hat Decision Manager 環境の全コンポーネントに対して、クライアントが RH-SSO 認証システムに作成されている。クライアントのセットアップには、コンポーネントの URL が含まれます。環境のデプロイ後に URL を確認し、編集できます。または、Red Hat Decision Manager のデプロイメントでクライアントを作成できます。ただし、このオプションの環境に対する制御の詳細度合はより低くなります。
- 「[追加の管理 KIE Server テンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

## 手順

1. 以下のパラメーターを設定します。
  - **RH-SSO URL (SSO\_URL)**: RH-SSO の URL。
  - **RH-SSO レルム名 (SSO\_REALM)**: Red Hat Decision Manager の RH-SSO レルム。
  - **RH-SSO が無効な SSL 証明書の検証 (SSO\_DISABLE\_SSL\_CERTIFICATE\_VALIDATION)**: RH-SSO インストールで有効な HTTPS 証明書を使用していない場合は **true** に設定します。
2. 以下の手順のいずれかを実行します。

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

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[追加の管理 KIE Server テンプレートデプロイの実行](#)」の手順に従います。

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

### 4.6.7. 追加の管理 KIE 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 KIE Server をデプロイするように設定する際に追加の設定を実行します。



#### 重要

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

#### 前提条件

- LDAP システムに Red Hat Decision Manager のユーザー名およびパスワードを作成している。利用可能なロールの一覧については、[5章 Red Hat Decision Manager ロールおよびユーザー](#) を参照してください。  
「[管理ユーザーのシークレットの作成](#)」で説明されているように、管理ユーザーのシークレットで設定されたユーザー名およびパスワードを使用してユーザーを作成する必要があります。このユーザーには **kie-server,rest-all,admin** ロールが必要です。
- 「[追加の管理 KIE Server テンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

## 手順

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

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

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[追加の管理 KIE Server テンプレートデプロイの実行](#)」の手順に従います。

### 4.6.8. 追加の管理 KIE Server の Prometheus メトリクス収集の有効化

KIE 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 KIE 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 KIE Server テンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始している。

## 手順

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

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[追加の管理 KIE Server テンプレートデプロイの実行](#)」の手順に従います。

Prometheus メトリクス収集の設定手順は、[KIE Server の管理および監視](#) を参照してください。

### 4.6.9. 追加の管理 KIE Server テンプレートデプロイの実行

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

## 手順

使用している方法に応じて、以下の手順を実行します。

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

## 第5章 RED HAT DECISION MANAGER ロールおよびユーザー

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

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

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

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



### 注記

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

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

## 第6章 OPENSIFT テンプレートの参考資料

Red Hat Decision Manager には、以下の OpenShift テンプレートが含まれています。このテンプレートにアクセスするには、Red Hat カスタマーポータル[の Software Downloads ページ](#)から、製品の配信可能ファイル **rhdm-7.8.0-openshift-templates.zip** をダウンロードして展開します。

- **rhdm78-authoring.yaml** は Business Central と、Business Central に接続された KIE Server を提供します。この環境を使用して、サービスや他のビジネスアセットをオーサリングしたり、ステージングまたは実稼働環境でこれらのサービスを実行できます。このテンプレートの詳細は、「[rhdm78-authoring.yaml template](#)」を参照してください。
- **rhdm78-authoring-ha.yaml** は高可用性 Business Central と Business Central に接続された KIE Server を提供します。この環境を使用して、サービスや他のビジネスアセットをオーサリングしたり、ステージングまたは実稼働環境でこれらのサービスを実行できます。このテンプレートの詳細は、「[rhdm78-authoring-ha.yaml テンプレート](#)」を参照してください。
- **rhdm78-kieserver.yaml** は KIE Server を提供します。KIE 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 KIE 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。このテンプレートの詳細は、「[rhdm78-kieserver.yaml テンプレート](#)」を参照してください。

### 6.1. RHDM78-AUTHORING.YAML TEMPLATE

Red Hat Decision Manager 7.8 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)

#### 6.1.1. パラメーター

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

変数名	イメージの環境変数	説明	値の例	必須
<b>APPLICATION_NAME</b>	—	アプリケーションの名前。	myapp	True
<b>CREDENTIALS_SECRET</b>	—	KIE_ADMIN_USER 値および KIE_ADMIN_PWD 値を含むシークレット。	rhpm-credentials	True
<b>KIE_SERVER_CONTROLLER_TOKEN</b>	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	ベアラ認証用の KIE Server コントローラトークン。 (org.kie.server.controller.token システムプロパティを設定)	—	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。 (org.kie.server.bypass.auth.user システムプロパティを設定)	false	False
<b>KIE_SERVER_MODE</b>	<b>KIE_SERVER_MODE</b>	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナ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)	<b>DEVELOPMENT</b>	False
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティ kie.mbeans および kie.scanner.mbeans を設定)。	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE Server のクラスフィルター (org.drools.server.filter.classes システムプロパティを設定)	true	False

変数名	イメージの環境変数	説明	値の例	必須
<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	false に設定すると、prometheus サーバー拡張が有効になります。 (org.kie.prometheus.server.ext.disabled システムプロパティを設定)	false	False
<b>DECISION_CENTRAL_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Decision Central の http サービスルートのカスタムホスト名。デフォルトホスト名は空白にします (例: insecure- <application-name>-rhdmcentr- <project>.<default-domain-suffix>)。	—	False
<b>DECISION_CENTRAL_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Decision Central の https サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr- <project>.<default-domain-suffix>)。	—	False
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	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
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	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
<b>DECISION_CENTRAL_HTTPS_SECRET</b>	—	Decision Central のキーストアファイルが含まれるシークレットの名前。	decisioncentral-app-secret	True
<b>DECISION_CENTRAL_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	keystore.jks	False
<b>DECISION_CENTRAL_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False
<b>DECISION_CENTRAL_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード。	mykeystorepass	False
<b>KIE_SERVER_HTTPS_SECRET</b>	—	キーストアファイルを含むシークレット名	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード。	mykeystorepass	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED</b>	<b>KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED</b>	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)。	false	False
<b>KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE</b>	<b>KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE</b>	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。 (org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティを設定します)	true	False
<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	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)	60000	False

変数名	イメージの環境変数	説明	値の例	必須
<b>IMAGE_STREAM_NAMESPACE</b>	—	Red Hat Decision Manager イメージの ImageStream がインストールされている名前空間。これらの ImageStreams は通常 OpenShift の名前空間にインストールされています。ImageStream を別の名前空間/プロジェクトにインストールしている場合に限りこのパラメーターを変更する必要があります。	openshift	True
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	—	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm-kieserver-rhel8 です。	rhdm-kieserver-rhel8	True
<b>IMAGE_STREAM_TAG</b>	—	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 7.8.0 です。	7.8.0	True
<b>MAVEN_MIRROR_URL</b>	<b>MAVEN_MIRROR_URL</b>	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	—	False
<b>MAVEN_MIRROR_OF</b>	<b>MAVEN_MIRROR_OF</b>	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
<b>MAVEN_REPO_ID</b>	<b>MAVEN_REPO_ID</b>	Maven リポジトリに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	repo-custom	False
<b>MAVEN_REPO_URL</b>	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/	False
<b>MAVEN_REPO_USERNAME</b>	<b>MAVEN_REPO_USERNAME</b>	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
<b>MAVEN_REPO_PASSWORD</b>	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	—	False
<b>GIT_HOOKS_DIR</b>	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリ (必要な場合)。	<b>/opt/kie/data/git/hooks</b>	False

変数名	イメージの環境変数	説明	値の例	必須
<b>DECISION_CENTRAL_VOLUME_CAPACITY</b>	—	Decision Central のランタイムデータに向けた永続ストレージのサイズ。	1Gi	True
<b>DECISION_CENTRAL_MEMORY_LIMIT</b>	—	Decision Central コンテナのメモリー制限。	2Gi	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	—	KIE Server のコンテナのメモリー制限。	1Gi	False
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL。	https://rh-sso.example.com/auth	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO レルム名。	—	False
<b>DECISION_CENTRAL_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	—	False
<b>DECISION_CENTRAL_SSO_SECRET</b>	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット。	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	—	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット。	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	クライアント作成に使用する RH-SSO レルムの管理者ユーザー名 (存在しない場合)。	—	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	—	False

変数名	イメージの環境変数	説明	値の例	必須
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性。	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント。	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報	パスワード	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	—	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	(uid={0})	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。	<b>SUBTREE_SCOPE</b>	False
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	10000	False
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されます。	distinguishedName	False
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定されている場合、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、DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	true	False

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

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

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

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

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

## 6.1.2. 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。

### 6.1.2.1. サービス

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

サービス	ポート	名前	説明
<b>\${APPLICATION_NAME}-rhdmcentr</b>	8080	http	Decision Central のすべての Web サーバーのポート。
	8443	https	

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

### 6.1.2.2. 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 (任意) で設定されます。詳細は、[Openshift ドキュメント](#) を参照してください。

サービス	セキュリティ	ホスト名
insecure- \${APPLICATION_NAME}- rhdmcentr-http	なし	<b>\${DECISION_CENTRAL_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}- rhdmcentr-https</b>	TLS パススルー	<b>\${DECISION_CENTRAL_HOSTNAME_HTTPS}</b>
insecure- \${APPLICATION_NAME}- kieserver-http	なし	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}- kieserver-https</b>	TLS パススルー	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

### 6.1.2.3. 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、トリガーされたイベントに対応するために作成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

#### 6.1.2.3.1. 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
<b>\${APPLICATION_NAME}-rhdmcentr</b>	ImageChange
<b>\${APPLICATION_NAME}-kieserver</b>	ImageChange

### 6.1.2.3.2. レプリカ

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

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

### 6.1.2.3.3. Pod テンプレート

#### 6.1.2.3.3.1. 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>

#### 6.1.2.3.3.2. イメージ

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

#### 6.1.2.3.3.3. Readiness Probe

`${APPLICATION_NAME}-rhdmcentr`

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

`${APPLICATION_NAME}-kieserver`

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

#### 6.1.2.3.3.4. Liveness Probe

`${APPLICATION_NAME}-rhdmcentr`

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

`${APPLICATION_NAME}-kieserver`

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

#### 6.1.2.3.3.5. 公開されたポート

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

#### 6.1.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
<b><code>\${APPLICATION_NAME}-rhdmcentr</code></b>	<b>APPLICATION_USE_RS_PROPERTIES</b>	–	<code>/opt/kie/data/configuration/application-users.properties</code>
	<b>APPLICATION_ROLES_PROPERTIES</b>	–	<code>/opt/kie/data/configuration/application-roles.properties</code>
	<b>KIE_ADMIN_USER</b>	管理ユーザー名。	認証情報のシークレットに合わせて設定
	<b>KIE_ADMIN_PWD</b>	管理ユーザーのパスワード。	認証情報のシークレットに合わせて設定
	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー <code>kie.mbeans</code> および <code>kie.scanner.mbeans</code> を設定)。	<b><code>\${KIE_MBEANS}</code></b>

デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_ENABLED</b>	–	false
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED</b>	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)。	<b>\${KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED}</b>
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_PREFER_KIESERVER_SERVICE</b>	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。 (org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティを設定します)	<b>\${KIE_SERVER_CONTROLLER_OPENSIFT_PREFER_KIESERVER_SERVICE}</b>
	<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	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)	<b>\${KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL}</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	ベアラー認証用の KIE Server コントローラートークン。 (org.kie.server.controller.token システムプロパティを設定)	<b>\${KIE_SERVER_CONTROLLER_TOKEN}</b>
	<b>WORKBENCH_ROUTE_NAME</b>	–	<b>\${APPLICATION_NAME}-rhdmcenr</b>

デプロイメント	変数名	説明	値の例
	<b>MAVEN_MIRROR_URL</b>	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	<b>\${MAVEN_MIRROR_URL}</b>
	<b>MAVEN_REPO_ID</b>	Maven リポジトリに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	<b>\${MAVEN_REPO_ID}</b>
	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<b>\${MAVEN_REPO_URL}</b>
	<b>MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするためのユーザー名 (必要な場合)。	<b>\${MAVEN_REPO_USERNAME}</b>
	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	<b>\${MAVEN_REPO_PASSWORD}</b>
	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリー (必要な場合)。	<b>\${GIT_HOOKS_DIR}</b>
	<b>HTTPS_KEYSTORE_DIR</b>	—	<b>/etc/decisioncentral-secret-volume</b>

デプロイメント	変数名	説明	値の例
	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイル名	<b>\${DECISION_CENTRAL_HTTPS_KEYSTORE}</b>
	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	<b>\${DECISION_CENTRAL_HTTPS_NAME}</b>
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	<b>\${DECISION_CENTRAL_HTTPS_PASSWORD}</b>
	<b>SSO_URL</b>	RH-SSO URL。	<b>\${SSO_URL}</b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レルム名。	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット。	<b>\${DECISION_CENTRAL_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	<b>\${DECISION_CENTRAL_SSO_CLIENT}</b>
	<b>SSO_USERNAME</b>	クライアント作成に使用する RH-SSO レルムの管理者ユーザー名 (存在しない場合)。	<b>\${SSO_USERNAME}</b>
	<b>SSO_PASSWORD</b>	クライアント作成に使用する RH-SSO レルムの管理者のパスワード。	<b>\${SSO_PASSWORD}</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性。	<b>\${SSO_PRINCIPAL_ATTRIBUTE}</b>

デプロイメント	変数名	説明	値の例
	<b>HOSTNAME_HTTP</b>	Decision Central の http サービスルートのカスタムホスト名。デフォルトホスト名は空白にします (例: insecure- <application-name>- rhdmcentr- <project>. <default-domain- suffix>)。	<b><code>\${DECISION_CENTRAL_HOSTNAME_HTTP}</code></b>
	<b>HOSTNAME_HTTPS</b>	Decision Central の https サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr- <project>.<default-domain- suffix>)。	<b><code>\${DECISION_CENTRAL_HOSTNAME_HTTPS}</code></b>
	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント。	<b><code>\${AUTH_LDAP_URL}</code></b>
	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN	<b><code>\${AUTH_LDAP_BIND_DN}</code></b>
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報	<b><code>\${AUTH_LDAP_BIND_CREDENTIAL}</code></b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	<b><code>\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}</code></b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	<b><code>\${AUTH_LDAP_BASE_CTX_DN}</code></b>

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

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

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

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

デプロイメント	変数名	説明	値の例
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	このパラメーターがある場合には、RoleMapping のログインモジュールで、指定したファイルを使用するように設定します。このパラメーターは、ロールを置換ロールに対してマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	<b>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	現在のロールを追加するか、マップされたロールに現在のロールを置き換えるか。true に設定した場合は、置き換えられます。	<b>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</b>
<b>\${APPLICATION_NAME}-kieserver</b>	<b>WORKBENCH_SERVICE_NAME</b>	—	<b>\${APPLICATION_NAME}-rhdmcenr</b>
	<b>KIE_ADMIN_USER</b>	管理ユーザー名。	認証情報のシークレットに合わせて設定
	<b>KIE_ADMIN_PWD</b>	管理ユーザーのパスワード。	認証情報のシークレットに合わせて設定
	<b>KIE_SERVER_MODE</b>	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナ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)	<b>\${KIE_SERVER_MODE}</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	<b>\${KIE_MBEANS}</b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE Server のクラスフィルター (org.drools.server.filter.classes システムプロパティーを設定)	<b>\${DROOLS_SERVER_FILTER_CLASSES}</b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	false に設定すると、prometheus サーバー拡張が有効になります。 (org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	<b>\${PROMETHEUS_SERVER_EXT_DISABLED}</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。 (org.kie.server.bypass.auth.user システムプロパティーを設定)	<b>\${KIE_SERVER_BYPASS_AUTH_USER}</b>
	<b>KIE_SERVER_CONTROLLER_SERVICE</b>	—	<b>\${APPLICATION_NAME}-rhdmcentr</b>
	<b>KIE_SERVER_CONTROLLER_PROTOCOL</b>	—	ws
	<b>KIE_SERVER_ID</b>	—	—
	<b>KIE_SERVER_ROUTE_NAME</b>	—	insecure-\${APPLICATION_NAME}-kieserver
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	—	ControllerBasedStartupStrategy

デプロイメント	変数名	説明	値の例
	<b>MAVEN_MIRROR_URL</b>	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	<b>\${MAVEN_MIRROR_URL}</b>
	<b>MAVEN_MIRROR_OF</b>	KIE Server の Maven ミラー設定。	<b>\${MAVEN_MIRROR_OF}</b>
	<b>MAVEN_REPOS</b>	—	RHDMCENTR,EXTERNAL
	<b>RHDMCENTR_MAVEN_REPO_ID</b>	—	repo-rhdmcentr
	<b>RHDMCENTR_MAVEN_REPO_SERVICE</b>	—	<b>\${APPLICATION_NAME}-rhdmcentr</b>
	<b>RHDMCENTR_MAVEN_REPO_PATH</b>	—	<b>/maven2/</b>
	<b>RHDMCENTR_MAVEN_REPO_USERNAME</b>	—	認証情報のシークレットに合わせて設定
	<b>RHDMCENTR_MAVEN_REPO_PASSWORD</b>	—	認証情報のシークレットに合わせて設定

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

デプロイメント	変数名	説明	値の例
	<b>SSO_REALM</b>	RH-SSO レalm名。	<b><code>\${SSO_REALM}</code></b>
	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット。	<b><code>\${KIE_SERVER_SSO_SECRET}</code></b>
	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	<b><code>\${KIE_SERVER_SSO_CLIENT}</code></b>
	<b>SSO_USERNAME</b>	クライアント作成に使用する RH-SSO レalmの管理者ユーザー名 (存在しない場合)。	<b><code>\${SSO_USERNAME}</code></b>
	<b>SSO_PASSWORD</b>	クライアント作成に使用する RH-SSO レalmの管理者のパスワード。	<b><code>\${SSO_PASSWORD}</code></b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b><code>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</code></b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性。	<b><code>\${SSO_PRINCIPAL_ATTRIBUTE}</code></b>
	<b>HOSTNAME_HTTP</b>	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>)。	<b><code>\${KIE_SERVER_HOSTNAME_HTTP}</code></b>
	<b>HOSTNAME_HTTPS</b>	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>)。	<b><code>\${KIE_SERVER_HOSTNAME_HTTPS}</code></b>
	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント。	<b><code>\${AUTH_LDAP_URL}</code></b>

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

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

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

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

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

#### 6.1.2.3.3.7. ボリューム

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

#### 6.1.2.4. 外部の依存関係

##### 6.1.2.4.1. ボリューム要求

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

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

#### 6.1.2.4.2. 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
```

## 6.2. RHDM78-AUTHORING-HA.YAML テンプレート

Red Hat Decision Manager 7.8 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)

### 6.2.1. パラメーター

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

変数名	イメージの環境変数	説明	値の例	必須
<b>APPLICATION_NAME</b>	—	アプリケーションの名前。	myapp	True
<b>CREDENTIALS_SECRET</b>	—	KIE_ADMIN_USER 値および KIE_ADMIN_PWD 値を含むシークレット。	rhpm-credentials	True
<b>KIE_SERVER_CONTROLLER_TOKEN</b>	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	ベアラ認証用の KIE Server コントローラートークン。 (org.kie.server.controller.token システムプロパティーを設定)	—	False
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。 (org.kie.server.bypass.auth.user システムプロパティーを設定)	false	False

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

変数名	イメージの環境変数	説明	値の例	必須
<b>DECISION_CENTRAL_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Decision Central の http サービスルートのカスタムホスト名。デフォルトホスト名は空白にします (例: insecure- <application-name>-rhdmcentr- <project>.<default-domain-suffix>)。	—	False
<b>DECISION_CENTRAL_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Decision Central の https サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合には空白にします (例: <application-name>-rhdmcentr- <project>.<default-domain-suffix>)。	—	False
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	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
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	KIE Server の https サービスルートのカスタムホスト名。デフォルトホスト名の場合は空白にします (例: <application-name>-kieserver- <project>.<default-domain-suffix>)。	—	False

変数名	イメージの環境変数	説明	値の例	必須
<b>DECISION_CENTRAL_HTTPS_SECRET</b>	–	Decision Central のキーストアファイルが含まれるシークレットの名前。	decisioncentral-app-secret	True
<b>DECISION_CENTRAL_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	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
<b>DECISION_CENTRAL_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	Decision Central のサーバー証明書に関連付けられている名前。	jboss	False
<b>DECISION_CENTRAL_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	Decision Central のキーストアおよび証明書のパスワード。	mykeystorepass	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	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
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	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
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	KIE Server のサーバー証明書に関連付けられている名前。	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	KIE Server のキーストアおよび証明書のパスワード。	mykeystorepass	False
<b>APPFORMER_JMS_BROKER_USER</b>	<b>APPFORMER_JMS_BROKER_USER</b>	JMS ブローカーに接続するためのユーザー名。	jmsBrokerUser	True
<b>APPFORMER_JMS_BROKER_PASSWORD</b>	<b>APPFORMER_JMS_BROKER_PASSWORD</b>	JMS ブローカーに接続するためのパスワード。	–	True

変数名	イメージの環境変数	説明	値の例	必須
<b>DATAGRID_IMAGE</b>	—	DataGrid イメージ。	registry.redhat.io/jboss-datagrid-7/datagrid73-openshift:1.5	True
<b>DATAGRID_CPU_LIMIT</b>	—	DataGrid Container の CPU 制限。	1000m	True
<b>DATAGRID_MEMORY_LIMIT</b>	—	DataGrid コンテナのメモリー制限。	2Gi	True
<b>DATAGRID_VOLUME_CAPACITY</b>	—	DataGrid のランタイムデータの永続ストレージのサイズ。	1Gi	True
<b>AMQ_BROKER_IMAGE</b>	—	AMQ ブローカーイメージ。	registry.redhat.io/amq7/amq-broker:7.6	True
<b>AMQ_ROLE</b>	—	標準ブローカーユーザーのユーザーロール。	admin	True
<b>AMQ_NAME</b>	—	ブローカーの名前。	broker	True
<b>AMQ_GLOBAL_MAX_SIZE</b>	—	メッセージデータが使用可能な最大メモリー量を指定します。値が指定されていない場合は、システムのメモリーの半分が割り当てられます。	10 gb	False
<b>AMQ_VOLUME_CAPACITY</b>	—	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
<b>AMQ_REPLICAS</b>	—	クラスターのブローカーレプリカ数。	2	True

変数名	イメージの環境変数	説明	値の例	必須
<b>DECISION_CENTRAL_CONTAINER_REPLICAS</b>	—	Decision Central Container Replicas は、起動する Decision Central のコンテナ数を定義します。	2	True
<b>KIE_SERVER_CONTAINER_REPLICAS</b>	—	KIE Server Container Replicas は、起動する KIE Server のコンテナ数を定義します。	2	True
<b>KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED</b>	<b>KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED</b>	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)。	false	False
<b>KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE</b>	<b>KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE</b>	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。 (org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティを設定します)	true	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	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)	60000	False
<b>IMAGE_STREAM_NAMESPACE</b>	—	Red Hat Decision Manager イメージの ImageStream がインストールされている名前空間。これらの ImageStreams は通常 OpenShift の名前空間にインストールされています。ImageStream を別の名前空間/プロジェクトにインストールしている場合に限りこのパラメーターを変更する必要があります。	openshift	True
<b>DECISION_CENTRAL_IMAGE_STREAM_NAME</b>	—	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
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	—	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm-kieserver-rhel8 です。	rhdm-kieserver-rhel8	True
<b>IMAGE_STREAM_TAG</b>	—	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 7.8.0 です。	7.8.0	True

変数名	イメージの環境変数	説明	値の例	必須
<b>MAVEN_MIRROR_URL</b>	<b>MAVEN_MIRROR_URL</b>	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	—	False
<b>MAVEN_MIRROR_OF</b>	<b>MAVEN_MIRROR_OF</b>	KIE Server の Maven ミラー設定。	external:*,!repo-rhdmcentr	False
<b>MAVEN_REPO_ID</b>	<b>MAVEN_REPO_ID</b>	Maven リポジトリに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	repo-custom	False
<b>MAVEN_REPO_URL</b>	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	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
<b>MAVEN_REPO_USERNAME</b>	<b>MAVEN_REPO_USERNAME</b>	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
<b>MAVEN_REPO_PASSWORD</b>	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	—	False
<b>GIT_HOOKS_DIR</b>	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリー (必要な場合)。	<b>/opt/kie/data/git/hooks</b>	False
<b>DECISION_CENTRAL_VOLUME_CAPACITY</b>	—	Decision Central のランタイムデータに向けた永続ストレージのサイズ。	1Gi	True
<b>DECISION_CENTRAL_MEMORY_LIMIT</b>	—	Decision Central コンテナのメモリー制限。	8Gi	True
<b>DECISION_CENTRAL_JAVA_MAX_MEM_RATIO</b>	<b>JAVA_MAX_MEM_RATIO</b>	Decision Central コンテナ JVM の最大メモリー比率。 <b>-Xmx</b> 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の範囲の上限が 80% であることを意味します。 <b>-Xmx</b> 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
<b>DECISION_CENTRAL_CPU_LIMIT</b>	—	Decision Central コンテナの CPU 制限。	2000m	True
<b>KIE_SERVER_MEMORY_LIMIT</b>	—	KIE Server のコンテナのメモリー制限。	1Gi	True

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_CPU_LIMIT</b>	–	KIE Server コンテナの CPU 制限。	1000m	True
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL。	https://rh-sso.example.com/auth	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO レalm 名。	–	False
<b>DECISION_CENTRAL_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	–	False
<b>DECISION_CENTRAL_SSO_SECRET</b>	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット。	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	–	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット。	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	クライアント作成に使用する RH-SSO レalm の管理者ユーザー名 (存在しない場合)。	–	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	クライアント作成に使用する RH-SSO レalm の管理者のパスワード。	–	False
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	false	False

変数名	イメージの環境変数	説明	値の例	必須
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性。	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	認証用に接続する LDAP エンドポイント。	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	認証に使用するバインド DN	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	認証に使用する LDAP の認証情報	パスワード	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	パスワードの復号に使用する JaasSecurityDomain の JMX ObjectName。	—	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	ユーザー検索を開始する最上位コンテキストの LDAP ベース DN	ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	認証するユーザーのコンテキストの検索に使用する LDAP 検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。検索フィルターの一般的な例は (uid={0}) です。	(uid={0})	False
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	使用する検索範囲。	<b>SUBTREE_SCOPE</b>	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	10000	False
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自身の DN に正しいユーザーマッピングを妨げる特殊文字 (バックスラッシュなど) が含まれる場合に必要になることがあります。属性が存在しない場合は、エントリーの DN が使用されます。	distinguishedName	False
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	DN がユーザー名に対して解析されるかどうかを示すフラグ。true に設定されている場合、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、DN はユーザー名に対して解析されません。このオプションは、usernameBeginString および usernameEndString とともに使用されます。	true	False

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

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

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

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

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

## 6.2.2. 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。

### 6.2.2.1. サービス

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

サービス	ポート	名前	説明
<b>\${APPLICATION_NAME}-rhdmcentr</b>	8080	http	Decision Central のすべての Web サーバーのポート。
	8443	https	

サービス	ポート	名前	説明
<b>\${APPLICATION_NAME}-rhdmcentr-ping</b>	8888	ping	rhdmcentr クラスターリングの JGroups ping ポート。
<b>\${APPLICATION_NAME}-datagrid-ping</b>	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。
<b>\${APPLICATION_NAME}-datagrid</b>	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。
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	すべての KIE Server Web サーバーのポート。
	8443	https	
<b>\${APPLICATION_NAME}-amq-tcp</b>	61616	–	ブローカーの OpenWire ポート。
<b>ping</b>	8888	–	amq クラスターリングの JGroups ping ポート。

#### 6.2.2.2. 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、サービスセクター、セキュリティ設定 (任意) で設定されます。詳細は、[Openshift ドキュメント](#) を参照してください。

サービス	セキュリティ	ホスト名
insecure- <b>\${APPLICATION_NAME}-rhdmcentr-http</b>	なし	<b>\${DECISION_CENTRAL_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-rhdmcentr-https</b>	TLS パススルー	<b>\${DECISION_CENTRAL_HOSTNAME_HTTPS}</b>
insecure- <b>\${APPLICATION_NAME}-kieserver-http</b>	なし	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS パススルー	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

### 6.2.2.3. 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、トリガーされたイベントに対応するために作成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

#### 6.2.2.3.1. 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

#### 6.2.2.3.2. レプリカ

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

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

#### 6.2.2.3.3. Pod テンプレート

##### 6.2.2.3.3.1. 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>

##### 6.2.2.3.3.2. イメージ

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

#### 6.2.2.3.3.3. Readiness Probe

**\${APPLICATION\_NAME}-rhdmcentr**

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

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

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

#### 6.2.2.3.3.4. Liveness Probe

**\${APPLICATION\_NAME}-rhdmcentr**

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

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

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

#### 6.2.2.3.3.5. 公開されたポート

デプロイメント	名前	ポート	プロトコル
<b>\${APPLICATION_NAME}-rhdmcentr</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	ping	8888	<b>TCP</b>
<b>\${APPLICATION_NAME}-kieserver</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>

## 6.2.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
<b>\${APPLICATION_NAME}-rhdmcentr</b>	<b>APPLICATION_USERS_PROPERTIES</b>	—	<b>/opt/kie/data/configuration/application-users.properties</b>
	<b>APPLICATION_ROLES_PROPERTIES</b>	—	<b>/opt/kie/data/configuration/application-roles.properties</b>
	<b>KIE_ADMIN_USER</b>	管理ユーザー名。	認証情報のシークレットに合わせて設定
	<b>KIE_ADMIN_PWD</b>	管理ユーザーのパスワード。	認証情報のシークレットに合わせて設定
	<b>KIE_MBEANS</b>	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	<b>\${KIE_MBEANS}</b>
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_ENABLED</b>	—	true
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED</b>	true に設定すると、KIE Server のグローバル検出機能はオンになります (org.kie.server.controller.openshift.global.discovery.enabled システムプロパティーを設定)。	<b>\${KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED}</b>
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_PREFER_KIESERVER_SERVICE</b>	Business Central の OpenShift 統合がオンの場合は、このパラメーターを true に設定すると、OpenShift 内部サービスエンドポイント経由での KIE Server への接続が有効になります。(org.kie.server.controller.openshift.prefer.kieserver.service システムプロパティーを設定します)	<b>\${KIE_SERVER_CONTROLLER_OPENSIFT_PREFER_KIESERVER_SERVICE}</b>

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

デプロイメント	変数名	説明	値の例
	<b>MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<b>\${MAVEN_REPO_URL}</b>
	<b>MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするためのユーザー名 (必要な場合)。	<b>\${MAVEN_REPO_USERNAME}</b>
	<b>MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	<b>\${MAVEN_REPO_PASSWORD}</b>
	<b>GIT_HOOKS_DIR</b>	git フックに使用するディレクトリー (必要な場合)。	<b>\${GIT_HOOKS_DIR}</b>
	<b>HTTPS_KEYSTORE_DIR</b>	—	<b>/etc/decisioncentral-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	Decision Central のシークレット内のキーストアファイルの名前。	<b>\${DECISION_CENTRAL_HTTPS_KEYSTORE}</b>
	<b>HTTPS_NAME</b>	Decision Central のサーバー証明書に関連付けられている名前。	<b>\${DECISION_CENTRAL_HTTPS_NAME}</b>
	<b>HTTPS_PASSWORD</b>	Decision Central のキーストアおよび証明書のパスワード。	<b>\${DECISION_CENTRAL_HTTPS_PASSWORD}</b>
	<b>JGROUPS_PING_PROTOCOL</b>	—	<b>openshift.DNS_PING</b>
	<b>OPENSIFT_DNS_PING_SERVICE_NAME</b>	—	<b>\${APPLICATION_NAME}-rhdmcentr-ping</b>
	<b>OPENSIFT_DNS_PING_SERVICE_PORT</b>	—	<b>8888</b>
	<b>APPFORMER_INFISPAN_SERVICE_NAME</b>	—	<b>\${APPLICATION_NAME}-datagrid</b>
	<b>APPFORMER_INFISPAN_PORT</b>	—	<b>11222</b>

デプロイメント	変数名	説明	値の例
	<b>APPFORMER_JMS_BROKER_ADDRESS</b>	–	<b>\${APPLICATION_NAME}-amq-tcp</b>
	<b>APPFORMER_JMS_BROKER_PORT</b>	–	61616
	<b>APPFORMER_JMS_BROKER_USER</b>	JMS ブローカーに接続するためのユーザー名。	<b>\${APPFORMER_JMS_BROKER_USER}</b>
	<b>APPFORMER_JMS_BROKER_PASSWORD</b>	JMS ブローカーに接続するためのパスワード。	<b>\${APPFORMER_JMS_BROKER_PASSWORD}</b>
	<b>JAVA_MAX_MEM_RATIO</b>	Decision Central コンテナ 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。	<b>\${DECISION_CENTRAL_JAVA_MAX_MEM_RATIO}</b>
	<b>SSO_URL</b>	RH-SSO URL。	<b>\${SSO_URL}</b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レalm 名。	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	Decision Central RH-SSO クライアントシークレット。	<b>\${DECISION_CENTRAL_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	Decision Central RH-SSO クライアント名。	<b>\${DECISION_CENTRAL_SSO_CLIENT}</b>
	<b>SSO_USERNAME</b>	クライアント作成に使用する RH-SSO レalm の管理者ユーザー名 (存在しない場合)。	<b>\${SSO_USERNAME}</b>

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

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

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

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

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

デプロイメント	変数名	説明	値の例
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	このパラメーターがある場合には、RoleMapping のログインモジュールで、指定したファイルを使用するように設定します。このパラメーターは、ロールを置換ロールに対してマップするプロパティファイルまたはリソースの完全修飾ファイルパスまたはファイル名を定義します。形式は original_role=role1,role2,role3 になります。	<b>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	現在のロールを追加するか、マップされたロールに現在のロールを置き換えるか。true に設定した場合は、置き換えられます。	<b>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</b>
<b>\${APPLICATION_NAME}-kieserver</b>	<b>WORKBENCH_SERVICE_NAME</b>	—	<b>\${APPLICATION_NAME}-rhdmcenr</b>
	<b>KIE_ADMIN_USER</b>	管理ユーザー名。	認証情報のシークレットに合わせて設定
	<b>KIE_ADMIN_PWD</b>	管理ユーザーのパスワード。	認証情報のシークレットに合わせて設定
	<b>KIE_SERVER_MODE</b>	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナ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)	<b>\${KIE_SERVER_MODE}</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_MBEANS</b>	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	<b><code>\${KIE_MBEANS}</code></b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE Server クラスのフィルタリング。 (org.drools.server.filter.classes システムプロパティーを設定)	<b><code>\${DROOLS_SERVER_FILTER_CLASSES}</code></b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	false に設定すると、prometheus サーバー拡張が有効になります。 (org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	<b><code>\${PROMETHEUS_SERVER_EXT_DISABLED}</code></b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。 (org.kie.server.bypass.auth.user システムプロパティーを設定)	<b><code>\${KIE_SERVER_BYPASS_AUTH_USER}</code></b>
	<b>KIE_SERVER_CONTROLLER_SERVICE</b>	—	<b><code>\${APPLICATION_NAME}-rhdmcentr</code></b>
	<b>KIE_SERVER_CONTROLLER_PROTOCOL</b>	—	ws
	<b>KIE_SERVER_ID</b>	—	—
	<b>KIE_SERVER_ROUTE_NAME</b>	—	insecure- <code>\${APPLICATION_NAME}</code> -kieserver
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	—	OpenShiftStartupStrategy

デプロイメント	変数名	説明	値の例
	<b>MAVEN_MIRROR_URL</b>	Decision Central および KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合、このミラーにはサービスのビルドおよびデプロイに必要なすべてのアーティファクトを含める必要があります。	<b>\${MAVEN_MIRROR_URL}</b>
	<b>MAVEN_MIRROR_OF</b>	KIE Server の Maven ミラー設定。	<b>\${MAVEN_MIRROR_OF}</b>
	<b>MAVEN_REPOS</b>	—	RHDMCENTR,EXTERNAL
	<b>RHDMCENTR_MAVEN_REPO_ID</b>	—	repo-rhdmcentr
	<b>RHDMCENTR_MAVEN_REPO_SERVICE</b>	—	<b>\${APPLICATION_NAME}-rhdmcentr</b>
	<b>RHDMCENTR_MAVEN_REPO_PATH</b>	—	<b>/maven2/</b>
	<b>RHDMCENTR_MAVEN_REPO_USERNAME</b>	—	認証情報のシークレットに合わせて設定
	<b>RHDMCENTR_MAVEN_REPO_PASSWORD</b>	—	認証情報のシークレットに合わせて設定

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

デプロイメント	変数名	説明	値の例
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レalm 名。	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット。	<b>\${KIE_SERVER_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	<b>\${KIE_SERVER_SSO_CLIENT}</b>
	<b>SSO_USERNAME</b>	クライアント作成に使用する RH-SSO レalm の管理者ユーザー名 (存在しない場合)。	<b>\${SSO_USERNAME}</b>
	<b>SSO_PASSWORD</b>	クライアント作成に使用する RH-SSO レalm の管理者のパスワード。	<b>\${SSO_PASSWORD}</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性。	<b>\${SSO_PRINCIPAL_ATTRIBUTE}</b>
	<b>HOSTNAME_HTTP</b>	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>)。	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
	<b>HOSTNAME_HTTPS</b>	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>)。	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

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

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

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

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

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

## 6.2.2.3.3.7. ボリューム

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

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

## 6.2.2.4. 外部の依存関係

### 6.2.2.4.1. ボリューム要求

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

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

### 6.2.2.4.2. 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

### 6.2.2.4.3. クラスターリング

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

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

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

1. **OPENSIFT\_DNS\_PING\_SERVICE\_NAME** 環境変数は、クラスターの ping サービス名に設定する必要があります (上記の表を参照)。設定していない場合には、サーバーは単一ノードのクラスター (ノードが 1 つのクラスター) のように機能します。
2. **OPENSIFT\_DNS\_PING\_SERVICE\_PORT** 環境変数は、ping サービスを公開するポート番号に設定する必要があります (上記の表を参照)。**DNS\_PING** プロトコルは可能な場合には SRV レコードからのポートを識別しようとします。デフォルト値は 8888 です。
3. ping ポートを公開する ping サービスは定義する必要があります。このサービスはヘッドレス (ClusterIP=None) で、以下の条件を満たす必要があります。

- a. ポートは、ポート検出が機能するように、名前を指定する必要があります。
- b. **service.alpha.kubernetes.io/tolerate-unready-endpoints** を **"true"** に指定してアノテーションを設定する必要があります。このアノテーションを省略すると、起動時にノードごとに独自の単一ノードのクラスターが形成され、(起動後でないと他のノードが検出されない)ので、起動後にこのクラスターが他のノードのクラスターにマージされます。

## DNS\_PING で使用する ping サービスの例

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

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

1. **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6.1 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
```

## 6.3. RHDM78-KIESERVER.YAML テンプレート

Red Hat Decision Manager 7.8 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)

### 6.3.1. パラメーター

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

変数名	イメージの環境変数	説明	値の例	必須
<b>APPLICATION_NAME</b>	—	アプリケーションの名前。	myapp	True
<b>MAVEN_MIRROR_URL</b>	<b>MAVEN_MIRROR_URL</b>	KIE Server が使用する必要のある Maven ミラー。ミラーを設定する場合には、このミラーにはサービスのデプロイに必要なすべてのアーティファクトを含める必要があります。	—	False
<b>MAVEN_MIRROR_OF</b>	<b>MAVEN_MIRROR_OF</b>	KIE Server の Maven ミラー設定。	external:*	False
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	Maven リポジトリに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	repo-custom	False

変数名	イメージの環境変数	説明	値の例	必須
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/	True
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするためのユーザー名 (必要な場合)。	—	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	—	False
<b>DECISION_CENTRAL_SERVICE</b>	<b>WORKBENCH_SERVICE_NAME</b>	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するのに使用される任意の Decision Central のサービス名。	myapp-rhdmcentr	False
<b>CREDENTIALS_SECRET</b>	—	KIE_ADMIN_USER 値および KIE_ADMIN_PWD 値を含むシークレット。	rhpm-credentials	True

変数名	イメージの環境変数	説明	値の例	必須
<b>IMAGE_STREAM_NAMESPACE</b>	—	Red Hat Decision Manager イメージの ImageStream がインストールされている名前空間。これらの ImageStreams は通常 OpenShift の名前空間にインストールされています。ImageStream を別の名前空間/プロジェクトにインストールしている場合に限りこのパラメーターを変更する必要があります。	openshift	True
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	—	KIE Server に使用するイメージストリームの名前。デフォルトは rhdm-kieserver-rhel8 です。	rhdm-kieserver-rhel8	True
<b>IMAGE_STREAM_TAG</b>	—	イメージストリーム内のイメージへの名前付きポインター。デフォルトは 7.8.0 です。	7.8.0	True

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

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

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_MEMORY_LIMIT</b>	—	KIE Server のコンテナのメモリー制限。	1Gi	False
<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server コンテナのデプロイメント設定。任意でエイリアスあり。 形式: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	rhdm-kieserver-library=org.openshift.quickstarts:rhdm-kieserver-library:1.6.0-SNAPSHOT	False
<b>KIE_SERVER_MGMT_DISABLED</b>	<b>KIE_SERVER_MGMT_DISABLED</b>	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.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
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL。	https://rh-sso.example.com/auth	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO レalm 名。	—	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	—	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット	252793ed-7118-4ca8-8dab-5622fa97d892	False

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

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

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

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

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

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

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

## 6.3.2. 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。

### 6.3.2.1. サービス

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

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

### 6.3.2.2. 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 (任意) で設定されます。詳細は、[Openshift ドキュメント](#) を参照してください。

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

### 6.3.2.3. 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、トリガーされたイベントに対応するために作成されます。詳細は、[Openshift ドキュメント](#) を参照してください。

#### 6.3.2.3.1. 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
<b>\${APPLICATION_NAME}-kieserver</b>	ImageChange

#### 6.3.2.3.2. レプリカ

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

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

### 6.3.2.3.3. Pod テンプレート

#### 6.3.2.3.3.1. 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>

#### 6.3.2.3.3.2. 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>

#### 6.3.2.3.3.3. Readiness Probe

`${APPLICATION_NAME}-kieserver`

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

#### 6.3.2.3.3.4. Liveness Probe

`${APPLICATION_NAME}-kieserver`

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

#### 6.3.2.3.3.5. 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

#### 6.3.2.3.3.6. 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>	必要かつ到達可能な場合にサービスルックアップ (maven リポジトリの使用など) を許可するのに使用される任意の Decision Central のサービス名。	<code>\${DECISION_CENTRAL_SERVICE}</code>

デプロイメント	変数名	説明	値の例
	<b>KIE_ADMIN_USER</b>	管理ユーザー名。	認証情報のシークレットに合わせて設定
	<b>KIE_ADMIN_PWD</b>	管理ユーザーのパスワード。	認証情報のシークレットに合わせて設定
	<b>KIE_SERVER_MODE</b>	KIE Server モード。有効な値は 'DEVELOPMENT' または 'PRODUCTION' です。実稼働モードでは、SNAPSHOT バージョンのアーティファクトは KIE Server にデプロイできず、既存のコンテナ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)	<b>\${KIE_SERVER_MODE}</b>
	<b>KIE_MBEANS</b>	KIE Server の mbeans が有効/無効になっています。(システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)	<b>\${KIE_MBEANS}</b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE Server クラスのフィルタリング。 (org.drools.server.filter.classes システムプロパティーを設定)	<b>\${DROOLS_SERVER_FILTER_CLASSES}</b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	false に設定すると、prometheus サーバー拡張が有効になります。 (org.kie.prometheus.server.ext.disabled システムプロパティーを設定)	<b>\${PROMETHEUS_SERVER_EXT_DISABLED}</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	KIE Server は、タスク関連の操作 (たとえばクエリー) については認証ユーザーをスキップできます。 (org.kie.server.bypass.auth.user システムプロパティーを設定)	<b>\${KIE_SERVER_BYPASS_AUTH_USER}</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_ID</b>	—	—
	<b>KIE_SERVER_ROUTE_NAME</b>	—	<b>\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server コンテナのデプロイメント設定。任意でエイリアスあり。形式: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	<b>\${KIE_SERVER_CONTAINER_DEPLOYMENT}</b>
	<b>MAVEN_MIRROR_URL</b>	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。	<b>\${MAVEN_MIRROR_URL}</b>
	<b>MAVEN_MIRROR_OFF</b>	KIE Server の Maven ミラー設定。	<b>\${MAVEN_MIRROR_OFF}</b>
	<b>MAVEN_REPOS</b>	—	RHDMCENTR,EXTERNAL
	<b>RHDMCENTR_MAVEN_REPO_ID</b>	—	repo-rhdmcentr
	<b>RHDMCENTR_MAVEN_REPO_SERVICE</b>	必要かつ到達可能な場合にサービススルックアップ(maven リポジトリの使用など)を許可するのに使用される任意の Decision Central のサービス名。	<b>\${DECISION_CENTRAL_SERVICE}</b>
	<b>RHDMCENTR_MAVEN_REPO_PATH</b>	—	<b>/maven2/</b>
	<b>RHDMCENTR_MAVEN_REPO_USERNAME</b>	—	認証情報のシークレットに合わせて設定

デプロイメント	変数名	説明	値の例
	<b>RHDMCENTR_MAVEN_REPO_PASSWORD</b>	—	認証情報のシークレットに合わせて設定
	<b>EXTERNAL_MAVEN_REPO_ID</b>	Maven リポジトリに使用する ID。これが設定されている場合は、MAVEN_MIRROR_OF に追加して、必要に応じて設定したミラーから除外できます。たとえば、external:*,!repo-rhdmcentr,!repo-custom などがあります。MAVEN_MIRROR_URL に設定されていても MAVEN_MIRROR_ID が設定されていない場合は、ID が無作為に生成され、MAVEN_MIRROR_OF では使用できません。	<b>\${MAVEN_REPO_ID}</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Maven リポジトリまたはサービスへの完全修飾 URL。	<b>\${MAVEN_REPO_URL}</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Maven リポジトリにアクセスするためのユーザー名 (必要な場合)。	<b>\${MAVEN_REPO_USERNAME}</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Maven リポジトリにアクセスするパスワード (必要な場合)。	<b>\${MAVEN_REPO_PASSWORD}</b>
	<b>KIE_SERVER_MGMT_DISABLED</b>	管理 api を無効にして、KIE コントローラーがデプロイ/デプロイ解除または起動/停止できないようにします。 org.kie.server.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。	<b>\${KIE_SERVER_MGMT_DISABLED}</b>

デプロイメント	変数名	説明	値の例
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	–	OpenShiftStartupStrategy
	<b>HTTPS_KEYSTORE_DIR</b>	–	/etc/kieserver-secret-volume
	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイルの名前。	<b>\${KIE_SERVER_HTTPS_KEYSTORE}</b>
	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	<b>\${KIE_SERVER_HTTPS_NAME}</b>
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード。	<b>\${KIE_SERVER_HTTPS_PASSWORD}</b>
	<b>JGROUPS_PING_PROTOCOL</b>	–	openshift.DNS_PING
	<b>OPENSIFT_DNS_PING_SERVICE_NAME</b>	–	<b>\${APPLICATION_NAME}-kieserver-ping</b>
	<b>OPENSIFT_DNS_PING_SERVICE_PORT</b>	–	8888
	<b>SSO_URL</b>	RH-SSO URL。	<b>\${SSO_URL}</b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	ROOT.war
	<b>SSO_REALM</b>	RH-SSO レalm名。	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	KIE Server の RH-SSO クライアントシークレット	<b>\${KIE_SERVER_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	KIE Server の RH-SSO クライアント名。	<b>\${KIE_SERVER_SSO_CLIENT}</b>
	<b>SSO_USERNAME</b>	クライアント作成に使用する RH-SSO レalmの管理者ユーザー名 (存在しない場合)。	<b>\${SSO_USERNAME}</b>
	<b>SSO_PASSWORD</b>	クライアント作成に使用する RH-SSO レalmの管理者のパスワード。	<b>\${SSO_PASSWORD}</b>

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

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

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

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

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

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

#### 6.3.2.3.3.7. ボリューム

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

#### 6.3.2.4. 外部の依存関係

##### 6.3.2.4.1. 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

## 6.4. OPENSIFT の使用に関するクイックリファレンス

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

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

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

- プロジェクトを作成するには、以下のコマンドを使用します。

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

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

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

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

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

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

```
$ oc get pods
```

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

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

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

- Pod のログを表示するには、以下のコマンドを使用します。

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

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

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

詳細は、[デプロイメントログの表示](#) を参照してください。

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

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

詳細は、[ビルドログのアクセス](#) を参照してください。

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

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

詳細は、[手動スケーリング](#) を参照してください。

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

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

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

## 付録A バージョン情報

本書の最終更新日: 2022 年 3 月 8 日 (火)