



# Red Hat Process Automation Manager 7.7

## Red Hat OpenShift Container Platform への Red Hat Process Automation Manager フリー フォーム管理サーバー環境のデプロイ

ガイド



# Red Hat Process Automation Manager 7.7 Red Hat OpenShift Container Platform への Red Hat Process Automation Manager フリーフォーム管理サーバー環境のデプロイ

---

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\_Process\_Automation\_Manager\_freeform\_managed\_server\_environment file |.

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

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

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

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

## 概要

本書は、Red Hat OpenShift Container Platform に Red Hat Process Automation Manager 7.7 フリーフォーム管理サーバー環境をデプロイする方法を説明します。

## 目次

前書き .....	4
第1章 RED HAT OPENSIFT CONTAINER PLATFORM における RED HAT PROCESS AUTOMATION MANAGER の概要 .....	5
第2章 OPENSIFT 環境に RED HAT PROCESS AUTOMATION MANAGER をデプロイする準備 .....	7
2.1. イメージストリームとイメージレジストリーの可用性確認 .....	7
2.2. KIE SERVER のシークレットの作成 .....	8
2.3. BUSINESS CENTRAL へのシークレットの作成 .....	9
2.4. 管理ユーザーのシークレットの作成 .....	9
2.5. 外部データベースのカスタム KIE SERVER 拡張イメージのビルド .....	10
2.6. NFS を使用した READWRITEMANY アクセスモードの永続ボリュームのプロビジョニング .....	12
2.7. オフラインで使用する MAVEN ミラーリポジトリの用意 .....	12
第3章 フリーフォーム管理サーバー環境 .....	14
3.1. フリーフォーム環境用の MONITORING および単一 KIE SERVER のデプロイ .....	14
3.1.1. Monitoring および単一の KIE Server 用のテンプレート設定の開始 .....	14
3.1.2. Monitoring および単一の KIE Server に必要なパラメーターの設定 .....	15
3.1.3. Monitoring および単一の KIE Server の Pod レプリカ数の設定 .....	16
3.1.4. 公開インターネットへの接続のない環境で Monitoring および単一の KIE Server の Maven ミラーへのアクセス設定 .....	17
3.1.5. Monitoring および単一の KIE Server の RH-SSO 認証用パラメーター設定 .....	18
3.1.6. Monitoring および単一の KIE Server の LDAP 認証用パラメーター設定 .....	19
3.1.7. Monitoring および単一の KIE Server の Prometheus メトリクス収集の有効化 .....	20
3.1.8. Monitoring および単一の KIE Server 用のテンプレートのデプロイ .....	21
3.2. フリーフォーム環境用の追加の管理 KIE SERVER のデプロイ .....	21
3.2.1. 追加の管理 KIE Server テンプレート設定の開始 .....	21
3.2.2. 追加の管理 KIE Server に必要なパラメーターの設定 .....	22
3.2.3. 追加の管理 KIE Server のイメージストリーム namespace の設定 .....	23
3.2.4. 追加の管理 KIE Server 用の Business Central Monitoring インスタンスについての情報の設定 .....	24
3.2.5. 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 .....	25
3.2.6. 追加の管理 KIE Server の RH-SSO 認証パラメーターの設定 .....	25
3.2.7. 追加の管理 KIE Server の LDAP 認証パラメーターの設定 .....	27
3.2.8. 追加の管理 KIE Server 用に外部データベースサーバーを使用するパラメーターの設定 .....	28
3.2.9. 追加の管理 KIE Server の Prometheus メトリクス収集の有効化 .....	29
3.2.10. 追加の管理 KIE Server テンプレートデプロイの実行 .....	30
3.3. (任意) LDAP ロールマッピングファイルの指定 .....	30
第4章 RED HAT PROCESS AUTOMATION MANAGER ロールおよびユーザー .....	32
第5章 OPENSIFT テンプレートの参考資料 .....	34
5.1. RHPAM77-MANAGED.YAML TEMPLATE .....	34
5.1.1. パラメーター .....	34
5.1.2. オブジェクト .....	50
5.1.2.1. サービス .....	50
5.1.2.2. ルート .....	51
5.1.2.3. デプロイメント設定 .....	51
5.1.2.3.1. トリガー .....	51
5.1.2.3.2. レプリカ .....	52
5.1.2.3.3. Pod テンプレート .....	52
5.1.2.4. 外部の依存関係 .....	73
5.1.2.4.1. ボリューム要求 .....	73

5.1.2.4.2. シークレット	73
5.2. OPENSIFT の使用に関するクイックリファレンス	73
付録A バージョン情報 .....	75



## 前書き

システムエンジニアは、Red Hat OpenShift Container Platform に Red Hat Process Automation Manager フリーフォーム管理サーバー環境をデプロイして、サービス、プロセスアプリケーション、およびその他のビジネスアセットを実行するためのインフラストラクチャーを提供できます。管理 KIE Server はいくつでもデプロイでき、この KIE Server は同じ Business Central Monitoring を使用して制御できます。必要に応じて KIE Server を追加および削除できます。Business Central Monitoring は、KIE Server への接続を自動的に確立します。同じ Business Central Monitoring インスタンスを使用して、イミュータブル KIE Server を監視することもできます。

### 前提条件

- Red Hat OpenShift Container Platform バージョン 3.11 がデプロイされている。
- OpenShift クラスター/namespace で 4 ギガバイト以上のメモリーが利用可能である。
- デプロイメントする 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 Container Platform 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、デプロイされるコンポーネントには以下の PV サイズが必要です。
  - Business Central Monitoring には、64Mi PV が必要です。
  - それぞれの KIE Server デプロイメントで、このデータベースに 1 つの 1Gi PV が必要になります。テンプレートパラメーターの PV サイズを変更できます。複数の KIE Server をデプロイする場合には、それぞれに別個のデータベース PV が必要です。この要件は、外部データベースサーバーを使用する場合には適用されません。
- お使いの OpenShift 環境で **ReadWriteMany** モードを使用した永続ボリュームをサポートしている。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。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 Process Automation Manager バージョン 7.5 以降、Red Hat OpenShift Container Platform 3.x のサポートは非推奨となっています。この機能は今後のリリースで削除されます。



### 注記

Red Hat Process Automation Manager テンプレートを Red Hat OpenShift Container Platform 4.x とともに使用しないでください。Red Hat Process Automation 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 Process Automation 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 PROCESS AUTOMATION MANAGER の概要

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

この場合に、Red Hat Process Automation 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 Process Automation 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)**とも呼ばれる) は、デシジョンサービス、プロセスアプリケーション、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。

通常、KIE Server にはデータベースサーバーが必要です。別の OpenShift Pod にデータベースサーバーを提供したり、別のデータベースサーバーを使用するように OpenShift で実行サーバーを設定したりできます。また、KIE Server では H2 データベースを使用できますが、使用する場合は、Pod をスケーリングできません。

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に必要な数だけ提供できます。Pod をスケールアップまたはスケールダウンすると、そのコピーはすべて同じデータベースサーバーを使用し、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。また、管理および監視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。また、Business Central を使用してプロセスの実行を監視することもできます。

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)。

- Business Central Monitoring は Web ベースの管理および監視コンソールです。KIE Server へのサービスのデプロイメントを管理し、監視情報を提供しますが、オーサリング機能は含まれません。このコンポーネントを使用して、ステージング環境および実稼働環境を管理できます。
- Smart Router は、KIE Server と、KIE Server と対話するその他のコンポーネントとの間の任意のレイヤーです。環境に、複数の KIE Server で実行するサービスが多数含まれる場合、Smart Router はすべてのクライアントアプリケーションに対応するエンドポイントを1つ提供します。クライアントアプリケーションは、サービスを要求する REST API 呼び出しを実行できます。Smart Router は、特定の要求を処理できる KIE Server を自動的に呼び出します。

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

以下の環境タイプが一般的です。

- オーサリング:** Business Central を使用してサービスを作成し、変更するために使用する環境です。これは、オーサリング作業用に Business Central を提供する Pod およびサービスのテスト実行用に KIE Server を提供する Pod で構成されます。この環境のデプロイメント手順については、『Red Hat [OpenShift Container Platform への Red Hat Process Automation Manager オーサリング環境のデプロイ](#)』を参照してください。
- 管理対象のデプロイメント:** ステージングおよび実稼働用として既存のサービスを実行するのに使用する環境。この環境には、KIE Server Pod のいくつかのグループが含まれます。このようなすべてのグループにサービスをデプロイおよびアンデプロイしたり、必要に応じてグループをスケールアップまたはスケールダウンしたりできます。Business Central Monitoring を使用してサービスをデプロイし、実行し、停止し、またそれらの実行を監視します。  
 2 種類の管理環境をデプロイできます。**自由形式** のサーバー環境では、最初に Business Central Monitoring と KIE Server を 1 つデプロイします。さらに、任意の数の KIE Server をデプロイできます。その後、追加として任意の数の KIE Server をデプロイできます。この環境のデプロイメント手順については、『[Red Hat OpenShift Container Platform への Red Hat Process Automation Manager フリーフォーム環境のデプロイ](#)』を参照してください。  
 または、**固定** の管理サーバー環境をデプロイすることもできます。単一デプロイメントには、Business Central Monitoring、Smart Router、および事前に設定された数の KIE Server (デフォルトでは 2 サーバーですが、テンプレートを変更して数を変更することができます) が含まれます。後のプロセスでは、サーバーを簡単に追加または削除することはできません。この環境のデプロイメント手順については、『Red Hat [OpenShift Container Platform への Red Hat Process Automation Manager 固定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。必要に応じて、Business Central Monitoring を使用して環境のパフォーマンスを監視したり、サービスインスタンスの一部を停止および再起動したりできますが、追加のサービスを KIE Server にデプロイしたり、既存のサービスのデプロイを解除したりすることはできません (コンテナの追加または削除はできません)。この環境のデプロイメント手順については、『Red Hat [OpenShift Container Platform への Red Hat Process Automation 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メント手順については、『Red Hat [OpenShift Container Platform への Red Hat Process Automation Manager 試用環境のデプロイ](#)』を参照してください。

OpenShift に Red Hat Process Automation Manager 環境をデプロイするには、Red Hat Process Automation Manager で提供されるテンプレートを使用できます。設定が環境に適したものになるようにテンプレートを変更できます。

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

OpenShift 環境に Red Hat Process Automation Manager をデプロイする前に、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、プロセスの新しいバージョン、または別のプロセス)をデプロイする場合は、このタスクを繰り返す必要はありません。

### 2.1. イメージストリームとイメージレジストリーの可用性確認

Red Hat Process Automation Manager コンポーネントを Red Hat OpenShift Container Platform にデプロイするには、OpenShift が Red Hat レジストリーから適切なイメージをダウンロードできることを確認する必要があります。これらのイメージをダウンロードするために、OpenShift ではイメージの場所情報が含まれる **イメージストリーム** が必要になります。また、OpenShift は、お使いのサービスアカウントのユーザー名とパスワードを使用して Red Hat レジストリー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 rhpam-businesscentral | grep -F 7.7  
$ oc get imagestreamtag -n openshift | grep -F rhpam-kieserver | grep -F 7.7
```

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 **rhcam-7.7.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードし、**rhcam 77-image-streams.yaml** ファイルを展開します。

g. 以下のコマンドを実行します。

```
$ oc apply -f rhcam77-image-streams.yaml
```



### 注記

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

## 2.2. 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、OpenShift ドキュメントの「[シークレット](#)」の章を参照してください。

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 Process Automation 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 Process Automation Manager 設定におけるこのデフォルトの値は **mykeystorepass** です。

5. **oc** コマンドを使用して、新しいキーストアファイルからシークレット **kieserver-app-secret** を生成します。

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

## 2.3. BUSINESS CENTRAL へのシークレットの作成

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

Business Central と 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 Process Automation 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 Process Automation Manager 設定におけるこのデフォルトの値は **mykeystorepass** です。
5. **oc** コマンドを使用して、新しいキーストアファイルからシークレット **businesscentral-app-secret** を生成します。

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

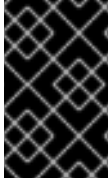
## 2.4. 管理ユーザーのシークレットの作成

Red Hat Process Automation 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、試用版テンプレート以外のテンプレートを使用して Red Hat Process Automation 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 Process Automation Manager のコンポーネントをデプロイする場合は、これら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 Monitoring 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、同じパスワードを持つ同じユーザーを Red Hat Process Automation Manager の **kie-server,rest-all,admin** ロールを使用して認証システムで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。

## 2.5. 外部データベースのカスタム KIE SERVER 拡張イメージのビルド

KIE Server に外部データベースサーバーを使用し、そのデータベースサーバーが MySQL または PostgreSQL 以外の場合は、環境をデプロイする前にこのサーバー用のドライバーを使用するカスタムの KIE Server 拡張イメージをビルドする必要があります。

このビルド手順の手順を完了して、次のデータベースサーバーのいずれかにドライバーを提供します。

- Microsoft SQL Server
- MariaDB
- IBM DB2
- Oracle データベース
- Sybase

データベースサーバーのサポートされるバージョンについては、「[Red Hat Process Automation Manager 7 でサポートされる構成](#)」を参照してください。

ビルド手順では、既存の KIE Server イメージを拡張するカスタム拡張イメージを作成します。このカスタム拡張イメージは OpenShift 環境にインポートしてから、**EXTENSIONS\_IMAGE** パラメーターで参照する必要があります。

## 前提条件

- **oc** コマンドを使用して OpenShift 環境にログインしている。OpenShift ユーザーには **registry-editor** ロールが必要です。
- Oracle Database または Sybase の場合は、データベースサーバーベンダーから JDBC ドライバーをダウンロードしている。
- 以下の必要なソフトウェアをインストールしている。
  - Docker
  - Cektit バージョン 3.2



- Cekit の以下のライブラリーおよび拡張機能:
  - **odcs-client**: **python3-odcs-client** パッケージまたは同様のパッケージで提供される。
  - **docker**: **python3-docker** パッケージまたは同様のパッケージで提供される。
  - **docker-squash**: **python3-docker-squash** または同様のパッケージで提供される。
  - **behave**: **python3-behave** パッケージまたは同様のパッケージで提供される。
  - **s2i**: **source-to-image** パッケージまたは同様のパッケージで提供される。

## 手順

1. IBM DB2、Oracle Database、または Sybase の場合、JDBC ドライバー JAR ファイルをローカルディレクトリーに指定します。
2. Red Hat カスタマーポータルの [Software Downloads](#) ページから利用可能な **rhpmam-7.7.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードします。
3. ファイルを展開し、コマンドラインで、展開したファイルの **templates/contrib/jdbc** ディレクトリーに変更します。このディレクトリーには、カスタムビルドのソースコードが含まれます。
4. データベースサーバーのタイプに応じて、以下のコマンドのいずれかを実行します。

- Microsoft SQL Server の場合:

```
make build mssql
```

- MariaDB の場合:

```
make build mariadb
```

- IBM DB2 の場合:

```
make build db2
```

- Oracle Database の場合:

```
make build oracle artifact=/tmp/ojdbc7.jar version=7.0
```

このコマンドで、**/tmp/ojdbc7.jar** をダウンロードされた Oracle Database ドライバーのパス名に置き換え、**7.0** をドライバーのバージョンに置き換えます。

- Sybase の場合:

```
make build sybase artifact=/tmp/jconn4-16.0_PL05.jar version=16.0_PL05
```

このコマンドで、**/tmp/jconn4-16.0\_PL05.jar** をダウンロードされた Sybase ドライバーのパス名に置き換え、**16.0\_PL05** をドライバーのバージョンに置き換えます。

5. 以下のコマンドを実行して、ローカルで利用可能な Docker イメージを一覧表示します。

```
docker images
```

ビルドされたイメージの名前 (例: **jboss-kie-db2-extension-openshift-image**) およびイメージのバージョンタグ (**11.1.4.4** など (**latest** タグではない)) をメモします。

6. OpenShift 環境のレジストリーに直接アクセスし、イメージをレジストリーにプッシュします。ユーザーパーミッションに応じて、イメージを **openshift** 名前空間またはプロジェクト名前空間にプッシュできます。レジストリーへのアクセスおよびイメージのプッシュの手順については、Red Hat OpenShift Container Platform 製品ドキュメントの「[Accessing the Registry Directly](#)」を参照してください。
7. 外部データベースサーバーをサポートするテンプレートを使用して KIE Server デプロイメントを設定する場合、以下のパラメーターを設定します。
  - **Drivers Extension Image (EXTENSIONS\_IMAGE)**: 拡張イメージの ImageStreamTag 定義 (例: **jboss-kie-db2-extension-openshift-image:11.1.4.4**)
  - **Drivers ImageStream Namespace (EXTENSIONS\_IMAGE\_NAMESPACE)**: 拡張イメージのアップロード先の名前空間 (例: **openshift** またはプロジェクト名前空間)

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

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

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、『[クラスターの設定](#)』ガイドの「[NFS を使用した永続ストレージ](#)」を参照してください。

## 2.7. オフラインで使用する MAVEN ミラーリポジトリの用意

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



### 注記

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

### 前提条件

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

### 手順

1. 書き込みアクセス権がある 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。

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

- a. Red Hat カスタマーポータル [Software Downloads](#) ページから利用可能な **rhpm-7.7.0-offliner.zip** の製品配信可能ファイルをダウンロードします。
- b. **rhpm-7.7.0-offliner.zip** ファイルの内容を任意のディレクトリーに展開します。
- c. ディレクトリーに移動し、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** サブディレクトリーを作成し、必要なアーティファクトをこのサブディレクトリー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 ユーティリティーを使用できます。
3. Business Central 外でサービスを開発し、追加の依存関係がある場合は、ミラーリポジトリにその依存関係を追加します。サービスを Maven プロジェクトとして開発した場合は、以下の手順を使用し、これらの依存関係を自動的に用意します。公開インターネットへに送信接続できるコンピューターで、この手順を実行します。
- a. ローカルの Maven キャッシュディレクトリー (`~/.m2/repository`) のバックアップを作成して、ディレクトリーを削除します。
  - b. **mvn clean install** コマンドを使用してプロジェクトのソースをビルドします。
  - c. すべてのプロジェクトで以下のコマンドを入力し、Maven を使用してプロジェクトで生成したすべてのアーティファクトのランタイムの依存関係をすべてダウンロードするようにします。

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

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

- d. ローカルの Maven キャッシュディレクトリー (`~/.m2/repository`) から作成した Maven ミラーリポジトリ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 ユーティリティーを使用できます。

## 第3章 フリーフォーム管理サーバー環境

KIE Server を実行する複数の異なる Pod で構成されるフリーフォームサーバー環境をデプロイできます。これらの KIE Server は、ステージングまたは実稼働環境を目的として、さまざまなサービスを実行できます。必要に応じて、サーバーをいつでも追加および削除できます。

Business Central Monitoring と管理 KIE Server 1 台をデプロイし、フリーフォーム管理サーバー環境のデプロイを開始します。Business Central Monitoring を使用して KIE Server 上のサービスの実行を監視し、必要に応じて管理できます。この環境には Smart Router は含まれていません。

追加の管理 KIE Server をデプロイすることもできます。各 KIE Server は、必要に応じて個別にスケーリングできます。

管理 KIE Server では、最初からサービスが読み込まれる訳ではありません。Business Central Monitoring または KIE Server の REST API を使用して、サーバーでプロセスをデプロイおよびデプロイ解除してください。

サーバーにデプロイするプロセス (KJAR ファイル) がある Maven リポジトリを提供する必要があります。統合プロセスは、必要なバージョンのプロセスが Maven リポジトリにアップロードされるようにする必要があります。開発環境で Business Central を使用してプロセスを作成し、Maven リポジトリにアップロードできます。

各 KIE Server はデータベースサーバーを使用します。通常、データベースサーバーも Pod で実行されますが、外部データベースサーバーを使用するように KIE Server を設定できます。

同じ名前空間にイミュータブル KIE Server をデプロイすることもできます。Business Central Monitoring を使用して、イミュータブルサーバーなど、その環境のすべての KIE Server に関するモニタリング情報を確認できます。イミュータブル KIE Server のデプロイ手順については、『[Deploying a Red Hat Process Automation Manager immutable server environment on Red Hat OpenShift Container Platform](#)』を参照してください。

### 3.1. フリーフォーム環境用の MONITORING および単一 KIE SERVER のデプロイ

フリーフォーム環境のデプロイを開始するには、Business Central Monitoring と、Pod で PostgreSQL データベースサーバーを使用する管理 KIE Server を 1 台デプロイします。サービスは、KIE Server には読み込まれません。Business Central Monitoring を使用して、サーバーでサービスをデプロイおよびデプロイ解除します。

その後、必要に応じて KIE Server を追加できます。

#### 3.1.1. Monitoring および単一の KIE Server 用のテンプレート設定の開始

Business Central Monitoring と管理 KIE Server 1 台をデプロイするには、**rhpm77-managed.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](#) ページから利用可能な **rhpm77-managed-7.7.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードします。
2. **rhpm77-managed.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、**rhcam77-managed.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>/rhcam77-managed.yaml -p
BUSINESS_CENTRAL_HTTPS_SECRET=businesscentral-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。
- 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。「[Monitoring および単一の KIE Server に必要なパラメーターの設定](#)」の手順を実行し、共通のパラメーターを設定します。テンプレートファイルを表示して、すべてのパラメーターの説明を確認します。

### 3.1.2. Monitoring および単一の KIE Server に必要なパラメーターの設定

Business Central Monitoring と管理 KIE Server 1 台をデプロイするようにテンプレートを設定するには、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

- 「[Monitoring および単一の KIE Server 用のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始していること。

#### 手順

1. 以下のパラメーターを設定します。
  - **認証情報シークレット (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 Monitoring Server Keystore Secret Name (BUSINESS\_CENTRAL\_HTTPS\_SECRET)**: 「[Business Central へのシークレットの作成](#)」で作成した Business Central のシークレットの名前。
  - **KIE Server キーストアのシークレット名 (KIE\_SERVER\_HTTPS\_SECRET)**: 「[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 Monitoring Server Certificate Name (BUSINESS\_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 Monitoring Server Keystore Password (BUSINESS\_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。
- **Enable KIE server global discovery (KIE\_SERVER\_CONTROLLER\_OPENSHIFT\_GLOBAL\_DISCOVERY\_ENABLED):** 同じ名前空間にある **OpenShiftStartupStrategy** が指定されたすべての KIE Server を Business Central Monitoring に検出させるには、このパラメーターを **true** に設定します。デフォルトでは、Business Central Monitoring は、**APPLICATION\_NAME** パラメーターが Business Central Monitoring と同じ値でデプロイされた KIE Server のみを検出します。
- **Maven リポジトリ URL(MAVEN\_REPO\_URL):** Maven リポジトリの URL。お使いの環境の KIE Server にデプロイするすべてのプロセス (KJAR ファイル) をこのリポジトリにアップロードする必要があります。
- **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。
- **KIE Server Mode(KIE\_SERVER\_MODE):** **rhpam77-managed.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、名前空間が **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、「[Monitoring および単一の KIE Server 用のテンプレートのデプロイ](#)」の手順に従います。

### 3.1.3. Monitoring および単一の KIE Server の Pod レプリカ数の設定

Business Central Monitoring および単一の管理 KIE Server をデプロイするテンプレートを設定する場合は、KIE Server および Business Central Monitoring のレプリカの初期数を設定します。

## 前提条件

- 「[Monitoring および単一の KIE Server 用のテンプレート設定の開始](#)」 に説明されているようにテンプレートの設定を開始していること。

## 手順

レプリカの数を設定するには、次のパラメーターを設定します。

- **Business Central Monitoring Container Replicas** (**BUSINESS\_CENTRAL\_MONITORING\_CONTAINER\_REPLICAS**): デプロイメント時に最初に Business Central Monitoring 用に最初に作成されるレプリカ数。Business Central Monitoring に高可用性設定を使用しない場合は、この数値を 1 に設定します。
- **KIE Server Container Replicas**(**KIE\_SERVER\_CONTAINER\_REPLICAS**): デプロイメントが KIE Server 用に最初に作成するレプリカの数。

## 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、「[Monitoring および単一の KIE Server 用のテンプレートのデプロイ](#)」の手順に従います。

### 3.1.4. 公開インターネットへの接続のない環境で Monitoring および単一の KIE Server の Maven ミラーへのアクセス設定

Business Central Monitoring および単一の管理 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、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

- 「[Monitoring および単一の KIE Server 用のテンプレート設定の開始](#)」 に説明されているようにテンプレートの設定を開始していること。

## 手順

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

- **Maven mirror URL** (**MAVEN\_MIRROR\_URL**): 「[オフラインで使用する Maven ミラーリポジトリの用意](#)」 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 (**BUSINESS\_CENTRAL\_MAVEN\_SERVICE**) を設定する場合には、ミラーからこのリポジトリ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-rhpamcentr)`。

- 両方のリポジトリを設定している場合は、ミラーからこのリポジトリを両方除外するように **MAVEN\_MIRROR\_OF** を変更します (例: `external:*,!repo-rhpamcentr,!repo-custom`)。 **repo-custom** は、 **MAVEN\_REPO\_ID** で設定した ID に置き換えます。

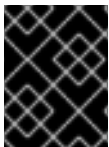
## 次のステップ

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、「[Monitoring および単一の KIE Server 用のテンプレートのデプロイ](#)」の手順に従います。

### 3.1.5. Monitoring および単一の KIE Server の RH-SSO 認証用パラメーター設定

RH-SSO 認証を使用する場合は、Business Central Monitoring および単一の管理 KIE Server をデプロイするようにテンプレートを設定するには次の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 Process Automation Manager のレルムが RH-SSO 認証システムに作成されている。
- Red Hat Process Automation Manager のユーザー名およびパスワードが RH-SSO 認証システムに作成されている。利用可能なロールの一覧については、[4章 Red Hat Process Automation 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。
- クライアントが、デプロイしている Red Hat Process Automation Manager 環境のすべてのコンポーネントについて RH-SSO 認証システムに作成されている。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 Process Automation Manager デプロイメントはクライアントを作成できます。ただし、このオプションの環境に対する制御の詳細度合はより低くなります。
- 「[Monitoring および単一の KIE Server 用のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始していること。

#### 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 Realm name (SSO\_REALM)**: Red Hat Process Automation 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 Process Automation 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 Monitoring RH-SSO Client name**  
(**BUSINESS\_CENTRAL\_SSO\_CLIENT**): Business Central Monitoring の RH-SSO クライアント名。
  - **Business Central Monitoring RH-SSO Client Secret**  
(**BUSINESS\_CENTRAL\_SSO\_SECRET**): Business Central Monitoring のクライアント向けに RH-SSO に設定されてい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。
- b. RH-SSO で Red Hat Process Automation Manager のクライアントを作成するには、テンプレートで以下のパラメーターを設定します。
  - **Business Central Monitoring RH-SSO Client name**  
(**BUSINESS\_CENTRAL\_SSO\_CLIENT**): Business Central Monitoring の RH-SSO で作成するクライアントの名前。
  - **Business Central Monitoring RH-SSO Client Secret**  
(**BUSINESS\_CENTRAL\_SSO\_SECRET**): Business Central Monitoring のクライアント向けに RH-SSO に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 Realm Admin Username**(**SSO\_USERNAME**) および **RH-SSO Realm Admin Password** (**SSO\_PASSWORD**): Red Hat Process Automation Manager の RH-SSO レalmのレalm管理者ユーザーのユーザー名およびパスワード。必要なクライアントを作成するためにこのユーザー名およびパスワードを指定する必要があります。

## 次のステップ

必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[Monitoring および単一の KIE Server 用のテンプレートのデプロイ](#)」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 Process Automation Manager のコンポーネントの URL が正しいことを確認してください。

### 3.1.6. Monitoring および単一の KIE Server の LDAP 認証用パラメーター設定

LDAP 認証を使用する場合は、Business Central Monitoring および単一の管理 KIE Server をデプロイするようにテンプレートを設定するには、次の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 Process Automation Manager のユーザー名およびパスワードを作成していること。利用可能なロールの一覧については、[4章 Red Hat Process Automation 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。
- 「[Monitoring および単一の KIE Server 用のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始していること。

### 手順

- 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 サーバーでデプロイメントに必要なすべてのロールが定義されていない場合は、Red Hat Process Automation Manager ロールに LDAP グループをマップできます。LDAP のロールマッピングを有効にするには、以下のパラメーターを設定します。
  - RoleMapping rolesProperties 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、「[Monitoring および単一の KIE Server 用のテンプレートのデプロイ](#)」の手順に従います。

## 3.1.7. Monitoring および単一の KIE Server の Prometheus メトリクス収集の有効化

Prometheus を使用してメトリクスを収集し、保存するように KIE Server デプロイメントを設定する必要がある場合は、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

- 「[Monitoring および単一の KIE Server 用のテンプレート設定の開始](#)」に説明されているようにテンプレートの設定を開始していること。



## 手順

Prometheus メトリクス収集のサポートを有効にするには、**Prometheus Server 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、「[Monitoring および単一の KIE Server 用のテンプレートのデプロイ](#)」の手順に従います。

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

### 3.1.8. Monitoring および単一の KIE Server 用のテンプレートのデプロイ

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

## 手順

使用している方法に応じて、以下の手順を実行します。

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

## 3.2. フリーフォーム環境用の追加の管理 KIE SERVER のデプロイ

管理 KIE Server は、フリーフォーム環境に追加できます。このサーバーは、Pod で PostgreSQL または MySQL データベースサーバーを使用するか、または外部データベースサーバーを使用できます。

Business Central Monitoring デプロイメントと同じプロジェクトにサーバーをデプロイします。

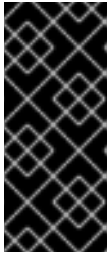
KIE Server は、Maven リポジトリからサービスを読み込みます。

サーバーは、サービスが読み込まれていない状態で起動します。サーバーへのサービスのデプロイおよびデプロイの解除は、Business Central Monitoring または KIE Server の REST API を使用します。

### 3.2.1. 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、以下のテンプレートファイルのいずれかを使用します。

- **rhcam77-kieserver-postgresql.yaml**: 永続ストレージに PostgreSQL Pod を使用します。他のテンプレートを使用する特別な理由がない限り、このテンプレートを使用します。
- **rhcam77-kieserver-mysql.yaml**: 永続ストレージに MySQL Pod を使用します。
- **rhcam77-kieserver-externaldb.yaml**: 永続ストレージに外部データベースサーバーを使用します。



## 重要

外部データベースサーバーの標準 KIE Server イメージには、MySQL および PostgreSQL 外部データベースサーバー用のドライバーが含まれます。別のデータベースサーバーを使用する場合は、カスタムの KIE Server イメージをビルドする必要があります。手順は、「[外部データベースのカスタム KIE Server 拡張イメージのビルド](#)」を参照してください。

## 手順

1. Red Hat カスタマーポータル [の Software Downloads](#) ページから利用可能な **rhpmam-7.7.0-openshift-templates.zip** の製品配信可能ファイルをダウンロードします。
2. 必要なテンプレートファイルを展開します。
3. 以下のいずれかの方法を使用してテンプレートのデプロイを開始します。
  - OpenShift Web UI を使用するには、OpenShift アプリケーションコンソールで **Add to Project → Import YAML / JSON** を選択してから **<template-file-name>.yaml** ファイルを選択するか、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
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。「[追加の管理 KIE Server に必要なパラメーターの設定](#)」の手順を実行し、共通のパラメーターを設定します。テンプレートファイルを表示して、すべてのパラメーターの説明を確認します。

### 3.2.2. 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こと。

## 手順

1. 以下のパラメーターを設定します。

- **認証情報シークレット (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 キーストアのシークレット名 (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別個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 Monitoring 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。
- **Maven repository URL (MAVEN\_REPO\_URL):** Maven リポジトリの URL。KIE Server にデプロイするすべてのプロセス (KJAR ファイル) をこのリポジトリにアップロードする必要があります。
- **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。
- **KIE Server Mode (KIE\_SERVER\_MODE):** `rhcam77-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、名前空間が **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。

### 3.2.3. 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 namespace でイメージストリームを作成した場合、テンプレートで namespace を設定する必要があります。

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

#### 前提条件

- 「[追加の管理 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こと。

#### 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 名前空間 (IMAGE\_STREAM\_NAMESPACE)** パラメーターを OpenShift プロジェクトの名前に設定します。

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

デプロイした Business Central Monitoring インスタンスから KIE Server への接続を有効にするには、Business Central Monitoring インスタンスの情報を設定する必要があります。

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

#### 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こと。

#### 手順

1. 以下のパラメーターを設定します。
  - **Name of the Business Central service (BUSINESS\_CENTRAL\_SERVICE)**: Business Central Monitoring の OpenShift サービス名。
2. 以下の設定が Business Central Monitoring の同じ設定と値に設定されていることを確認します。
  - **Maven リポジトリの URL (MAVEN\_REPO\_URL)**: サービスのデプロイに使用する必要のある外部 Maven リポジトリの URL。
  - **Maven リポジトリのユーザー名 (MAVEN\_REPO\_USERNAME)**: Maven リポジトリのユーザー名。
  - **Maven リポジトリのパスワード (MAVEN\_REPO\_PASSWORD)**: Maven リポジトリのパスワード。

#### 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。

### 3.2.5. 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こと。

#### 手順

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

- **Maven mirror URL (MAVEN\_MIRROR\_URL):** 「[オフラインで使用する Maven ミラーリポジトリの用意](#)」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 (**BUSINESS\_CENTRAL\_MAVEN\_SERVICE**) を設定する場合には、ミラーからこのリポジトリ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-rhpamcentr**)。
  - 両方のリポジトリを設定している場合は、ミラーからこのリポジトリを両方除外するように **MAVEN\_MIRROR\_OF** を変更します (例: **external:\*;!repo-rhpamcentr;!repo-custom**)。repo-custom は、**MAVEN\_REPO\_ID** で設定した ID に置き換えます。

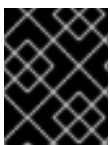
#### 次のステップ

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。

### 3.2.6. 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 Process Automation Manager のレルムが RH-SSO 認証システムに作成されている。
- Red Hat Process Automation Manager のユーザー名およびパスワードが RH-SSO 認証システムに作成されている。利用可能なロールの一覧については、[4章 Red Hat Process Automation 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。
- クライアントが、デプロイしている Red Hat Process Automation Manager 環境のすべてのコンポーネントについて RH-SSO 認証システムに作成されている。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 Process Automation Manager デプロイメントはクライアントを作成できます。ただし、このオプションの環境に対する制御の詳細度はより低くなります。
- 「[追加の管理 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こと。

## 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 Realm name (SSO\_REALM):** Red Hat Process Automation 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。
- 以下の手順のいずれかを実行します。
  - RH-SSO で Red Hat Process Automation 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 Monitoring RH-SSO Client name (BUSINESS\_CENTRAL\_SSO\_CLIENT):** Business Central Monitoring 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。
  - RH-SSO で Red Hat Process Automation Manager のクライアントを作成するには、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 Realm Admin Username (SSO\_USERNAME) および RH-SSO Realm Admin**



**Password (SSO\_PASSWORD):** Red Hat Process Automation Manager の RH-SSO レルムのレルム管理者ユーザーのユーザー名およびパスワード。必要なクライアントを作成するためにこのユーザー名およびパスワードを指定する必要があります。

## 次のステップ

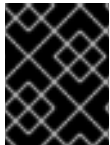
必要な場合は、追加のパラメーターを設定します。

デプロイを完了するには、「[追加の管理 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 Process Automation Manager のコンポーネントの URL が正しいことを確認してください。

### 3.2.7. 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 Process Automation Manager のユーザー名およびパスワードを作成していること。利用可能なロールの一覧については、[4章 Red Hat Process Automation 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こと。

## 手順

- 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 サーバーでデプロイメントに必要なすべてのロールが定義されていない場合は、Red Hat Process Automation Manager ロールに LDAP グループをマップできます。LDAP のロールマッピングを有効にするには、以下のパラメーターを設定します。
  - RoleMapping rolesProperties 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。

### 3.2.8. 追加の管理 KIE Server 用に外部データベースサーバーを使用するパラメーターの設定

**rhpm77-kieserver-externaldb.yaml** テンプレートを使用して KIE Server 用に外部データベースサーバーを使用する場合は、追加の管理 KIE Server をデプロイするようにテンプレートを設定する時に次の追加の設定を実行します。

#### 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こと。

#### 手順

- 以下のパラメーターを設定します。

- KIE Server External Database Driver(**KIE\_SERVER\_EXTERNALDB\_DRIVER**): サーバーの種類に応じたサーバーのドライバ。
  - mysql**
  - postgresql**
  - mariadb**
  - mssql**
  - db2**
  - oracle**
  - sybase**
- KIE Server External Database User(**KIE\_SERVER\_EXTERNALDB\_USER**) および KIE Server External Database Password (**KIE\_SERVER\_EXTERNALDB\_PWD**): 外部データベースサーバーのユーザー名およびパスワード。
- KIE Server External Database URL(**KIE\_SERVER\_EXTERNALDB\_URL**): 外部データベースサーバーの JDBC URL。
- KIE Server External Database Host(**KIE\_SERVER\_EXTERNALDB\_SERVICE\_HOST**) および KIE Server External Database Port (**KIE\_SERVER\_EXTERNALDB\_SERVICE\_PORT**): 外部データベースサーバーのホスト名およびポート番号。これらのパラメーターを、**KIE\_SERVER\_EXTERNALDB\_URL** パラメーターを設定する代わりに設定できます。



- KIE Server External Database Dialect(**KIE\_SERVER\_EXTERNALDB\_DIALECT**): サーバーの種類に応じたサーバーの Hibernate ダイアレクト。
    - **org.hibernate.dialect.MySQL5InnoDBDialect** (MySQL および MariaDB で使用される)
    - **org.hibernate.dialect.PostgreSQL82Dialect**
    - **org.hibernate.dialect.SQLServer2012Dialect** (MS SQL で使用される)
    - **org.hibernate.dialect.DB2Dialect**
    - **org.hibernate.dialect.Oracle10gDialect**
    - **org.hibernate.dialect.SybaseASE157Dialect**
  - KIE Server External Database name(**KIE\_SERVER\_EXTERNALDB\_DB**): 外部データベースサーバーで使用するデータベース名。
  - JDBC Connection Checker class (**KIE\_SERVER\_EXTERNALDB\_CONNECTION\_CHECKER**): データベースサーバーの JDBC connection checker class の名前。この情報がないと、データベースサーバー接続は、データベースサーバーの再起動時などで接続が失われた後に復元することができません。
  - JDBC Exception Sorter class (**KIE\_SERVER\_EXTERNALDB\_EXCEPTION\_SORTER**): データベースサーバーの JDBC exception sorter class の名前。この情報がないと、データベースサーバー接続は、データベースサーバーの再起動時などで接続が失われた後に復元することができません。
2. 「外部データベースのカスタム KIE Server 拡張イメージのビルド」で説明されているように、MySQL または PostgreSQL 以外の外部データベースサーバーを使用するためにカスタムイメージを作成している場合は、以下のパラメーターを設定します。
- Drivers Extension Image (**EXTENSIONS\_IMAGE**): 拡張イメージの ImageStreamTag 定義 (例: **jboss-kie-db2-extension-openshift-image:11.1.4.4**)
  - Drivers ImageStream Namespace (**EXTENSIONS\_IMAGE\_NAMESPACE**): 拡張イメージのアップロード先の名前空間 (例: **openshift** またはプロジェクト名前空間)

## 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。

### 3.2.9. 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こと。

## 手順

Prometheus メトリクス収集のサポートを有効にするには、**Prometheus Server 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 メトリクス収集の方法については、「[KIE Server の管理および監視](#)」を参照してください。

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

## 手順

使用している方法に応じて、以下の手順を実行します。

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

## 3.3. (任意) LDAP ロールマッピングファイルの指定

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

## 手順

1. **my-role-map** など、ロールマッピングのプロパティファイルを作成します。ファイルには、次の形式のエントリ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。たとえば、以下ようになります。

```
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** 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。

## 第4章 RED HAT PROCESS AUTOMATION 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。

このセクションでは、利用可能な Red Hat Process Automation Manager ユーザーロールについて説明します。



### 注記

**admin**、**analyst**、**developer**、**manager**、**process-admin**、**user**、および **rest-all** のロールは Business Central 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 Process Automation 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。これらは、プロジェクトのモデリングと実行を行うことができます。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。
- **developer:** **developer** ロールを持つユーザーは、ほぼすべての機能にアクセスができ、ルール、モデル、プロセスフロー、フォーム、およびダッシュボードを管理できます。アセットリポジトリを管理し、プロジェクトを作成、ビルド、およびデプロイでき、Red Hat CodeReady Studio を使用してプロセスを表示できます。**developer** ロールが割り当てられているユーザーには、新規リポジトリの作成やクローン作成などの、特定の管理機能は表示されません。
- **manager:** **manager** ロールを持つユーザーはレポートを表示できます。このユーザーは通常、ビジネスプロセス、そのパフォーマンス、ビジネスインジケター、その他のビジネス関連のレポートに関する統計に関心があります。このルールを持つユーザーがアクセスできるのはプロセスおよびタスクのレポートに限られます。

- **process-admin: process-admin** ロールを持つユーザーは、ビジネスプロセス管理者です。ビジネスプロセス、ビジネスタスク、および実行エラーへの完全アクセスがあります。このユーザーは、ビジネスレポートを表示でき、タスク受信箱リストにアクセスできます。
- **user: user** ロールを持つユーザーは、タスクの受信箱リストで有効です。これには、現在実行しているプロセスの一部であるビジネスタスクも含まれます。このルールを持つユーザーはプロセスとタスクのレポートを確認して、プロセスを管理できます。
- **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。このロールは、Business Central で **Manage** ビューおよび **Track** ビューにアクセスするユーザーにとって必須となります。

## 第5章 OPENSIFT テンプレートの参考資料

Red Hat Process Automation Manager は以下の OpenShift テンプレートを提供します。テンプレートにアクセスするには、Red Hat カスタマーポータル[の Software Downloads ページ](#)から、`rhcam -7.7.0-openshift-templates.zip` の製品配信可能ファイルをダウンロードし、これを展開します。

- **rhcam77-managed.yaml** は、高可用性 Business Central Monitoring インスタンス、KIE Server、KIE Server が使用する PostgreSQL インスタンスを提供します。**OpenShiftStartupStrategy** が有効になっているため、これらのインスタンスでも OpenShiftStartupStrategy が有効になっている限り、Business Central Monitoring インスタンスは同じプロジェクト内の他の KIE Server インスタンスに自動的に接続できます。

この環境で使用される他のテンプレートについての参考情報は、『Red Hat [OpenShift Container Platform への Red Hat Process Automation Manager イミュータブルサーバー環境のデプロイメント](#)』の参照セクションを参照してください。

### 5.1. RHPAM77-MANAGED.YAML TEMPLATE

Red Hat Process Automation Manager 7.7 向けの、管理 HA 実稼働ランタイム環境のアプリケーションテンプレート (非推奨)

#### 5.1.1. パラメーター

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

変数名	イメージの環境変数	説明	値の例	必須
<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

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-rhpamcentr,!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/	True
<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

変数名	イメージの環境変数	説明	値の例	必須
<b>BUSINESS_CENTRAL_SERVICE</b>	<b>RHPAMCENTRAL_MAVEN_REPO_SERVICE</b>	maven リポジトリの使用状況など、サービスのルックアップができるように任意の Business Central に到達可能な場合に使用するサービス名 (必要な場合)	myapp-rhpamcentrmon	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。	rhpam-credentials	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)	5000	False
<b>IMAGE_STREAM_NAMESPACE</b>	—	Red Hat Process Automation 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 を異なる名前空間/プロジェクトにインストールしている場合にのみこれを変更する必要があります。デフォルトは「openshift」です。	openshift	True
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	—	KIE Server に使用するイメージストリームの名前。デフォルトは「rhpam-kieserver-rhel8」です。	rhpam-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「7.7.0」です。	7.7.0	True

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_CONTROLLER_TOKEN</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)	—	False
<b>KIE_SERVER_PERSISTENCE_DS</b>	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE Server 永続データソース。 (org.kie.server.persistence.ds システムプロパティを設定)	java:/jboss/datasources/rhpam	False
<b>POSTGRESQL_IMAGE_STREAM_NAMESPACE</b>	—	PostgreSQL イメージの ImageStream がインストールされている名前空間。ImageStream は openshift namespace にすでにインストールされています。ImageStream を異なる名前空間/プロジェクトにインストールしている場合にのみこれを変更する必要があります。デフォルトは「openshift」です。	openshift	False
<b>POSTGRESQL_IMAGE_STREAM_TAG</b>	—	PostgreSQL イメージのバージョン。これは PostgreSQL バージョンに対応するように意図されています。デフォルトは「10」です。	10	False
<b>KIE_SERVER_POSTGRESQL_USER</b>	<b>RHPAM_USERNAME</b>	KIE Server PostgreSQL データベースのユーザー名。	rhpam	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_POSTGRESQL_PASSWORD</b>	<b>RHPAM_PASSWORD</b>	KIE Server PostgreSQL データベースのパスワード。	—	False
<b>KIE_SERVER_POSTGRESQL_DATABASE</b>	<b>RHPAM_DATABASE</b>	KIE Server PostgreSQL データベース名。	rhpm7	False
<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	PostgreSQL による XA トランザクションの処理を許可します。	100	True
<b>DB_VOLUME_CAPACITY</b>	—	データベースボリュームの永続ストレージのサイズ。	1Gi	True
<b>KIE_SERVER_POSTGRESQL_DIALECT</b>	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE Server PostgreSQL Hibernate 方言。	org.hibernate.dialect.PostgreSQLDialect	True
<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

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE Server の mbeans の有効化/無効化 (システムプロパティー kie.mbeans および kie.scanner.mbeans を設定)。	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE Server 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)	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ーを設定)	false	False
<b>BUSINESS_CENTRAL_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	http サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合は空白にします (例: insecure- <application-name>- rhpamcentrmon- <project>.<default-domain-suffix>)。	—	False
<b>BUSINESS_CENTRAL_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合は空白にします (例: <application-name>- rhpamcentrmon- <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_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>BUSINESS_CENTRAL_HTTPS_SECRET</b>	—	Business 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。	businesscentral-app-secret	True
<b>BUSINESS_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名	keystore.jks	False
<b>BUSINESS_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>BUSINESS_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>	—	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>	シークレット内のキーストアファイル名	keystore.jks	False

変数名	イメージの環境変数	説明	値の例	必須
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	サーバー証明書に関連付けられている名前	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	mykeystorepass	False
<b>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>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	EJB タイマーサービスのデータベースデータストアの更新間隔を設定します。	30000	False
<b>BUSINESS_CENTRAL_MEMORY_LIMIT</b>	–	Business Central Monitoring 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>BUSINESS_CENTRAL_MONITORING_CONTAINER_REPLICAS</b>	–	Business Central Monitoring Container Replicas は、起動する Business Central Monitoring コンテナ数を定義します。	3	True
<b>KIE_SERVER_CONTAINER_REPLICAS</b>	–	KIE Server Container Replicas は、起動する KIE Server コンテナ数を定義します。	3	True

変数名	イメージの環境変数	説明	値の例	必須
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL。	https://rh-sso.example.com/auth	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO レルム名。	—	False
<b>BUSINESS_CENTRAL_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	Business Central Monitoring RH-SSO クライアント名。	—	False
<b>BUSINESS_CENTRAL_SSO_SECRET</b>	<b>SSO_SECRET</b>	Business Central Monitoring 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
<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

変数名	イメージの環境変数	説明	値の例	必須
<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
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	ユーザーまたはロールの検索のタイムアウト (ミリ秒単位)。	10000	False



変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	ユーザーの DN を含むユーザーエントリーの属性の名前。これは、ユーザー自体の DN に特殊文字 (たとえば、正しいユーザーマッピングを防ぐバックスラッシュ) が含まれてい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
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	—	False

変数名	イメージの環境変数	説明	値の例	必須
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	ユーザー名を公開するため、DN の最後から削除される文字列を定義します。このオプションは 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、実際のロールがである DN ではなく、ユーザーロールを含むオブジェクトがある 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

## 5.1.2. オブジェクト

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

### 5.1.2.1. サービス

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

サービス	ポート	名前	説明
<b>\${APPLICATION_NAME}-rhpamcentrmon</b>	8080	http	すべての Business Central Monitoring 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}-rhpmcentrmon-ping</b>	8888	ping	クラスタリング向けの JGroups ping ポート。
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	すべての KIE Server Web サーバーのポート。(1つ目の KIE server)
	8443	https	
<b>\${APPLICATION_NAME}-kieserver-ping</b>	8888	ping	クラスタリング向けの JGroups ping ポート。
<b>\${APPLICATION_NAME}-postgresql</b>	5432	—	最初のデータベースサーバーのポート。

### 5.1.2.2. ルート

ルートとは、**www.example.com** など、外部から到達可能なホスト名を指定して、サービスを公開する手段です。ルーターは、定義したルートや、サービスで特定したエンドポイントを使用して、外部のクライアントからアプリケーションに名前付きの接続を提供します。各ルートは、ルート名、サービスセレクター、セキュリティ設定 (任意) で構成されます。詳細情報は、[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}-rhpmcentrmon-http</b>	なし	<b>\${BUSINESS_CENTRAL_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-rhpmcentrmon-https</b>	TLS パススルー	<b>\${BUSINESS_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>

### 5.1.2.3. デプロイメント設定

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

#### 5.1.2.3.1. トリガー

トリガーは、OpenShift 内外を問わず、イベントが発生すると新規デプロイメントを作成するように促します。詳細情報は、[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}-rhpamcentrmon</code>	ImageChange
<code>\${APPLICATION_NAME}-kieserver</code>	ImageChange
<code>\${APPLICATION_NAME}-postgresql</code>	ImageChange

#### 5.1.2.3.2. レプリカ

レプリケーションコントローラーを使用すると、指定した数だけ、Pod の「レプリカ」を一度に実行させることができます。レプリカが増えると、レプリケーションコントローラーが Pod の一部を終了させます。レプリカが足りない場合には、起動させます。詳細は、[コンテナ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}-rhpamcentrmon</code>	3
<code>\${APPLICATION_NAME}-kieserver</code>	3
<code>\${APPLICATION_NAME}-postgresql</code>	1

#### 5.1.2.3.3. Pod テンプレート

##### 5.1.2.3.3.1. サービスアカウント

サービスアカウントは、各プロジェクト内に存在する API オブジェクトです。他の API オブジェクトのように作成し、削除できます。詳細情報は、[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}-rhpamcentrmon</code>	<code>\${APPLICATION_NAME}-rhpamsvc</code>
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-rhpamsvc</code>

##### 5.1.2.3.3.2. イメージ

デプロイメント	イメージ
<code>\${APPLICATION_NAME}-rhpamcentrmon</code>	<code>rhpam-businesscentral-monitoring-rhel8</code>
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${KIE_SERVER_IMAGE_STREAM_NAME}</code>



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

#### 5.1.2.3.3.3. Readiness プロブ

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

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

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

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

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

/usr/libexec/check-container

#### 5.1.2.3.3.4. Liveness Probe

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

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

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

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

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

/usr/libexec/check-container --live

#### 5.1.2.3.3.5. 公開されたポート

デプロイメント	名前	ポート	プロトコル
<b>\${APPLICATION_NAME}-rhpamcentrmon</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>

デプロイメント	名前	ポート	プロトコル
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	ping	8888	<b>TCP</b>
<b>\${APPLICATION_NAME}-postgresql</b>	–	5432	<b>TCP</b>

#### 5.1.2.3.3.6. イメージの環境変数

デプロイメント	変数名	説明	値の例
<b>\${APPLICATION_NAME}-rhpamcentrmon</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>	–	–
	<b>KIE_ADMIN_PWD</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>

デプロイメント	変数名	説明	値の例
	<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-rhpamcentr,!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>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を設定)。	<b>\${KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED}</b>

デプロイメント	変数名	説明	値の例
	<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ーを設定します)	<b><code>\${KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE}</code></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ーを設定)	<b><code>\${KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL}</code></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ーを設定)	<b><code>\${KIE_SERVER_CONTROLLER_TOKEN}</code></b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b><code>/etc/businesscentral-secret-volume</code></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><code>\${BUSINESS_CENTRAL_HTTPS_KEYSTORE}</code></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><code>\${BUSINESS_CENTRAL_HTTPS_NAME}</code></b>
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード。	<b><code>\${BUSINESS_CENTRAL_HTTPS_PASSWORD}</code></b>
	<b>JGROUPS_PING_PROTOCOL</b>	–	<b><code>openshift.DNS_PING</code></b>
	<b>OPENSIFT_DNS_PING_SERVICE_NAME</b>	–	<b><code>\${APPLICATION_NAME}-rhpmcentrmon-ping</code></b>

デプロイメント	変数名	説明	値の例
	<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>	Business Central Monitoring RH-SSO クライアントシークレット。	<b>\${BUSINESS_CENTRAL_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	Business Central Monitoring RH-SSO クライアント名。	<b>\${BUSINESS_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>
	<b>SSO_PASSWORD</b>	クライアント作成に使用する RH-SSO レalm の管理者のパスワード。	<b>\${SSO_PASSWORD}</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO が無効な SSL 証明書の検証。	<b>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	ユーザー名として使用する RH-SSO プリンシパル属性。	<b>\${SSO_PRINCIPAL_ATTRIBUTE}</b>
	<b>HOSTNAME_HTTP</b>	http サービスルートのカスタムホスト名。デフォルトのホスト名を使用する場合は空白にします (例: insecure- <application-name>- rhpamcentrmon- <project>.<default-domain-suffix>)。	<b>\${BUSINESS_CENTRAL_HOSTNAME_HTTP}</b>

デプロイメント	変数名	説明	値の例
	<b>HOSTNAME_HTTPS</b>	https サービスルートのカスタムのホスト名。デフォルトのホスト名を使用する場合は空白にします (例: <application-name>-rhpamcentrmon-<project>.<default-domain-suffix>)。	<b><code>\${BUSINESS_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>
	<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>

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、ユーザー自体の DN に特殊文字 (たとえば、正しいユーザーマッピングを防ぐバックスラッシュ) が含まれてい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>
	<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><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 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><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、実際のロールがである DN ではなく、ユーザーロールを含むオブジェクトがある 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。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。	<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>\${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}-rhpamcentrmon</b>
	<b>KIE_ADMIN_USER</b>	—	—
	<b>KIE_ADMIN_PWD</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>\${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 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>
	<b>KIE_SERVER_ID</b>	—	—
	<b>KIE_SERVER_ROUTE_NAME</b>	—	<b>\${APPLICATION_NAME}-kieserver</b>
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	—	OpenShiftStartupStrategy
	<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>

デプロイメント	変数名	説明	値の例
	<b>MAVEN_REPOS</b>	—	RHPAMCENTR,EXTERNAL
	<b>RHPAMCENTR_MAVEN_REPO_ID</b>	—	repo-rhpamcentr
	<b>RHPAMCENTR_MAVEN_REPO_SERVICE</b>	maven リポジトリの使用状況など、サービスのルックアップができるように任意の Business Central に到達可能な場合に使用するサービス名 (必要な場合)	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>RHPAMCENTR_MAVEN_REPO_PATH</b>	—	/maven2/
	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	—	—
	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</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-rhpamcentr,!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>

デプロイメント	変数名	説明	値の例
	<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_PERSISTENCE_DS</b>	KIE Server 永続データソース。 (org.kie.server.persistence.ds システムプロパティを設定)	<b>\${KIE_SERVER_PERSISTENCE_DS}</b>
	<b>DATASOURCES</b>	—	<b>RHPAM</b>
	<b>RHPAM_JNDI</b>	KIE Server 永続データソース。 (org.kie.server.persistence.ds システムプロパティを設定)	<b>\${KIE_SERVER_PERSISTENCE_DS}</b>
	<b>RHPAM_JTA</b>	—	true
	<b>RHPAM_DATABASE</b>	KIE Server PostgreSQL データベース名。	<b>\${KIE_SERVER_POSTGRES_DB}</b>
	<b>RHPAM_DRIVER</b>	—	postgresql
	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE Server PostgreSQL Hibernate 方言。	<b>\${KIE_SERVER_POSTGRES_DIALECT}</b>
	<b>RHPAM_USERNAME</b>	KIE Server PostgreSQL データベースのユーザー名。	<b>\${KIE_SERVER_POSTGRES_USER}</b>
	<b>RHPAM_PASSWORD</b>	KIE Server PostgreSQL データベースのパスワード。	<b>\${KIE_SERVER_POSTGRES_PWD}</b>
	<b>RHPAM_SERVICE_HOST</b>	—	<b>\${APPLICATION_NAME}-postgresql</b>
	<b>RHPAM_SERVICE_PORT</b>	—	5432

デプロイメント	変数名	説明	値の例
	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	EJB タイマーサービスのデータベースデータストアの更新間隔を設定します。	<b><code>\${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}</code></b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b><code>/etc/kieserver-secret-volume</code></b>
	<b>HTTPS_KEYSTORE</b>	シークレット内のキーストアファイル名	<b><code>\${KIE_SERVER_HTTPS_KEYSTORE}</code></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><code>\${KIE_SERVER_HTTPS_NAME}</code></b>
	<b>HTTPS_PASSWORD</b>	キーストアおよび証明書のパスワード	<b><code>\${KIE_SERVER_HTTPS_PASSWORD}</code></b>
	<b>JGROUPS_PING_PROTOCOL</b>	–	<b><code>openshift.DNS_PING</code></b>
	<b>OPENSIFT_DNS_PING_SERVICE_NAME</b>	–	<b><code>\${APPLICATION_NAME}-kieserver-ping</code></b>
	<b>OPENSIFT_DNS_PING_SERVICE_PORT</b>	–	<b><code>8888</code></b>
	<b>SSO_URL</b>	RH-SSO URL。	<b><code>\${SSO_URL}</code></b>
	<b>SSO_OPENIDCONNECT_DEPLOYMENTS</b>	–	<b><code>ROOT.war</code></b>
	<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>

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>	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>\${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、ユーザー自体の DN に特殊文字 (たとえば、正しいユーザーマッピングを防ぐバックスラッシュ) が含まれてい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_STR ING</b>	ユーザー名を公開するため、DN の最初から削除される文字列を定義します。このオプションは usernameEndString と合わせて使用し、parseUsername が true に設定されている場合にのみ考慮されます。	<b>\${AUTH_LDAP_USE RNAME_BEGIN_STR ING}</b>
	<b>AUTH_LDAP_USER NAME_END_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_USE RNAME_END_STRIN G}</b>
	<b>AUTH_LDAP_ROLE_ ATTRIBUTE_ID</b>	ユーザーロールを含む属性の名前。	<b>\${AUTH_LDAP_ROL E_ATTRIBUTE_ID}</b>
	<b>AUTH_LDAP_ROLE S_CTX_DN</b>	ユーザーロールを検索するコンテキストの固定 DN。これは、実際のロールがである DN ではなく、ユーザーロールを含むオブジェクトがある DN です。たとえば、Microsoft Active Directory サーバーでは、これは、ユーザーアカウントが存在する DN です。	<b>\${AUTH_LDAP_ROL ES_CTX_DN}</b>

デプロイメント	変数名	説明	値の例
	<b>AUTH_LDAP_ROLE_FILTER</b>	認証済みユーザーと関連付けられたロールを検索するために使用される検索フィルター。{0} 式を使用しているフィルターに、入力ユーザー名、またはログインモジュールコールバックから取得した userDN が置換されます。認証済み userDN は {1} が使用されたフィルターに置き換えられます。入力ユーザー名に一致する検索フィルター例は (member={0}) です。認証済み userDN に一致する他の例は (member={1}) です。	<b><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>\${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}-postgresql</b>	<b>POSTGRESQL_USER</b>	KIE Server PostgreSQL データベースのユーザー名。	<b>\${KIE_SERVER_POSTGRESQL_USER}</b>
	<b>POSTGRESQL_PASSWORD</b>	KIE Server PostgreSQL データベースのパスワード。	<b>\${KIE_SERVER_POSTGRESQL_PWD}</b>
	<b>POSTGRESQL_DATABASE</b>	KIE Server PostgreSQL データベース名。	<b>\${KIE_SERVER_POSTGRESQL_DB}</b>
	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	PostgreSQL による XA トランザクションの処理を許可します。	<b>\${POSTGRESQL_MAX_PREPARED_TRANSACTIONS}</b>

#### 5.1.2.3.3.7. ボリューム

デプロイメント	名前	mountPath	目的	readOnly
<b>\${APPLICATION_NAME}-rhpamcentrmon</b>	businesscentral-keystore-volume	<b>/etc/businesscentral-secret-volume</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
<code>\${APPLICATION_NAME}-postgresql</code>	<code>\${APPLICATION_NAME}-postgresql-pvol</code>	<code>/var/lib/pgsql/data</code>	postgresql	false

#### 5.1.2.4. 外部の依存関係

##### 5.1.2.4.1. ボリューム要求

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

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

##### 5.1.2.4.2. シークレット

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

businesscentral-app-secret kieserver-app-secret

## 5.2. 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 Process Automation Manager テンプレートをデプロイし、モニターし、管理し、デプロイ解除するには、OpenShift Web コンソールまたは **oc** コマンドを使用できます。

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

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

- プロジェクトを作成するには、以下のコマンドを使用します。

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

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

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

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

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

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

```
$ oc get pods
```

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

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

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

- Pod のログを表示するには、以下のコマンドを使用します。

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

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

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

詳細は、「[デプロイメントログの表示](#)」を参照してください。

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

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

詳細は、「[ビルドログのアクセス](#)」を参照してください。

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

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

詳細は、「[手動スケーリング](#)」を参照してください。

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

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

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

## 付録A バージョン情報

本書の最終更新日：2021年6月25日（金）