



## Red Hat Process Automation Manager 7.5

Deploying a Red Hat Process Automation  
Manager immutable server environment on  
Red Hat OpenShift Container Platform



# Red Hat Process Automation Manager 7.5 Deploying a Red Hat Process Automation Manager immutable server environment on Red Hat OpenShift Container Platform

---

Red Hat Customer Content Services

[brms-docs@redhat.com](mailto:brms-docs@redhat.com)

## Legal Notice

Copyright © 2021 Red Hat, Inc.

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

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

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

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

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

Linux<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.

## Abstract

This document describes how to deploy a Red Hat Process Automation Manager 7.5 immutable server environment on Red Hat OpenShift Container Platform.

# Table of Contents

<b>PREFACE</b> .....	<b>6</b>
<b>CHAPTER 1. OVERVIEW OF RED HAT PROCESS AUTOMATION MANAGER ON RED HAT OPENSIFT CONTAINER PLATFORM</b> .....	<b>7</b>
<b>CHAPTER 2. PREPARING TO DEPLOY RED HAT PROCESS AUTOMATION MANAGER IN YOUR OPENSIFT ENVIRONMENT</b> .....	<b>9</b>
2.1. ENSURING THE AVAILABILITY OF IMAGE STREAMS AND THE IMAGE REGISTRY	9
2.2. CREATING THE SECRETS FOR PROCESS SERVER	10
2.3. CREATING THE SECRETS FOR BUSINESS CENTRAL	11
2.4. CREATING THE SECRETS FOR SMART ROUTER	11
2.5. BUILDING A CUSTOM PROCESS SERVER EXTENSION IMAGE FOR AN EXTERNAL DATABASE	12
2.6. EXTRACTING THE SOURCE CODE FROM BUSINESS CENTRAL FOR USE IN AN S2I BUILD	14
2.7. PREPARING A MAVEN MIRROR REPOSITORY FOR OFFLINE USE	14
<b>CHAPTER 3. ENVIRONMENT WITH IMMUTABLE SERVERS</b> .....	<b>17</b>
3.1. DEPLOYING BUSINESS CENTRAL MONITORING AND SMART ROUTER FOR AN ENVIRONMENT WITH IMMUTABLE SERVERS	17
3.1.1. Starting configuration of the template for monitoring and Smart Router	18
3.1.2. Setting required parameters for monitoring and Smart Router	19
3.1.3. Configuring the image stream namespace for monitoring and Smart Router	20
3.1.4. Setting parameters for RH-SSO authentication for monitoring and Smart Router	20
3.1.5. Setting parameters for LDAP authentication for monitoring and Smart Router	22
3.1.6. Completing deployment of the template for monitoring and Smart Router	23
3.2. DEPLOYING AN IMMUTABLE PROCESS SERVER USING AN S2I BUILD	23
3.2.1. Starting configuration of the template for an immutable Process Server using S2I	24
3.2.2. Setting required parameters for an immutable Process Server using S2I	25
3.2.3. Configuring the image stream namespace for an immutable Process Server using S2I	26
3.2.4. Configuring information about a Business Central or Business Central Monitoring instance for an immutable Process Server using S2I	26
3.2.5. Setting an optional Maven repository for an immutable Process Server using S2I	27
3.2.6. Configuring access to a Maven mirror in an environment without a connection to the public Internet for an immutable Process Server using S2I	28
3.2.7. Configuring communication with an AMQ server for an immutable Process Server using S2I	28
3.2.8. Setting parameters for RH-SSO authentication for an immutable Process Server using S2I	29
3.2.9. Setting parameters for LDAP authentication for an immutable Process Server using S2I	31
3.2.10. Setting parameters for using an external database server for an immutable Process Server using S2I	32
3.2.11. Enabling Prometheus metric collection for an immutable Process Server using S2I	34
3.2.12. Completing deployment of the template for an immutable Process Server using S2I	34
3.3. MODIFYING THE TEMPLATE FOR DEPLOYING AN IMMUTABLE PROCESS SERVER USING S2I	34
3.4. DEPLOYING AN IMMUTABLE PROCESS SERVER FROM KJAR SERVICES	36
3.4.1. Starting configuration of the template for an immutable Process Server from KJAR services	36
3.4.2. Setting required parameters for an immutable Process Server from KJAR services	37
3.4.3. Configuring the image stream namespace for an immutable Process Server from KJAR services	38
3.4.4. Configuring information about a Business Central or Business Central Monitoring instance for an immutable Process Server from KJAR services	39
3.4.5. Configuring access to a Maven mirror in an environment without a connection to the public Internet for an immutable Process Server from KJAR services	40
3.4.6. Setting parameters for RH-SSO authentication for an immutable Process Server from KJAR services	40
3.4.7. Setting parameters for LDAP authentication for an immutable Process Server from KJAR services	42
3.4.8. Setting parameters for using an external database server for an immutable Process Server from KJAR	

services	43
3.4.9. Enabling Prometheus metric collection for an immutable Process Server from KJAR services	45
3.4.10. Completing deployment of the template for an immutable Process Server from KJAR services	45
3.5. (OPTIONAL) PROVIDING THE LDAP ROLE MAPPING FILE	45
<b>CHAPTER 4. RED HAT PROCESS AUTOMATION MANAGER ROLES AND USERS</b>	<b>47</b>
<b>CHAPTER 5. OPENSIFT TEMPLATE REFERENCE INFORMATION</b>	<b>49</b>
5.1. RHPAM75-PROD-IMMUTABLE-MONITOR.YAML TEMPLATE	49
5.1.1. Parameters	49
5.1.2. Objects	63
5.1.2.1. Services	63
5.1.2.2. Routes	63
5.1.2.3. Deployment Configurations	63
5.1.2.3.1. Triggers	64
5.1.2.3.2. Replicas	64
5.1.2.3.3. Pod Template	64
5.1.2.3.3.1. Service Accounts	64
5.1.2.3.3.2. Image	64
5.1.2.3.3.3. Readiness Probe	65
5.1.2.3.3.4. Liveness Probe	65
5.1.2.3.3.5. Exposed Ports	65
5.1.2.3.3.6. Image Environment Variables	65
5.1.2.3.3.7. Volumes	76
5.1.2.4. External Dependencies	76
5.1.2.4.1. Volume Claims	76
5.1.2.4.2. Secrets	77
5.2. RHPAM75-PROD-IMMUTABLE-KIESERVER.YAML TEMPLATE	77
5.2.1. Parameters	77
5.2.2. Objects	92
5.2.2.1. Services	92
5.2.2.2. Routes	92
5.2.2.3. Build Configurations	92
5.2.2.4. Deployment Configurations	93
5.2.2.4.1. Triggers	93
5.2.2.4.2. Replicas	93
5.2.2.4.3. Pod Template	93
5.2.2.4.3.1. Service Accounts	93
5.2.2.4.3.2. Image	94
5.2.2.4.3.3. Readiness Probe	94
5.2.2.4.3.4. Liveness Probe	94
5.2.2.4.3.5. Exposed Ports	94
5.2.2.4.3.6. Image Environment Variables	95
5.2.2.4.3.7. Volumes	106
5.2.2.5. External Dependencies	106
5.2.2.5.1. Volume Claims	106
5.2.2.5.2. Secrets	106
5.3. RHPAM75-PROD-IMMUTABLE-KIESERVER-AMQ.YAML TEMPLATE	106
5.3.1. Parameters	106
5.3.2. Objects	124
5.3.2.1. Services	124
5.3.2.2. Routes	125
5.3.2.3. Build Configurations	126

---

5.3.2.4. Deployment Configurations	126
5.3.2.4.1. Triggers	126
5.3.2.4.2. Replicas	126
5.3.2.4.3. Pod Template	127
5.3.2.4.3.1. Service Accounts	127
5.3.2.4.3.2. Image	127
5.3.2.4.3.3. Readiness Probe	127
5.3.2.4.3.4. Liveness Probe	127
5.3.2.4.3.5. Exposed Ports	128
5.3.2.4.3.6. Image Environment Variables	128
5.3.2.4.3.7. Volumes	143
5.3.2.5. External Dependencies	143
5.3.2.5.1. Volume Claims	143
5.3.2.5.2. Secrets	143
5.4. RHPAM75-KIESERVER-EXTERNALDB.YAML TEMPLATE	143
5.4.1. Parameters	144
5.4.2. Objects	161
5.4.2.1. Services	161
5.4.2.2. Routes	161
5.4.2.3. Build Configurations	161
5.4.2.4. Deployment Configurations	162
5.4.2.4.1. Triggers	162
5.4.2.4.2. Replicas	162
5.4.2.4.3. Pod Template	162
5.4.2.4.3.1. Service Accounts	162
5.4.2.4.3.2. Image	162
5.4.2.4.3.3. Readiness Probe	162
5.4.2.4.3.4. Liveness Probe	163
5.4.2.4.3.5. Exposed Ports	163
5.4.2.4.3.6. Image Environment Variables	163
5.4.2.4.3.7. Volumes	176
5.4.2.5. External Dependencies	176
5.4.2.5.1. Secrets	176
5.5. RHPAM75-KIESERVER-MYSQL.YAML TEMPLATE	176
5.5.1. Parameters	176
5.5.2. Objects	191
5.5.2.1. Services	191
5.5.2.2. Routes	191
5.5.2.3. Deployment Configurations	191
5.5.2.3.1. Triggers	191
5.5.2.3.2. Replicas	192
5.5.2.3.3. Pod Template	192
5.5.2.3.3.1. Service Accounts	192
5.5.2.3.3.2. Image	192
5.5.2.3.3.3. Readiness Probe	192
5.5.2.3.3.4. Liveness Probe	193
5.5.2.3.3.5. Exposed Ports	193
5.5.2.3.3.6. Image Environment Variables	193
5.5.2.3.3.7. Volumes	204
5.5.2.4. External Dependencies	204
5.5.2.4.1. Volume Claims	204
5.5.2.4.2. Secrets	205
5.6. RHPAM75-KIESERVER-POSTGRESQL.YAML TEMPLATE	205

---

5.6.1. Parameters	205
5.6.2. Objects	220
5.6.2.1. Services	220
5.6.2.2. Routes	220
5.6.2.3. Deployment Configurations	220
5.6.2.3.1. Triggers	220
5.6.2.3.2. Replicas	221
5.6.2.3.3. Pod Template	221
5.6.2.3.3.1. Service Accounts	221
5.6.2.3.3.2. Image	221
5.6.2.3.3.3. Readiness Probe	221
5.6.2.3.3.4. Liveness Probe	222
5.6.2.3.3.5. Exposed Ports	222
5.6.2.3.3.6. Image Environment Variables	222
5.6.2.3.3.7. Volumes	234
5.6.2.4. External Dependencies	234
5.6.2.4.1. Volume Claims	234
5.6.2.4.2. Secrets	234
5.7. OPENSIFT USAGE QUICK REFERENCE	234
<b>APPENDIX A. VERSIONING INFORMATION</b> .....	<b>236</b>



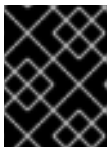


## PREFACE

As a system engineer, you can deploy a Red Hat Process Automation Manager immutable server environment on Red Hat OpenShift Container Platform to provide an infrastructure to execute services, process applications, and other business assets. You can use standard integration tools to manage the immutable Process Server image. You can create new server images to add and update the business assets.

### Prerequisites

- Red Hat OpenShift Container Platform version 3.11 is deployed.
- At least four gigabytes of memory are available in the OpenShift cluster/namespace.
  - If you do not deploy monitoring infrastructure but only deploy an immutable Process Server, three gigabytes can be sufficient.
- The OpenShift project for the deployment has been created.
- You are logged in to the project using the **oc** command. For more information about the **oc** command-line tool, see the OpenShift [CLI Reference](#). If you want to use the OpenShift Web console to deploy templates, you must also be logged on using the Web console.
- Dynamic persistent volume (PV) provisioning is enabled. Alternatively, if dynamic PV provisioning is not enabled, enough persistent volumes must be available. By default, the following sizes are required:
  - Each immutable server deployment includes a replicated set of Process Server pods, which, by default, requires one 1Gi PV for the database. You can change the database PV size in the template parameters. You can deploy multiple immutable servers; each requires a separate database PV. This requirement does not apply if you use an external database server.
  - If you deploy the immutable monitoring template, two 64Mi PVs are also required (one for Business Central Monitoring and one for Smart Router).
- If you intend to deploy the immutable monitoring template, your OpenShift environment supports persistent volumes with **ReadWriteMany** mode. For information about access mode support in OpenShift Online volume plug-ins, see [Access Modes](#).



### IMPORTANT

**ReadWriteMany** mode is not supported on OpenShift Online and OpenShift Dedicated.



### NOTE

Since Red Hat Process Automation Manager version 7.5, support for Red Hat OpenShift Container Platform 3.x is deprecated, including installation using all templates and using the Automation Broker (Ansible Playbook). New features might not be added, and this functionality will be removed in a future release.

# CHAPTER 1. OVERVIEW OF RED HAT PROCESS AUTOMATION MANAGER ON RED HAT OPENSIFT CONTAINER PLATFORM

You can deploy Red Hat Process Automation Manager into a Red Hat OpenShift Container Platform environment.

In this solution, components of Red Hat Process Automation Manager are deployed as separate OpenShift pods. You can scale each of the pods up and down individually to provide as few or as many containers as required for a particular component. You can use standard OpenShift methods to manage the pods and balance the load.

The following key components of Red Hat Process Automation Manager are available on OpenShift:

- Process Server, also known as *Execution Server* or *KIE Server*, is the infrastructure element that runs decision services, process applications, and other deployable assets (collectively referred to as *services*). All logic of the services runs on execution servers.

A database server is normally required for Process Server. You can provide a database server in another OpenShift pod or configure an execution server on OpenShift to use any other database server. Alternatively, Process Server can use an H2 database; in this case, you cannot scale the pod.

You can scale up a Process Server pod to provide as many copies as required, running on the same host or different hosts. As you scale a pod up or down, all of its copies use the same database server and run the same services. OpenShift provides load balancing and a request can be handled by any of the pods.

You can deploy a separate Process Server pod to run a different group of services. That pod can also be scaled up or down. You can have as many separate replicated Process Server pods as required.

- Business Central is a web-based interactive environment used for authoring services. It also provides a management and monitoring console. You can use Business Central to develop services and deploy them to Process Servers. You can also use Business Central to monitor the execution of processes.

Business Central is a centralized application. However, you can configure it for high availability, where multiple pods run and share the same data.

Business Central includes a Git repository that holds the source for the services that you develop on it. It also includes a built-in Maven repository. Depending on configuration, Business Central can place the compiled services (KJAR files) into the built-in Maven repository or (if configured) into an external Maven repository.



## IMPORTANT

In the current version, high-availability Business Central functionality is for Technology Preview only. For more information on Red Hat Technology Preview features, see [Technology Preview Features Scope](#).

- Business Central Monitoring is a web-based management and monitoring console. It can manage the deployment of services to Process Servers and provide monitoring information, but does not include authoring capabilities. You can use this component to manage staging and production environments.
- Smart Router is an optional layer between Process Servers and other components that interact with them. When your environment includes many services running on different Process

Servers, Smart Router provides a single endpoint to all client applications. A client application can make a REST API call that requires any service. Smart Router automatically calls the Process Server that can process a particular request.

You can arrange these and other components into various environment configurations within OpenShift.

The following environment types are typical:

- *Authoring*: An environment for creating and modifying services using Business Central. It consists of pods that provide Business Central for the authoring work and a Process Server for test execution of the services. For instructions about deploying this environment, see [Deploying a Red Hat Process Automation Manager authoring environment on Red Hat OpenShift Container Platform](#).
- *Managed deployment*: An environment for running existing services for staging and production purposes. This environment includes several groups of Process Server pods; you can deploy and undeploy services on every such group and also scale the group up or down as necessary. Use Business Central Monitoring to deploy, run, and stop the services and to monitor their execution. You can deploy two types of managed environment. In a *freeform* server environment, you initially deploy Business Central Monitoring and one Process Server. You can additionally deploy any number of Process Servers. Business Central Monitoring can connect to all servers in the same namespace. For instructions about deploying this environment, see [Deploying a Red Hat Process Automation Manager freeform managed server environment on Red Hat OpenShift Container Platform](#).

Alternatively, you can deploy a *fixed* managed server environment. A single deployment includes Business Central Monitoring, Smart Router, and a preset number of Process Servers (by default, two servers, but you can modify the template to change the number). You cannot easily add or remove servers at a later time. For instructions about deploying this environment, see [Deploying a Red Hat Process Automation Manager fixed managed server environment on Red Hat OpenShift Container Platform](#).

- *Deployment with immutable servers*: An alternate environment for running existing services for staging and production purposes. In this environment, when you deploy a Process Server pod, it builds an image that loads and starts a service or group of services. You cannot stop any service on the pod or add any new service to the pod. If you want to use another version of a service or modify the configuration in any other way, you deploy a new server image and displace the old one. In this system, the Process Server runs like any other pod on the OpenShift environment; you can use any container-based integration workflows and do not need to use any other tools to manage the pods. Optionally, you can use Business Central Monitoring to monitor the performance of the environment and to stop and restart some of the service instances, but not to deploy additional services to any Process Server or undeploy any existing ones (you cannot add or remove containers). For instructions about deploying this environment, see [Deploying a Red Hat Process Automation Manager immutable server environment on Red Hat OpenShift Container Platform](#).

You can also deploy a *trial* or evaluation environment. This environment includes Business Central and a Process Server. You can set it up quickly and use it to evaluate or demonstrate developing and running assets. However, the environment does not use any persistent storage, and any work you do in the environment is not saved. For instructions about deploying this environment, see [Deploying a Red Hat Process Automation Manager trial environment on Red Hat OpenShift Container Platform](#).

To deploy a Red Hat Process Automation Manager environment on OpenShift, you can use the templates that are provided with Red Hat Process Automation Manager. You can modify the templates to ensure that the configuration suits your environment.

## CHAPTER 2. PREPARING TO DEPLOY RED HAT PROCESS AUTOMATION MANAGER IN YOUR OPENSIFT ENVIRONMENT

Before deploying Red Hat Process Automation Manager in your OpenShift environment, you must complete several tasks. You do not need to repeat these tasks if you want to deploy additional images, for example, for new versions of processes or for other processes.

### 2.1. ENSURING THE AVAILABILITY OF IMAGE STREAMS AND THE IMAGE REGISTRY

To deploy Red Hat Process Automation Manager components on Red Hat OpenShift Container Platform, you must ensure that OpenShift can download the correct images from the Red Hat registry. To download the images, OpenShift requires *image streams*, which contain the information about the location of images. OpenShift also must be configured to authenticate with the Red Hat registry using your service account user name and password.

Some versions of the OpenShift environment include the required image streams. You must check if they are available. If image streams are available in OpenShift by default, you can use them if the OpenShift infrastructure is configured for registry authentication server. The administrator must complete the registry authentication configuration when installing the OpenShift environment.

Otherwise, you can configure registry authentication in your own project and install the image streams in that project.

#### Procedure

1. Determine whether Red Hat OpenShift Container Platform is configured with the user name and password for Red Hat registry access. For details about the required configuration, see [Configuring a Registry Location](#). If you are using an OpenShift Online subscription, it is configured for Red Hat registry access.
2. If Red Hat OpenShift Container Platform is configured with the user name and password for Red Hat registry access, enter the following commands:

```
$ oc get imagestreamtag -n openshift | grep -F rhpam-businesscentral | grep -F 7.5
$ oc get imagestreamtag -n openshift | grep -F rhpam-kieserver | grep -F 7.5
```

If the outputs of both commands are not empty, the required image streams are available in the **openshift** namespace and no further action is required.

3. If the output of one or both of the commands is empty or if OpenShift is not configured with the user name and password for Red Hat registry access, complete the following steps:
  - a. Ensure you are logged in to OpenShift with the **oc** command and that your project is active.
  - b. Complete the steps documented in [Registry Service Accounts for Shared Environments](#). You must log in to the Red Hat Customer Portal to access the document and to complete the steps to create a registry service account.
  - c. Select the **OpenShift Secret** tab and click the link under **Download secret** to download the YAML secret file.
  - d. View the downloaded file and note the name that is listed in the **name:** entry.

- e. Enter the following commands:

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

Replace **<file\_name>** with the name of the downloaded file and **<secret\_name>** with the name that is listed in the **name:** entry of the file.

- f. Download the **rhcam-7.5.1-openshift-templates.zip** product deliverable file from the [Software Downloads](#) page and extract the **rhcam75-image-streams.yaml** file.
- g. Enter the following command:

```
$ oc apply -f rhcam75-image-streams.yaml
```



#### NOTE

If you complete these steps, you install the image streams into the namespace of your project. In this case, when you deploy the templates, you must set the **IMAGE\_STREAM\_NAMESPACE** parameter to the name of this project.

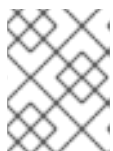
## 2.2. CREATING THE SECRETS FOR PROCESS SERVER

OpenShift uses objects called *secrets* to hold sensitive information such as passwords or keystores. For more information about OpenShift secrets, see the [Secrets chapter](#) in the OpenShift documentation.

You must create an SSL certificate for HTTP access to Process Server and provide it to your OpenShift environment as a secret.

### Procedure

1. Generate an SSL keystore with a private and public key for SSL encryption for Process Server. For more information on how to create a keystore with self-signed or purchased SSL certificates, see [Generate a SSL Encryption Key and Certificate](#).



#### NOTE

In a production environment, generate a valid signed certificate that matches the expected URL for Process Server.

2. Save the keystore in a file named **keystore.jks**.
3. Record the name of the certificate. The default value for this name in Red Hat Process Automation Manager configuration is **jboss**.
4. Record the password of the keystore file. The default value for this name in Red Hat Process Automation Manager configuration is **mykeystorepass**.
5. Use the **oc** command to generate a secret named **kieserver-app-secret** from the new keystore file:

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

## 2.3. CREATING THE SECRETS FOR BUSINESS CENTRAL

You must create an SSL certificate for HTTP access to Business Central and provide it to your OpenShift environment as a secret.

Do not use the same certificate and keystore for Business Central and Process Server.

### Procedure

1. Generate an SSL keystore with a private and public key for SSL encryption for Business Central. For more information on how to create a keystore with self-signed or purchased SSL certificates, see [Generate a SSL Encryption Key and Certificate](#).



### NOTE

In a production environment, generate a valid signed certificate that matches the expected URL for Business Central.

2. Save the keystore in a file named **keystore.jks**.
3. Record the name of the certificate. The default value for this name in Red Hat Process Automation Manager configuration is **jboss**.
4. Record the password of the keystore file. The default value for this name in Red Hat Process Automation Manager configuration is **mykeystorepass**.
5. Use the **oc** command to generate a secret named **businesscentral-app-secret** from the new keystore file:

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

## 2.4. CREATING THE SECRETS FOR SMART ROUTER

You must create an SSL certificate for HTTP access to Smart Router and provide it to your OpenShift environment as a secret.

Do not use the same certificate and keystore for Smart Router as the ones used for Process Server or Business Central.

### Procedure

1. Generate an SSL keystore with a private and public key for SSL encryption for Smart Router. For more information on how to create a keystore with self-signed or purchased SSL certificates, see [Generate a SSL Encryption Key and Certificate](#).



### NOTE

In a production environment, generate a valid signed certificate that matches the expected URL for Smart Router.

2. Save the keystore in a file named **keystore.jks**.

3. Record the name of the certificate. The default value for this name in Red Hat Process Automation Manager configuration is **jboss**.
4. Record the password of the keystore file. The default value for this name in Red Hat Process Automation Manager configuration is **mykeystorepass**.
5. Use the **oc** command to generate a secret named **smartrouter-app-secret** from the new keystore file:

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

## 2.5. BUILDING A CUSTOM PROCESS SERVER EXTENSION IMAGE FOR AN EXTERNAL DATABASE

If you want to use an external database server for a Process Server and the database server is not a MySQL or PostgreSQL server, you must build a custom Process Server extension image with drivers for this server before deploying your environment.

Complete the steps in this build procedure to provide drivers for any of the following database servers:

- Microsoft SQL Server
- MariaDB
- IBM DB2
- Oracle Database
- Sybase

For the supported versions of the database servers, see [Red Hat Process Automation Manager 7 Supported Configurations](#).

The build procedure creates a custom extension image that extends the existing Process Server image. You must import this custom extension image into your OpenShift environment and then reference it in the **EXTENSION\_IMAGE** parameter.

### Prerequisites

- You are logged in to your OpenShift environment using the **oc** command. Your OpenShift user must have the **registry-editor** role.
- For Oracle Database or Sybase, you downloaded the JDBC driver from the database server vendor.
- You have installed the following required software:
  - Docker
  - Cektit version 3.2
  - The following libraries and extensions for Cektit:
    - **odcs-client**, provided by the **python3-odcs-client** package or similar package
    - **docker**, provided by the **python3-docker** package or similar package



- **docker-squash**, provided by the **python3-docker-squash** package or similar package
- **behave**, provided by the **python3-behave** package or similar package
- **s2i**, provided by the **source-to-image** package or similar package

## Procedure

1. For IBM DB2, Oracle Database, or Sybase, provide the JDBC driver JAR file in a local directory.
2. Download the **rhpam-7.5.1-openshift-templates.zip** product deliverable file from the [Software Downloads](#) page of the Red Hat Customer Portal.
3. Unzip the file and, using the command line, change to the **templates/contrib/jdbc** directory of the unzipped file. This directory contains the source code for the custom build.
4. Run one of the following commands, depending on the database server type:

- For Microsoft SQL Server:

```
make build mssql
```

- For MariaDB:

```
make build mariadb
```

- For IBM DB2:

```
make build db2
```

- For Oracle Database:

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

In this command, replace **/tmp/ojdbc7.jar** with the path name of the downloaded Oracle Database driver and **7.0** with the version of the driver.

- For Sybase:

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

In this command, replace **/tmp/jconn4-16.0\_PL05.jar** with the path name of the downloaded Sybase driver and **16.0\_PL05** with the version of the driver.

5. Run the following command to list the Docker images that are available locally:

```
docker images
```

Note the name of the image that was built, for example, **jboss-kie-db2-extension-openshift-image**, and the version tag of the image, for example, **11.1.4.4** (not the **latest** tag).

6. Access the registry of your OpenShift environment directly and push the image to the registry. Depending on your user permissions, you can push the image into the **openshift** namespace or into a project namespace. For instructions about accessing the registry and pushing the images, see [Accessing the Registry Directly](#).

- When configuring your Process Server deployment with a template that supports an external database server, set the following parameters:
  - Drivers Extension Image (`EXTENSIONS_IMAGE`):** The ImageStreamTag definition of the extension image, for example, **`jboss-kie-db2-extension-openshift-image:11.1.4.4`**
  - Drivers ImageStream Namespace (`EXTENSIONS_IMAGE_NAMESPACE`):** The namespace to which you uploaded the extension image, for example, **`openshift`** or your project namespace.

## 2.6. EXTRACTING THE SOURCE CODE FROM BUSINESS CENTRAL FOR USE IN AN S2I BUILD

If you are using Business Central for authoring services, you can extract the source code for your service and place it into a separate Git repository, such as GitHub or an on-premise installation of GitLab, for use in the S2I build.

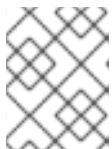
### Procedure

- Use the following command to extract the source code:

```
git clone https://<business-central-host>:443/git/<MySpace>/<MyProject>
```

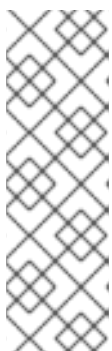
In this command, replace the following variables:

- <business-central-host>** with the host on which Business Central is running
- <MySpace>** with the name of the Business Central space in which the project is located
- <MyProject>** with the name of the project



#### NOTE

To view the full Git URL for a project in Business Central, click **Menu → Design → <MyProject> → Settings**.



#### NOTE

If you are using self-signed certificates for HTTPS communication, the command might fail with an **SSL certificate problem** error message. In this case, disable SSL certificate verification in **git**, for example, using the **`GIT_SSL_NO_VERIFY`** environment variable:

```
env GIT_SSL_NO_VERIFY=true git clone https://<business-central-host>:443/git/<MySpace>/<MyProject>
```

- Upload the source code to another Git repository, such as GitHub or GitLab, for the S2I build.

## 2.7. PREPARING A MAVEN MIRROR REPOSITORY FOR OFFLINE USE

If your Red Hat OpenShift Container Platform environment does not have outgoing access to the public Internet, you must prepare a Maven repository with a mirror of all the necessary artifacts and make this repository available to your environment.



## NOTE

You do not need to complete this procedure if your Red Hat OpenShift Container Platform environment is connected to the Internet.

## Prerequisites

- A computer that has outgoing access to the public Internet is available.

## Procedure

1. Prepare a Maven release repository to which you can write. The repository must allow read access without authentication. Your OpenShift environment must have access to this repository. You can deploy a Nexus repository manager in the OpenShift environment. For instructions about setting up Nexus on OpenShift, see [Setting up Nexus](#). Use this repository as a mirror repository. If you are planning to create immutable servers from KJAR services or to deploy Business Central Monitoring, place your services in this repository as well. You must configure this repository as the external Maven repository. You cannot configure a separate mirror repository in an immutable environment.
2. On the computer that has an outgoing connection to the public Internet, complete the following steps:

- a. Download the latest version of the [Offliner tool](#).
- b. Download the **rhcam-7.5.1-offliner.txt** product deliverable file from the [Software Downloads](#) page of the Red Hat Customer Portal.
- c. Enter the following command to use the Offliner tool to download the required artifacts:

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

Replace **/home/user/temp** with an empty temporary directory and **<version>** with the version of the Offliner tool that you downloaded. The download can take a significant amount of time.

- d. Upload all artifacts from the temporary directory to the Maven mirror repository that you prepared. You can use the [Maven Repository Provisioner](#) utility to upload the artifacts.
3. If you developed services outside Business Central and they have additional dependencies, add the dependencies to the mirror repository. If you developed the services as Maven projects, you can use the following steps to prepare these dependencies automatically. Complete the steps on the computer that has an outgoing connection to the public Internet.
    - a. Create a backup of the local Maven cache directory (**~/.m2/repository**) and then clear the directory.
    - b. Build the source of your projects using the **mvn clean install** command.
    - c. For every project, enter the following command to ensure that Maven downloads all runtime dependencies for all the artifacts generated by the project:

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

Replace **/path/to/project/pom.xml** with the correct path to the **pom.xml** file of the project.

- d. Upload all artifacts from the local Maven cache directory (`~/.m2/repository`) to the Maven mirror repository that you prepared. You can use the [Maven Repository Provisioner](#) utility to upload the artifacts.

## CHAPTER 3. ENVIRONMENT WITH IMMUTABLE SERVERS

You can deploy an environment that includes one or more pods running *immutable* Process Server with preloaded services. The database servers are, by default, also run in pods. Each Process Server pod can be separately scaled as necessary.

On an immutable Process Server, any services must be loaded onto the server at the time the image is created. You cannot deploy or undeploy services on a running immutable Process Server. The advantage of this approach is that the Process Server with the services in it runs like any other containerized service and does not require specialized management. The Process Server runs like any other pod on the OpenShift environment; you can use any container-based integration workflows as necessary.

When you create a Process Server image, you can build your services using S2I (Source to Image). Provide a Git repository with the source of your services and other business assets; if you develop the services or assets in Business Central, copy the source into a separate repository for the S2I build. OpenShift automatically builds the source, installs the services into the Process Server image, and starts the containers with the services.

If you are using Business Central for authoring services, you can extract the source for your process and place it into a separate Git repository (such as GitHub or an on-premise installation of GitLab) for use in the S2I build.

Alternatively, you can create a similar Process Server deployment using services that are already built as KJAR files. In this case, you must provide the services in a Maven repository. You can use the built-in repository of the Business Central or your own repository (for example, a Nexus deployment). When the server pod starts, it retrieves the KJAR services from the Maven repository. Services on the pod are never updated or changed. At every restart or scaling of the pod, the server retrieves the files from the repository, so you must ensure they do not change on the Maven repository to keep the deployment immutable.

With both methods of creating immutable images, no further management of the image is required. If you want to use a new version of a service, you can build a new image.

Optionally, you can also deploy a pod with Business Central Monitoring and a pod with Smart Router.

You can use Business Central Monitoring to start and stop (but not deploy) services on your Process Servers and to view monitoring data. The Business Central Monitoring instance can automatically discover any Process Servers in the same namespace, including immutable Process Servers and managed Process Servers. This feature requires the **OpenShiftStartupStrategy** setting, which is enabled for all Process Servers except those deployed in a fixed managed infrastructure. For instructions about deploying managed Process Servers with the **OpenShiftStartupStrategy** setting enabled, see [Deploying a Red Hat Process Automation Manager freeform managed server environment on Red Hat OpenShift Container Platform](#).

Smart Router is a single endpoint that can receive calls from client applications to any of your services and route each call automatically to the server that runs the service.

If you want to use Business Central Monitoring, you must provide a Maven repository. Your integration process must ensure that all the versions of KJAR files built into any Process Server image are also available in the Maven repository.

### 3.1. DEPLOYING BUSINESS CENTRAL MONITORING AND SMART ROUTER FOR AN ENVIRONMENT WITH IMMUTABLE SERVERS

You can deploy Business Central Monitoring and Smart Router for an environment with immutable servers.

You can use Business Central Monitoring to start and stop (but not deploy) services on your Process Servers and to view monitoring data. The Business Central Monitoring automatically discovers any Process Servers in the same namespace, including immutable Process Servers and managed Process Servers. This feature requires the **OpenShiftStartupStrategy** setting, which is enabled by default for all Process Servers except those deployed in a fixed managed infrastructure. For instructions about deploying managed Process Servers with the **OpenShiftStartupStrategy** setting enabled, see [Deploying a Red Hat Process Automation Manager freeform managed server environment on Red Hat OpenShift Container Platform](#).

Smart Router is a single endpoint that can receive calls from client applications to any of your services and route each call automatically to the server that runs the service.

If you want to use Business Central Monitoring, you must provide a Maven repository. Your integration process must ensure that all the versions of KJAR files built into any Process Server image are also available in the Maven repository.

### 3.1.1. Starting configuration of the template for monitoring and Smart Router

To deploy monitoring and Smart Router for an environment with immutable servers, use the **rhcam75-immutable-monitor.yaml** template file.

#### Procedure

1. Download the **rhcam-7.5.1-openshift-templates.zip** product deliverable file from the [Software Downloads](#) page of the Red Hat Customer Portal.
2. Extract the **rhcam75-immutable-monitor.yaml** template file.
3. Use one of the following methods to start deploying the template:
  - To use the OpenShift Web UI, in the OpenShift application console select **Add to Project** → **Import YAML / JSON** and then select or paste the **rhcam75-immutable-monitor.yaml** file. In the **Add Template** window, ensure **Process the template** is selected and click **Continue**.
  - To use the OpenShift command line console, prepare the following command line:

```
oc new-app -f <template-path>/rhcam75-immutable-monitor.yaml -p
BUSINESS_CENTRAL_HTTPS_SECRET=businesscentral-app-secret -p
PARAMETER=value
```

In this command line, make the following changes:

- Replace **<template-path>** with the path to the downloaded template file.
- Use as many **-p PARAMETER=value** pairs as needed to set the required parameters.

#### Next steps

Set the parameters for the template. Follow the steps in [Section 3.1.2, "Setting required parameters for monitoring and Smart Router"](#) to set common parameters. You can view the template file to see descriptions for all parameters.

### 3.1.2. Setting required parameters for monitoring and Smart Router

When configuring the template to deploy monitoring and Smart Router for an environment with immutable servers, you must set the following parameters in all cases.

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.1.1, "Starting configuration of the template for monitoring and Smart Router"](#).

#### Procedure

1. Set the following parameters:

- **Business Central Monitoring Server Keystore Secret Name** (**BUSINESS\_CENTRAL\_HTTPS\_SECRET**): The name of the secret for Business Central, as created in [Section 2.3, "Creating the secrets for Business Central"](#).
- **Smart Router Keystore Secret Name** (**KIE\_SERVER\_ROUTER\_HTTPS\_SECRET**): The name of the secret for Smart Router, as created in [Section 2.4, "Creating the secrets for Smart Router"](#).
- **Business Central Monitoring Server Certificate Name** (**BUSINESS\_CENTRAL\_HTTPS\_NAME**): The name of the certificate in the keystore that you created in [Section 2.3, "Creating the secrets for Business Central"](#).
- **Business Central Monitoring Server Keystore Password** (**BUSINESS\_CENTRAL\_HTTPS\_PASSWORD**): The password for the keystore that you created in [Section 2.3, "Creating the secrets for Business Central"](#).
- **Smart Router Certificate Name** (**KIE\_SERVER\_ROUTER\_HTTPS\_NAME**): The name of the certificate in the keystore that you created in [Section 2.4, "Creating the secrets for Smart Router"](#).
- **Smart Router Keystore Password** (**KIE\_SERVER\_ROUTER\_HTTPS\_PASSWORD**): The password for the keystore that you created in [Section 2.4, "Creating the secrets for Smart Router"](#).
- **Application Name** (**APPLICATION\_NAME**): The name of the OpenShift application. It is used in the default URLs for Business Central Monitoring and Process Server. OpenShift uses the application name to create a separate set of deployment configurations, services, routes, labels, and artifacts.
- **Enable KIE server global discovery** (**KIE\_SERVER\_CONTROLLER\_OPENSHIFT\_GLOBAL\_DISCOVERY\_ENABLED**): Set this parameter to **true** if you want Business Central Monitoring to discover all Process Servers with the **OpenShiftStartupStrategy** in the same namespace. By default, Business Central Monitoring discovers only Process Servers that are deployed with the same value of the **APPLICATION\_NAME** parameter as Business Central Monitoring itself.
- **Maven repository URL** (**MAVEN\_REPO\_URL**): A URL for a Maven repository. You must upload all the processes (KJAR files) that are to be deployed on any Process Servers in your environment into this repository.
- **Maven repository ID** (**MAVEN\_REPO\_ID**): An identifier for the Maven repository. The default value is **repo-custom**.

- **Maven repository username (MAVEN\_REPO\_USERNAME)**: The username for the Maven repository.
  - **Maven repository password (MAVEN\_REPO\_PASSWORD)**: The password for the Maven repository.
  - **ImageStream Namespace (IMAGE\_STREAM\_NAMESPACE)**: The namespace where the image streams are available. If the image streams were already available in your OpenShift environment (see [Section 2.1, “Ensuring the availability of image streams and the image registry”](#)), the namespace is **openshift**. If you have installed the image streams file, the namespace is the name of the OpenShift project.
2. You can set the following user names and passwords. By default, the deployment automatically generates the passwords.
- **KIE Admin User (KIE\_ADMIN\_USER)** and **KIE Admin Password (KIE\_ADMIN\_PWD)**: The user name and password for the administrative user. If you want to use the Business Central Monitoring to control or monitor any Process Servers, you must set and record the user name and password.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.1.6, “Completing deployment of the template for monitoring and Smart Router”](#).

### 3.1.3. Configuring the image stream namespace for monitoring and Smart Router

If you created image streams in a namespace that is not **openshift**, you must configure the namespace in the template.

If all image streams were already available in your Red Hat OpenShift Container Platform environment, you can skip this procedure.

## Prerequisites

- You started the configuration of the template, as described in [Section 3.1.1, “Starting configuration of the template for monitoring and Smart Router”](#).

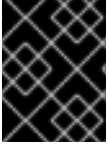
## Procedure

If you installed an image streams file according to instructions in [Section 2.1, “Ensuring the availability of image streams and the image registry”](#), set the **ImageStream Namespace (IMAGE\_STREAM\_NAMESPACE)** parameter to the name of your OpenShift project.

### 3.1.4. Setting parameters for RH-SSO authentication for monitoring and Smart Router

If you want to use RH-SSO authentication, complete the following additional configuration when configuring the template to deploy monitoring and Smart Router for an environment with immutable servers.





## IMPORTANT

Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

### Prerequisites

- A realm for Red Hat Process Automation Manager is created in the RH-SSO authentication system.
- User names and passwords for Red Hat Process Automation Manager are created in the RH-SSO authentication system. For a list of the available roles, see [Chapter 4, Red Hat Process Automation Manager roles and users](#). The following users are required in order to set the parameters for the environment:
  - An administrative user with the **kie-server,rest-all,admin** roles. This user can administer and use the environment. Process Servers use this user to authenticate with Business Central Monitoring.
  - A server user with the **kie-server,rest-all,user** roles. This user can make REST API calls to the Process Server. Business Central Monitoring uses this user to authenticate with Process Servers.
- Clients are created in the RH-SSO authentication system for all components of the Red Hat Process Automation Manager environment that you are deploying. The client setup contains the URLs for the components. You can review and edit the URLs after deploying the environment. Alternatively, the Red Hat Process Automation Manager deployment can create the clients. However, this option provides less detailed control over the environment.
- You started the configuration of the template, as described in [Section 3.1.1, “Starting configuration of the template for monitoring and Smart Router”](#).

### Procedure

1. Set the **KIE\_ADMIN\_USER** and **KIE\_ADMIN\_PASSWORD** parameters of the template to the user name and password of the administrative user that you created in the RH-SSO authentication system.
2. Set the **KIE\_SERVER\_USER** and **KIE\_SERVER\_PASSWORD** parameters of the template to the user name and password of the server user that you created in the RH-SSO authentication system.
3. Set the following parameters:
  - **RH-SSO URL (SSO\_URL)**: The URL for RH-SSO.
  - **RH-SSO Realm name (SSO\_REALM)**: The RH-SSO realm for Red Hat Process Automation Manager.
  - **RH-SSO Disable SSL Certificate Validation (SSO\_DISABLE\_SSL\_CERTIFICATE\_VALIDATION)**: Set to **true** if your RH-SSO installation does not use a valid HTTPS certificate.
4. Complete one of the following procedures:
  - a. If you created the client for Red Hat Process Automation Manager within RH-SSO, set the following parameters in the template:

- **Business Central Monitoring RH-SSO Client name**  
(**BUSINESS\_CENTRAL\_SSO\_CLIENT**): The RH-SSO client name for Business Central Monitoring.
  - **Business Central Monitoring RH-SSO Client Secret**  
(**BUSINESS\_CENTRAL\_SSO\_SECRET**): The secret string that is set in RH-SSO for the client for Business Central Monitoring.
- b. To create the clients for Red Hat Process Automation Manager within RH-SSO, set the following parameters in the template:
- **Business Central Monitoring RH-SSO Client name**  
(**BUSINESS\_CENTRAL\_SSO\_CLIENT**): The name of the client to create in RH-SSO for Business Central Monitoring.
  - **Business Central Monitoring RH-SSO Client Secret**  
(**BUSINESS\_CENTRAL\_SSO\_SECRET**): The secret string to set in RH-SSO for the client for Business Central Monitoring.
  - **RH-SSO Realm Admin Username**(**SSO\_USERNAME**) and **RH-SSO Realm Admin Password** (**SSO\_PASSWORD**): The user name and password for the realm administrator user for the RH-SSO realm for Red Hat Process Automation Manager. You must provide this user name and password in order to create the required clients.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.1.6, “Completing deployment of the template for monitoring and Smart Router”](#).

After completing the deployment, review the URLs for components of Red Hat Process Automation Manager in the RH-SSO authentication system to ensure they are correct.

## 3.1.5. Setting parameters for LDAP authentication for monitoring and Smart Router

If you want to use LDAP authentication, complete the following additional configuration when configuring the template to deploy monitoring and Smart Router for an environment with immutable servers.



### IMPORTANT

Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

## Prerequisites

- You created user names and passwords for Red Hat Process Automation Manager in the LDAP system. For a list of the available roles, see [Chapter 4, Red Hat Process Automation Manager roles and users](#). As a minimum, in order to set the parameters for the environment, you created an administrative user with the **kie-server,rest-all,admin** roles. The default user name for this user is **adminUser**. This user can administer and use the environment.
- You started the configuration of the template, as described in [Section 3.1.1, “Starting configuration of the template for monitoring and Smart Router”](#).

## Procedure

## Procedure

1. In the LDAP service, create all user names in the deployment parameters. If you do not set any of the parameters, create users with the default user names. The created users must also be assigned to roles:
  - **KIE\_ADMIN\_USER**: default user name **adminUser**, roles: **kie-server,rest-all,admin**  
For the user roles that you can configure in LDAP, see [Roles and users](#).
2. Set the **AUTH\_LDAP\*** parameters of the template. These parameters correspond to the settings of the **LdapExtended** Login module of Red Hat JBoss EAP. For instructions about using these settings, see [LdapExtended login module](#).  
If the LDAP server does not define all the roles required for your deployment, you can map LDAP groups to Red Hat Process Automation Manager roles. To enable LDAP role mapping, set the following parameters:
  - **RoleMapping rolesProperties file path (AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES)**: The fully qualified path name of a file that defines role mapping, for example, **/opt/eap/standalone/configuration/rolemapping/rolemapping.properties**. You must provide this file and mount it at this path in all applicable deployment configurations; for instructions, see [Section 3.5, "\(Optional\) Providing the LDAP role mapping file"](#).
  - **RoleMapping replaceRole property (AUTH\_ROLE\_MAPPER\_REPLACE\_ROLE)**: If set to **true**, mapped roles replace the roles defined on the LDAP server; if set to **false**, both mapped roles and roles defined on the LDAP server are set as user application roles. The default setting is **false**.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.1.6, "Completing deployment of the template for monitoring and Smart Router"](#).

### 3.1.6. Completing deployment of the template for monitoring and Smart Router

After setting all the required parameters in the OpenShift Web UI or in the command line, complete deployment of the template.

## Procedure

Depending on the method that you are using, complete the following steps:

- In the OpenShift Web UI, click **Create**.
  - If the **This will create resources that may have security or project behavior implications** message appears, click **Create Anyway**.
- Complete the command line and press Enter.

## 3.2. DEPLOYING AN IMMUTABLE PROCESS SERVER USING AN S2I BUILD

You can deploy an immutable Process Server using an S2I build. When you deploy the server, the deployment procedure retrieves the source code for any services that must run on this server, builds the services, and includes them in the server image.

You cannot deploy or undeploy services on a running immutable Process Server. You can use Business Central or Business Central Monitoring to view monitoring information. The Process Server runs like any other pod on the OpenShift environment; you can use any container-based integration workflows as necessary.

You can enable JMS capabilities of the immutable Process Server. With JMS capabilities you can interact with the server through JMS API using an external AMQ message broker.

By default, this server uses a PostgreSQL database server in a pod. To use a MySQL database server in a pod or an external database server, you can modify the template.

If a Business Central or Business Central Monitoring is deployed in the same namespace, it discovers the immutable Process Server automatically. You can use Business Central or Business Central Monitoring to start and stop (but not deploy) services on the immutable Process Server and to view monitoring data.

### 3.2.1. Starting configuration of the template for an immutable Process Server using S2I

To deploy an immutable Process Server using an S2I build, use the **rhpm75-prod-immutable-kieserver-amq.yaml** template file if you want to enable JMS capabilities. Otherwise, use the **rhpm75-prod-immutable-kieserver.yaml** template file.

#### Procedure

1. Download the **rhpm75-7.5.1-openshift-templates.zip** product deliverable file from the [Software Downloads](#) page of the Red Hat Customer Portal.
2. Extract the required template file.
3. By default, the template includes two Process Servers. Each of the serves uses a PostgreSQL database server in a pod. To change the number of Process Servers or to use a MySQL database server in a pod or an external database server, modify the template as described in [Section 3.3, "Modifying the template for deploying an immutable Process Server using S2I"](#).
4. Use one of the following methods to start deploying the template:
  - To use the OpenShift Web UI, in the OpenShift application console select **Add to Project** → **Import YAML / JSON** and then select or paste the **<template-file-name>.yaml** file. In the **Add Template** window, ensure **Process the template** is selected and click **Continue**.
  - To use the OpenShift command line console, prepare the following command line:

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

In this command line, make the following changes:

- Replace **<template-path>** with the path to the downloaded template file.
- Replace **<template-file-name>** with the name of the template file.
- Use as many **-p PARAMETER=value** pairs as needed to set the required parameters.

#### Next steps

Set the parameters for the template. Follow the steps in [Section 3.2.2, “Setting required parameters for an immutable Process Server using S2I”](#) to set common parameters. You can view the template file to see descriptions for all parameters.

### 3.2.2. Setting required parameters for an immutable Process Server using S2I

When configuring the template to deploy an immutable Process Server using an S2I build, you must set the following parameters in all cases.

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#).

#### Procedure

1. Set the following parameters:

- **KIE Server Keystore Secret Name (KIE\_SERVER\_HTTPS\_SECRET):** The name of the secret for Process Server, as created in [Section 2.2, “Creating the secrets for Process Server”](#).
- **KIE Server Certificate Name (KIE\_SERVER\_HTTPS\_NAME):** The name of the certificate in the keystore that you created in [Section 2.2, “Creating the secrets for Process Server”](#).
- **KIE Server Keystore Password (KIE\_SERVER\_HTTPS\_PASSWORD):** The password for the keystore that you created in [Section 2.2, “Creating the secrets for Process Server”](#).
- **Application Name (APPLICATION\_NAME):** The name of the OpenShift application. It is used in the default URLs for Business Central Monitoring and Process Server. OpenShift uses the application name to create a separate set of deployment configurations, services, routes, labels, and artifacts. You can deploy several applications using the same template into the same project, as long as you use different application names. Also, the application name determines the name of the server configuration (server template) that the Process Server joins on Business Central or Business Central Monitoring. If you are deploying several Process Servers, you must ensure each of the servers has a different application name.
- **KIE Server Container Deployment (KIE\_SERVER\_CONTAINER\_DEPLOYMENT):** The identifying information of the decision service (KJAR file) that the deployment must pull from the local or external repository after building your source. The format is **<containerId>=<groupId>:<artifactId>:<version>** or, if you want to specify an alias name for the container, **<containerId>(<aliasId>)=<groupId>:<artifactId>:<version>**. You can provide two or more KJAR files using the | separator, as illustrated in the following example:

```
containerId=groupId:artifactId:version|c2(alias2)=g2:a2:v2
```

To avoid duplicate container IDs, the artifact ID must be unique for each artifact built or used in your project.

- **Git Repository URL (SOURCE\_REPOSITORY\_URL):** The URL for the Git repository that contains the source for your services.
- **Git Reference (SOURCE\_REPOSITORY\_REF):** The branch in the Git repository.
- **Context Directory (CONTEXT\_DIR):** The path to the source within the project downloaded from the Git repository.

- **Artifact Directory (ARTIFACT\_DIR)**: The path within the project that contains the required binary files (KJAR files and any other necessary files) after a successful Maven build. Normally this directory is the target directory of the build. However, you can provide prebuilt binaries in this directory in the Git repository.
  - **ImageStream Namespace (IMAGE\_STREAM\_NAMESPACE)**: The namespace where the image streams are available. If the image streams were already available in your OpenShift environment (see [Section 2.1, “Ensuring the availability of image streams and the image registry”](#)), the namespace is **openshift**. If you have installed the image streams file, the namespace is the name of the OpenShift project.
2. You can set the following user name and password. By default, the deployment automatically generates the password.
    - **KIE Server User (KIE\_SERVER\_USER)** and **KIE Server Password (KIE\_SERVER\_PWD)**: The user name and password that a client application can use to connect to any of the Process Servers.

### Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, “Completing deployment of the template for an immutable Process Server using S2I”](#).

### 3.2.3. Configuring the image stream namespace for an immutable Process Server using S2I

If you created image streams in a namespace that is not **openshift**, you must configure the namespace in the template.

If all image streams were already available in your Red Hat OpenShift Container Platform environment, you can skip this procedure.

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#).

#### Procedure

If you installed an image streams file according to instructions in [Section 2.1, “Ensuring the availability of image streams and the image registry”](#), set the **ImageStream Namespace (IMAGE\_STREAM\_NAMESPACE)** parameter to the name of your OpenShift project.

### 3.2.4. Configuring information about a Business Central or Business Central Monitoring instance for an immutable Process Server using S2I

If you want to enable a connection from a Business Central or Business Central Monitoring instance in the same namespace to the Process Server, you must configure information about the Business Central or Business Central Monitoring instance.

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#).

## Procedure

1. Set the following parameters:

- **KIE Admin User (KIE\_ADMIN\_USER)** and **KIE Admin Password (KIE\_ADMIN\_PWD)**: The user name and password for the administrative user. These values must be the same as the **KIE\_ADMIN\_USER** and **KIE\_ADMIN\_PWD** settings for the Business Central or Business Central Monitoring. If the Business Central or Business Central Monitoring uses RH-SSO or LDAP authentication, these values must be a user name and password configured in the authentication system with an administrator role for the Business Central or Business Central Monitoring.
- **Name of the Business Central service (BUSINESS\_CENTRAL\_SERVICE)**: The OpenShift service name for the Business Central or Business Central Monitoring.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, "Completing deployment of the template for an immutable Process Server using S2I"](#).

### 3.2.5. Setting an optional Maven repository for an immutable Process Server using S2I

When configuring the template to deploy an immutable Process Server using an S2I build, if your source build includes dependencies that are not available on the public Maven tree and require a separate custom Maven repository, you must set parameters to access the repository.

## Prerequisites

- You started the configuration of the template, as described in [Section 3.2.1, "Starting configuration of the template for an immutable Process Server using S2I"](#).

## Procedure

To configure access to a custom Maven repository, set the following parameters:

- **Maven repository URL (MAVEN\_REPO\_URL)**: The URL for the Maven repository.
- **Maven repository ID (MAVEN\_REPO\_ID)**: An identifier for the Maven repository. The default value is **repo-custom**.
- **Maven repository username (MAVEN\_REPO\_USERNAME)**: The username for the Maven repository.
- **Maven repository password (MAVEN\_REPO\_PASSWORD)**: The password for the Maven repository.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, "Completing deployment of the template for an immutable Process Server using S2I"](#).

### 3.2.6. Configuring access to a Maven mirror in an environment without a connection to the public Internet for an immutable Process Server using S2I

When configuring the template to deploy an immutable Process Server using an S2I build, if your OpenShift environment does not have a connection to the public Internet, you must configure access to a Maven mirror that you set up according to [Section 2.7, “Preparing a Maven mirror repository for offline use”](#).

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#).

#### Procedure

To configure access to the Maven mirror, set the following parameters:

- **Maven mirror URL (MAVEN\_MIRROR\_URL)**: The URL for the Maven mirror repository that you set up in [Section 2.7, “Preparing a Maven mirror repository for offline use”](#). This URL must be accessible from a pod in your OpenShift environment.
- **Maven mirror of (MAVEN\_MIRROR\_OF)**: The value that determines which artifacts are to be retrieved from the mirror. For instructions about setting the **mirrorOf** value, see [Mirror Settings](#) in the Apache Maven documentation. The default value is **external:\***. With this value, Maven retrieves every required artifact from the mirror and does not query any other repositories.
  - If you configure an external Maven repository (**MAVEN\_REPO\_URL**), change **MAVEN\_MIRROR\_OF** to exclude the artifacts in this repository from the mirror, for example, **external:\*,!repo-custom**. Replace **repo-custom** with the ID that you configured in **MAVEN\_REPO\_ID**.
  - If you configure a built-in Business Central Maven repository (**BUSINESS\_CENTRAL\_MAVEN\_SERVICE**), change **MAVEN\_MIRROR\_OF** to exclude the artifacts in this repository from the mirror: **external:\*,!repo-rhpamcentr**.
  - If you configure both repositories, change **MAVEN\_MIRROR\_OF** to exclude the artifacts in both repositories from the mirror: **external:\*,!repo-rhpamcentr,!repo-custom**. Replace **repo-custom** with the ID that you configured in **MAVEN\_REPO\_ID**.

#### Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, “Completing deployment of the template for an immutable Process Server using S2I”](#).

### 3.2.7. Configuring communication with an AMQ server for an immutable Process Server using S2I

If you use the **rhpam75-prod-immutable-kieserver-amq.yaml** template file, JMS capabilities of the Process Server are enabled. You can interact with the server through JMS API, using an external AMQ message broker.

If necessary for your environment, you can modify the JMS configuration.

#### Prerequisites



- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#), using the **rhpan75-prod-immutable-kieserver-amq.yaml** template file.

## Procedure

Set any of the following parameters as required for your environment:

- **AMQ Username (AMQ\_USERNAME)** and **AMQ Password (AMQ\_PASSWORD)**: The user name and password of a standard broker user, if user authentication in the broker is required in your environment.
- **AMQ Role (AMQ\_ROLE)**: The user role for the standard broker user. The default role is **admin**.
- **AMQ Queues (AMQ\_QUEUES)**: AMQ queue names, separated by commas. These queues are automatically created when the broker starts and are accessible as JNDI resources in the JBoss EAP server. If you use custom queue names, you must also set the same queue names in the **KIE\_SERVER\_JMS\_QUEUE\_RESPONSE**, **KIE\_SERVER\_JMS\_QUEUE\_REQUEST**, **KIE\_SERVER\_JMS\_QUEUE\_SIGNAL**, **KIE\_SERVER\_JMS\_QUEUE\_AUDIT**, and **KIE\_SERVER\_JMS\_QUEUE\_EXECUTOR** parameters.
- **AMQ Global Max Size (AMQ\_GLOBAL\_MAX\_SIZE)**: The maximum amount of memory that message data can consume. If no value is specified, half of the memory available in the pod is allocated.
- **AMQ Protocols (AMQ\_PROTOCOL)**: Broker protocols that the Process Server can use to communicate with the AMQ server, separated by commas. Allowed values are **openwire**, **amqp**, **stomp**, and **mqtt**. Only **openwire** is supported by JBoss EAP. The default value is **openwire**.
- **AMQ Broker Image (AMQ\_BROKER\_IMAGESTREAM\_NAME)**: The image stream name for the AMQ broker image.

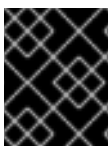
## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, “Completing deployment of the template for an immutable Process Server using S2I”](#).

### 3.2.8. Setting parameters for RH-SSO authentication for an immutable Process Server using S2I

If you want to use RH-SSO authentication, complete the following additional configuration when configuring the template to deploy an immutable Process Server using an S2I build.



#### IMPORTANT

Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

## Prerequisites

- A realm for Red Hat Process Automation Manager is created in the RH-SSO authentication system.
- User names and passwords for Red Hat Process Automation Manager are created in the RH-SSO authentication system. For a list of the available roles, see [Chapter 4, Red Hat Process](#)

*Automation Manager roles and users.* In order to set the parameters for the environment, an administrative user with the **kie-server,rest-all,admin** roles is required. The default user name for this user is **adminUser**. This user can administer and use the environment.

- Clients are created in the RH-SSO authentication system for all components of the Red Hat Process Automation Manager environment that you are deploying. The client setup contains the URLs for the components. You can review and edit the URLs after deploying the environment. Alternatively, the Red Hat Process Automation Manager deployment can create the clients. However, this option provides less detailed control over the environment.
- You started the configuration of the template, as described in [Section 3.2.1, "Starting configuration of the template for an immutable Process Server using S2I"](#).

## Procedure

1. Set the **KIE\_ADMIN\_USER** and **KIE\_ADMIN\_PASSWORD** parameters of the template to the user name and password of the administrative user that you created in the RH-SSO authentication system.
2. Set the following parameters:
  - **RH-SSO URL (SSO\_URL)**: The URL for RH-SSO.
  - **RH-SSO Realm name (SSO\_REALM)**: The RH-SSO realm for Red Hat Process Automation Manager.
  - **RH-SSO Disable SSL Certificate Validation (SSO\_DISABLE\_SSL\_CERTIFICATE\_VALIDATION)**: Set to **true** if your RH-SSO installation does not use a valid HTTPS certificate.
3. Complete one of the following procedures:
  - a. If you created the client for Red Hat Process Automation Manager within RH-SSO, set the following parameters in the template:
    - **Business Central or Business Central Monitoring RH-SSO Client name (BUSINESS\_CENTRAL\_SSO\_CLIENT)**: The RH-SSO client name for Business Central or Business Central Monitoring.
    - **KIE Server RH-SSO Client name (KIE\_SERVER\_SSO\_CLIENT)**: The RH-SSO client name for Process Server.
    - **KIE Server RH-SSO Client Secret (KIE\_SERVER\_SSO\_SECRET)**: The secret string that is set in RH-SSO for the client for Process Server.
  - b. To create the clients for Red Hat Process Automation Manager within RH-SSO, set the following parameters in the template:
    - **KIE Server RH-SSO Client name (KIE\_SERVER\_SSO\_CLIENT)**: The name of the client to create in RH-SSO for Process Server.
    - **KIE Server RH-SSO Client Secret (KIE\_SERVER\_SSO\_SECRET)**: The secret string to set in RH-SSO for the client for Process Server.
    - **RH-SSO Realm Admin Username (SSO\_USERNAME)** and **RH-SSO Realm Admin Password (SSO\_PASSWORD)**: The user name and password for the realm administrator user for the RH-SSO realm for Red Hat Process Automation Manager. You must provide this user name and password in order to create the required clients.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, “Completing deployment of the template for an immutable Process Server using S2I”](#).

After completing the deployment, review the URLs for components of Red Hat Process Automation Manager in the RH-SSO authentication system to ensure they are correct.

### 3.2.9. Setting parameters for LDAP authentication for an immutable Process Server using S2I

If you want to use LDAP authentication, complete the following additional configuration when configuring the template to deploy an immutable Process Server using an S2I build.



#### IMPORTANT

Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

#### Prerequisites

- You created user names and passwords for Red Hat Process Automation Manager in the LDAP system. For a list of the available roles, see [Chapter 4, Red Hat Process Automation Manager roles and users](#). As a minimum, in order to set the parameters for the environment, you created the following users:
  - An administrative user with the **kie-server,rest-all,admin** roles. This user can administer and use the environment.
  - A server user with the **kie-server,rest-all,user** roles. This user can make REST API calls to the Process Server.
- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#).

#### Procedure

1. In the LDAP service, create all user names in the deployment parameters. If you do not set any of the parameters, create users with the default user names. The created users must also be assigned to roles:
  - **KIE\_ADMIN\_USER**: default user name **adminUser**, roles: **kie-server,rest-all,admin**
  - **KIE\_SERVER\_USER**: default user name **executionUser**, roles **kie-server,rest-all,guest**  
For the user roles that you can configure in LDAP, see [Roles and users](#).
2. Set the **AUTH\_LDAP\*** parameters of the template. These parameters correspond to the settings of the **LdapExtended** Login module of Red Hat JBoss EAP. For instructions about using these settings, see [LdapExtended login module](#).  
If the LDAP server does not define all the roles required for your deployment, you can map LDAP groups to Red Hat Process Automation Manager roles. To enable LDAP role mapping, set the following parameters:
  - **RoleMapping rolesProperties** file path

(**AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES**): The fully qualified path name of a file that defines role mapping, for example, `/opt/eap/standalone/configuration/rolemapping/rolemapping.properties`. You must provide this file and mount it at this path in all applicable deployment configurations; for instructions, see [Section 3.5, “\(Optional\) Providing the LDAP role mapping file”](#).

- **RoleMapping replaceRole property (AUTH\_ROLE\_MAPPER\_REPLACE\_ROLE)**: If set to **true**, mapped roles replace the roles defined on the LDAP server; if set to **false**, both mapped roles and roles defined on the LDAP server are set as user application roles. The default setting is **false**.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, “Completing deployment of the template for an immutable Process Server using S2I”](#).

## 3.2.10. Setting parameters for using an external database server for an immutable Process Server using S2I

If you modified the template to use an external database server for the Process Server, as described in [Section 3.3, “Modifying the template for deploying an immutable Process Server using S2I”](#), complete the following additional configuration when configuring the template to deploy an immutable Process Server using an S2I build.

### Prerequisites

- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#).

### Procedure

1. Set the following parameters:

- **KIE Server External Database Driver (KIE\_SERVER\_EXTERNALDB\_DRIVER)**: The driver for the server, depending on the server type:
  - **mysql**
  - **postgresql**
  - **mariadb**
  - **mssql**
  - **db2**
  - **oracle**
  - **sybase**
- **KIE Server External Database User (KIE\_SERVER\_EXTERNALDB\_USER)** and **KIE Server External Database Password (KIE\_SERVER\_EXTERNALDB\_PWD)**: The user name and password for the external database server

- **KIE Server External Database URL**(**KIE\_SERVER\_EXTERNALDB\_URL**): The JDBC URL for the external database server
  - **KIE Server External Database Dialect**(**KIE\_SERVER\_EXTERNALDB\_DIALECT**): The Hibernate dialect for the server, depending on the server type:
    - **org.hibernate.dialect.MySQL5InnoDBDialect** (used for MySQL and MariaDB)
    - **org.hibernate.dialect.PostgreSQL82Dialect**
    - **org.hibernate.dialect.SQLServer2012Dialect** (used for MS SQL)
    - **org.hibernate.dialect.DB2Dialect**
    - **org.hibernate.dialect.Oracle10gDialect**
    - **org.hibernate.dialect.SybaseASE157Dialect**
  - **KIE Server External Database Host**(**KIE\_SERVER\_EXTERNALDB\_SERVICE\_HOST**): The host name of the external database server
  - **KIE Server External Database Port**(**KIE\_SERVER\_EXTERNALDB\_SERVICE\_PORT**): The port number of the external database server
  - **KIE Server External Database name**(**KIE\_SERVER\_EXTERNALDB\_DB**): The database name to use on the external database server
  - **JDBC Connection Checker class** (**KIE\_SERVER\_EXTERNALDB\_CONNECTION\_CHECKER**): The name of the JDBC connection checker class for the database server. Without this information, a database server connection cannot be restored after it is lost, for example, if the database server is rebooted.
  - **JDBC Exception Sorter class** (**KIE\_SERVER\_EXTERNALDB\_EXCEPTION\_SORTER**): The name of the JDBC exception sorter class for the database server. Without this information, a database server connection cannot be restored after it is lost, for example, if the database server is rebooted.
2. If you created a custom image for using an external database server other than MySQL or PostgreSQL, as described in [Section 2.5, "Building a custom Process Server extension image for an external database"](#), set the following parameters:
- **Drivers Extension Image** (**EXTENSIONS\_IMAGE**): The ImageStreamTag definition of the extension image, for example, **jboss-kie-db2-extension-openshift-image:11.1.4.4**
  - **Drivers ImageStream Namespace** (**EXTENSIONS\_IMAGE\_NAMESPACE**): The namespace to which you uploaded the extension image, for example, **openshift** or your project namespace.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, "Completing deployment of the template for an immutable Process Server using S2I"](#).

### 3.2.11. Enabling Prometheus metric collection for an immutable Process Server using S2I

If you want to configure your Process Server deployment to use Prometheus to collect and store metrics, enable support for this feature in Process Server at deployment time.

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.2.1, “Starting configuration of the template for an immutable Process Server using S2I”](#).

#### Procedure

To enable support for Prometheus metric collection, set the **Prometheus Server Extension Disabled (PROMETHEUS\_SERVER\_EXT\_DISABLED)** parameter to **false**.

#### Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.2.12, “Completing deployment of the template for an immutable Process Server using S2I”](#).

For instructions about configuring Prometheus metrics collection, see [Managing and monitoring Process Server](#).

### 3.2.12. Completing deployment of the template for an immutable Process Server using S2I

After setting all the required parameters in the OpenShift Web UI or in the command line, complete deployment of the template.

#### Procedure

Depending on the method that you are using, complete the following steps:

- In the OpenShift Web UI, click **Create**.
  - If the **This will create resources that may have security or project behavior implications** message appears, click **Create Anyway**.
- Complete the command line and press Enter.

## 3.3. MODIFYING THE TEMPLATE FOR DEPLOYING AN IMMUTABLE PROCESS SERVER USING S2I

By default, the template for deploying an immutable server using S2I creates a separate PostgreSQL pod to provide the database server for each replicable Process Server. If you prefer to use MySQL or an external server (outside the OpenShift project), modify the **rhpan75-prod-immutable-kieserver.yaml** or **rhpan75-prod-immutable-kieserver-amq.yaml** template file before deploying the server.

An OpenShift template defines a set of objects that can be created by OpenShift. To change an environment configuration, you need to modify, add, or delete these objects. To simplify this task, comments are provided in the Red Hat Process Automation Manager templates.

Some comments mark blocks within the template, starting with **BEGIN** and ending with **END**. For example, the following block is named **Sample block**:

```
## Sample block BEGIN
sample line 1
sample line 2
sample line 3
## Sample block END
```

For some changes, you might need to replace a block in one template file with a block from another template file provided with Red Hat Process Automation Manager. In this case, delete the block, then paste the new block in its exact location.

## Procedure

- If you want to use MySQL instead of PostgreSQL, replace several blocks of the file, marked with comments from **BEGIN** to **END**, with blocks from the **rhpm75-kieserver-mysql.yaml** file:
  1. Replace the block named **PostgreSQL database parameters** with the block named **MySQL database parameters**. (Take this block and all subsequent replacement blocks from the **rhpm75-kieserver-postgresql.yaml** file.)
  2. Replace the block named **PostgreSQL service** with the block named **MySQL service**.
  3. Replace the block named **PostgreSQL driver settings** with the block named **MySQL driver settings**.
  4. Replace the block named **PostgreSQL deployment config** with the block named **MySQL deployment config**.
  5. Replace the block named **PostgreSQL persistent volume claim** with the block named **MySQL persistent volume claim**.
- If you want to use an external database server, replace several blocks of the file, marked with comments from **BEGIN** to **END**, with blocks from the **rhpm75-kieserver-externaldb.yaml** file, and also remove some blocks:
  1. Replace the block named **PostgreSQL database parameters** with the block named **External database parameters**. (Take this block and all subsequent replacement blocks from the **rhpm75-kieserver-externaldb.yaml** file.)
  2. Replace the block named **PostgreSQL driver settings** with the block named **External database driver settings**.
  3. Remove the following blocks of the file, marked with comments from **BEGIN** to **END**:
    - **PostgreSQL service**
    - **PostgreSQL deployment config**
    - **PostgreSQL persistent volume claim**



## IMPORTANT

The standard Process Server image includes drivers for MySQL and PostgreSQL external database servers. If you want to use another database server, you must build a custom Process Server image. For instructions, see [Section 2.5, “Building a custom Process Server extension image for an external database”](#).

## 3.4. DEPLOYING AN IMMUTABLE PROCESS SERVER FROM KJAR SERVICES

You can deploy an immutable Process Server using services that are already built as KJAR files.

You must provide the services in a Maven repository. You can use the built-in repository of the Business Central or your own repository (for example, a Nexus deployment). When the server pod starts, it retrieves the KJAR services from the Maven repository. Services on the pod are never updated or changed. At every restart or scaling of the pod, the server retrieves the files from the repository, so you must ensure they do not change on the Maven repository to keep the deployment immutable.

You cannot deploy or undeploy services on a running immutable Process Server. You can use Business Central or Business Central Monitoring to view monitoring information. The Process Server runs like any other pod on the OpenShift environment; you can use any container-based integration workflows as necessary.

By default, this server uses a PostgreSQL database server in a pod. To use a MySQL database server in a pod or an external database server, you can modify the template.

If a Business Central or Business Central Monitoring is deployed in the same namespace, it discovers the immutable Process Server automatically. You can use Business Central or Business Central Monitoring to start and stop (but not deploy) services on the immutable Process Server and to view monitoring data.

### 3.4.1. Starting configuration of the template for an immutable Process Server from KJAR services

To deploy an immutable Process Server from KJAR services, use one of the following template files:

- **rhpm75-kieserver-postgresql.yaml** to use a PostgreSQL pod for persistent storage. Use this template unless you have a specific reason to use another template.
- **rhpm75-kieserver-mysql.yaml** to use a MySQL pod for persistent storage.
- **rhpm75-kieserver-externaldb.yaml** to use an external database server for persistent storage.



## IMPORTANT

The standard Process Server image for an external database server includes drivers for MySQL and PostgreSQL external database servers. If you want to use another database server, you must build a custom Process Server image. For instructions, see [Section 2.5, “Building a custom Process Server extension image for an external database”](#).

### Procedure

1. Download the **rhpm-7.5.1-openshift-templates.zip** product deliverable file from the [Software Downloads](#) page of the Red Hat Customer Portal.



2. Extract the required template file.
3. Use one of the following methods to start deploying the template:
  - To use the OpenShift Web UI, in the OpenShift application console select **Add to Project** → **Import YAML / JSON** and then select or paste the **<template-file-name>.yaml** file. In the **Add Template** window, ensure **Process the template** is selected and click **Continue**.
  - To use the OpenShift command line console, prepare the following command line:

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

In this command line, make the following changes:

- Replace **<template-path>** with the path to the downloaded template file.
- Replace **<template-file-name>** with the name of the template file.
- Use as many **-p PARAMETER=value** pairs as needed to set the required parameters.

### Next steps

Set the parameters for the template. Follow the steps in [Section 3.4.2, “Setting required parameters for an immutable Process Server from KJAR services”](#) to set common parameters. You can view the template file to see descriptions for all parameters.

## 3.4.2. Setting required parameters for an immutable Process Server from KJAR services

When configuring the template to deploy an immutable Process Server from KJAR services, you must set the following parameters in all cases.

### Prerequisites

- You started the configuration of the template, as described in [Section 3.4.1, “Starting configuration of the template for an immutable Process Server from KJAR services”](#).

### Procedure

1. Set the following parameters:
  - **KIE Server Keystore Secret Name (KIE\_SERVER\_HTTPS\_SECRET)**: The name of the secret for Process Server, as created in [Section 2.2, “Creating the secrets for Process Server”](#).
  - **KIE Server Certificate Name (KIE\_SERVER\_HTTPS\_NAME)**: The name of the certificate in the keystore that you created in [Section 2.2, “Creating the secrets for Process Server”](#).
  - **KIE Server Keystore Password (KIE\_SERVER\_HTTPS\_PASSWORD)**: The password for the keystore that you created in [Section 2.2, “Creating the secrets for Process Server”](#).
  - **Application Name (APPLICATION\_NAME)**: The name of the OpenShift application. It is used in the default URLs for Business Central Monitoring and Process Server. OpenShift uses the application name to create a separate set of deployment configurations, services, routes, labels, and artifacts. You can deploy several applications using the same template

into the same project, as long as you use different application names. Also, the application name determines the name of the server configuration (server template) that the Process Server joins on Business Central or Business Central Monitoring. If you are deploying several Process Servers, you must ensure each of the servers has a different application name.

- **Maven repository URL (MAVEN\_REPO\_URL):** A URL for a Maven repository. You must upload all the processes (KJAR files) that are to be deployed on the Process Server into this repository.
- **Maven repository ID (MAVEN\_REPO\_ID):** An identifier for the Maven repository. The default value is **repo-custom**.
- **Maven repository username (MAVEN\_REPO\_USERNAME):** The username for the Maven repository.
- **Maven repository password (MAVEN\_REPO\_PASSWORD):** The password for the Maven repository.
- **KIE Server Container Deployment (KIE\_SERVER\_CONTAINER\_DEPLOYMENT):** The identifying information of the decision services (KJAR files) that the deployment must pull from the Maven repository. The format is **<containerId>=<groupId>:<artifactId>:<version>** or, if you want to specify an alias name for the container, **<containerId> (<aliasId>)=<groupId>:<artifactId>:<version>**. You can provide two or more KJAR files using the | separator, as illustrated in the following example:

```
containerId=groupId:artifactId:version|c2(alias2)=g2:a2:v2
```

- **KIE Server Mode (KIE\_SERVER\_MODE):** In the **rhpam75-kieserver-\*.yaml** templates the default value is **PRODUCTION**. In **PRODUCTION** mode, you cannot deploy **SNAPSHOT** versions of KJAR artifacts on the Process Server and cannot change versions of an artifact in an existing container. To deploy a new version with **PRODUCTION** mode, create a new container on the same Process Server. To deploy **SNAPSHOT** versions or to change versions of an artifact in an existing container, set this parameter to **DEVELOPMENT**.
  - **ImageStream Namespace (IMAGE\_STREAM\_NAMESPACE):** The namespace where the image streams are available. If the image streams were already available in your OpenShift environment (see [Section 2.1, "Ensuring the availability of image streams and the image registry"](#)), the namespace is **openshift**. If you have installed the image streams file, the namespace is the name of the OpenShift project.
2. You can set the following user name and password. By default, the deployment automatically generates the password.
- **KIE Server User (KIE\_SERVER\_USER) and KIE Server Password (KIE\_SERVER\_PWD):** The user name and password that a client application can use to connect to any of the Process Servers.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.4.10, "Completing deployment of the template for an immutable Process Server from KJAR services"](#).

### 3.4.3. Configuring the image stream namespace for an immutable Process Server from KJAR services

If you created image streams in a namespace that is not **openshift**, you must configure the namespace in the template.

If all image streams were already available in your Red Hat OpenShift Container Platform environment, you can skip this procedure.

### Prerequisites

- You started the configuration of the template, as described in [Section 3.4.1, “Starting configuration of the template for an immutable Process Server from KJAR services”](#).

### Procedure

If you installed an image streams file according to instructions in [Section 2.1, “Ensuring the availability of image streams and the image registry”](#), set the **ImageStream Namespace (IMAGE\_STREAM\_NAMESPACE)** parameter to the name of your OpenShift project.

### 3.4.4. Configuring information about a Business Central or Business Central Monitoring instance for an immutable Process Server from KJAR services

If you want to enable a connection from a Business Central or Business Central Monitoring instance in the same namespace to the Process Server, you must configure information about the Business Central or Business Central Monitoring instance.

### Prerequisites

- You started the configuration of the template, as described in [Section 3.4.1, “Starting configuration of the template for an immutable Process Server from KJAR services”](#).

### Procedure

1. Set the following parameters:
  - **KIE Admin User (KIE\_ADMIN\_USER)** and **KIE Admin Password (KIE\_ADMIN\_PWD)**: The user name and password for the administrative user. These values must be the same as the **KIE\_ADMIN\_USER** and **KIE\_ADMIN\_PWD** settings for the Business Central or Business Central Monitoring. If the Business Central or Business Central Monitoring uses RH-SSO or LDAP authentication, these values must be a user name and password configured in the authentication system with an administrator role for the Business Central or Business Central Monitoring.
  - **Name of the Business Central service (BUSINESS\_CENTRAL\_SERVICE)**: The OpenShift service name for the Business Central or Business Central Monitoring.
2. Ensure that the following settings are set to the same value as the same settings for the Business Central or Business Central Monitoring:
  - **Maven repository URL (MAVEN\_REPO\_URL)**: A URL for the external Maven repository from which services must be deployed.
  - **Maven repository username (MAVEN\_REPO\_USERNAME)**: The username for the Maven repository.
  - **Maven repository password (MAVEN\_REPO\_PASSWORD)**: The password for the Maven repository.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.4.10, “Completing deployment of the template for an immutable Process Server from KJAR services”](#).

### 3.4.5. Configuring access to a Maven mirror in an environment without a connection to the public Internet for an immutable Process Server from KJAR services

When configuring the template to deploy an immutable Process Server from KJAR services, if your OpenShift environment does not have a connection to the public Internet, you must configure access to a Maven mirror that you set up according to [Section 2.7, “Preparing a Maven mirror repository for offline use”](#).

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.4.1, “Starting configuration of the template for an immutable Process Server from KJAR services”](#).

#### Procedure

To configure access to the Maven mirror, set the following parameters:

- **Maven mirror URL (MAVEN\_MIRROR\_URL)**: The URL for the Maven mirror repository that you set up in [Section 2.7, “Preparing a Maven mirror repository for offline use”](#). This URL must be accessible from a pod in your OpenShift environment.
- **Maven mirror of (MAVEN\_MIRROR\_OF)**: The value that determines which artifacts are to be retrieved from the mirror. For instructions about setting the **mirrorOf** value, see [Mirror Settings](#) in the Apache Maven documentation. The default value is **external:\***. With this value, Maven retrieves every required artifact from the mirror and does not query any other repositories.
  - If you configure an external Maven repository (**MAVEN\_REPO\_URL**), change **MAVEN\_MIRROR\_OF** to exclude the artifacts in this repository from the mirror, for example, **external:\*,!repo-custom**. Replace **repo-custom** with the ID that you configured in **MAVEN\_REPO\_ID**.
  - If you configure a built-in Business Central Maven repository (**BUSINESS\_CENTRAL\_MAVEN\_SERVICE**), change **MAVEN\_MIRROR\_OF** to exclude the artifacts in this repository from the mirror: **external:\*,!repo-rhpamcentr**.
  - If you configure both repositories, change **MAVEN\_MIRROR\_OF** to exclude the artifacts in both repositories from the mirror: **external:\*,!repo-rhpamcentr,!repo-custom**. Replace **repo-custom** with the ID that you configured in **MAVEN\_REPO\_ID**.

## Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.4.10, “Completing deployment of the template for an immutable Process Server from KJAR services”](#).

### 3.4.6. Setting parameters for RH-SSO authentication for an immutable Process Server from KJAR services

If you want to use RH-SSO authentication, complete the following additional configuration when configuring the template to deploy an immutable Process Server from KJAR services.



## IMPORTANT

Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

### Prerequisites

- A realm for Red Hat Process Automation Manager is created in the RH-SSO authentication system.
- User names and passwords for Red Hat Process Automation Manager are created in the RH-SSO authentication system. For a list of the available roles, see [Chapter 4, Red Hat Process Automation Manager roles and users](#). In order to set the parameters for the environment, an administrative user with the **kie-server,rest-all,admin** roles is required. The default user name for this user is **adminUser**. This user can administer and use the environment.
- Clients are created in the RH-SSO authentication system for all components of the Red Hat Process Automation Manager environment that you are deploying. The client setup contains the URLs for the components. You can review and edit the URLs after deploying the environment. Alternatively, the Red Hat Process Automation Manager deployment can create the clients. However, this option provides less detailed control over the environment.
- You started the configuration of the template, as described in [Section 3.4.1, “Starting configuration of the template for an immutable Process Server from KJAR services”](#).

### Procedure

1. Set the **KIE\_ADMIN\_USER** and **KIE\_ADMIN\_PASSWORD** parameters of the template to the user name and password of the administrative user that you created in the RH-SSO authentication system.
2. Set the following parameters:
  - **RH-SSO URL (SSO\_URL)**: The URL for RH-SSO.
  - **RH-SSO Realm name (SSO\_REALM)**: The RH-SSO realm for Red Hat Process Automation Manager.
  - **RH-SSO Disable SSL Certificate Validation (SSO\_DISABLE\_SSL\_CERTIFICATE\_VALIDATION)**: Set to **true** if your RH-SSO installation does not use a valid HTTPS certificate.
3. Complete one of the following procedures:
  - a. If you created the client for Red Hat Process Automation Manager within RH-SSO, set the following parameters in the template:
    - **Business Central or Business Central Monitoring RH-SSO Client name (BUSINESS\_CENTRAL\_SSO\_CLIENT)**: The RH-SSO client name for Business Central or Business Central Monitoring.
    - **KIE Server RH-SSO Client name (KIE\_SERVER\_SSO\_CLIENT)**: The RH-SSO client name for Process Server.

- **KIE Server RH-SSO Client Secret**(**KIE\_SERVER\_SSO\_SECRET**): The secret string that is set in RH-SSO for the client for Process Server.
- b. To create the clients for Red Hat Process Automation Manager within RH-SSO, set the following parameters in the template:
- **KIE Server RH-SSO Client name**(**KIE\_SERVER\_SSO\_CLIENT**): The name of the client to create in RH-SSO for Process Server.
  - **KIE Server RH-SSO Client Secret**(**KIE\_SERVER\_SSO\_SECRET**): The secret string to set in RH-SSO for the client for Process Server.
  - **RH-SSO Realm Admin Username**(**SSO\_USERNAME**) and **RH-SSO Realm Admin Password** (**SSO\_PASSWORD**): The user name and password for the realm administrator user for the RH-SSO realm for Red Hat Process Automation Manager. You must provide this user name and password in order to create the required clients.

## Next steps

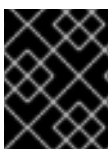
If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.4.10, “Completing deployment of the template for an immutable Process Server from KJAR services”](#).

After completing the deployment, review the URLs for components of Red Hat Process Automation Manager in the RH-SSO authentication system to ensure they are correct.

## 3.4.7. Setting parameters for LDAP authentication for an immutable Process Server from KJAR services

If you want to use LDAP authentication, complete the following additional configuration when configuring the template to deploy an immutable Process Server from KJAR services.



### IMPORTANT

Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

## Prerequisites

- You created user names and passwords for Red Hat Process Automation Manager in the LDAP system. For a list of the available roles, see [Chapter 4, Red Hat Process Automation Manager roles and users](#). As a minimum, in order to set the parameters for the environment, you created the following users:
  - An administrative user with the **kie-server,rest-all,admin** roles. This user can administer and use the environment.
  - A server user with the **kie-server,rest-all,user** roles. This user can make REST API calls to the Process Server.
- You started the configuration of the template, as described in [Section 3.4.1, “Starting configuration of the template for an immutable Process Server from KJAR services”](#).

## Procedure

1. In the LDAP service, create all user names in the deployment parameters. If you do not set any of the parameters, create users with the default user names. The created users must also be assigned to roles:
  - **KIE\_ADMIN\_USER**: default user name **adminUser**, roles: **kie-server,rest-all,admin**
  - **KIE\_SERVER\_USER**: default user name **executionUser**, roles **kie-server,rest-all,guest**  
For the user roles that you can configure in LDAP, see [Roles and users](#).
2. Set the **AUTH\_LDAP\*** parameters of the template. These parameters correspond to the settings of the **LdapExtended** Login module of Red Hat JBoss EAP. For instructions about using these settings, see [LdapExtended login module](#).  
If the LDAP server does not define all the roles required for your deployment, you can map LDAP groups to Red Hat Process Automation Manager roles. To enable LDAP role mapping, set the following parameters:
  - **RoleMapping rolesProperties file path** (**AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES**): The fully qualified path name of a file that defines role mapping, for example, **/opt/eap/standalone/configuration/rolemapping/rolemapping.properties**. You must provide this file and mount it at this path in all applicable deployment configurations; for instructions, see [Section 3.5, "\(Optional\) Providing the LDAP role mapping file"](#).
  - **RoleMapping replaceRole property** (**AUTH\_ROLE\_MAPPER\_REPLACE\_ROLE**): If set to **true**, mapped roles replace the roles defined on the LDAP server; if set to **false**, both mapped roles and roles defined on the LDAP server are set as user application roles. The default setting is **false**.

### Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.4.10, "Completing deployment of the template for an immutable Process Server from KJAR services"](#).

### 3.4.8. Setting parameters for using an external database server for an immutable Process Server from KJAR services

If you are using the **rhcam75-kieserver-externaldb.yaml** template to use an external database server for the Process Server, complete the following additional configuration when configuring the template to deploy an immutable Process Server from KJAR services.

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.4.1, "Starting configuration of the template for an immutable Process Server from KJAR services"](#).

#### Procedure

1. Set the following parameters:
  - **KIE Server External Database Driver**(**KIE\_SERVER\_EXTERNALDB\_DRIVER**): The driver for the server, depending on the server type:
    - **mysql**
    - **postgresql**

- **mariadb**
  - **mssql**
  - **db2**
  - **oracle**
  - **sybase**
  - **KIE Server External Database User**(**KIE\_SERVER\_EXTERNALDB\_USER**) and **KIE Server External Database Password** (**KIE\_SERVER\_EXTERNALDB\_PWD**): The user name and password for the external database server
  - **KIE Server External Database URL**(**KIE\_SERVER\_EXTERNALDB\_URL**): The JDBC URL for the external database server
  - **KIE Server External Database Dialect**(**KIE\_SERVER\_EXTERNALDB\_DIALECT**): The Hibernate dialect for the server, depending on the server type:
    - **org.hibernate.dialect.MySQL5InnoDBDialect** (used for MySQL and MariaDB)
    - **org.hibernate.dialect.PostgreSQL82Dialect**
    - **org.hibernate.dialect.SQLServer2012Dialect** (used for MS SQL)
    - **org.hibernate.dialect.DB2Dialect**
    - **org.hibernate.dialect.Oracle10gDialect**
    - **org.hibernate.dialect.SybaseASE157Dialect**
  - **KIE Server External Database Host**(**KIE\_SERVER\_EXTERNALDB\_SERVICE\_HOST**): The host name of the external database server
  - **KIE Server External Database Port**(**KIE\_SERVER\_EXTERNALDB\_SERVICE\_PORT**): The port number of the external database server
  - **KIE Server External Database name**(**KIE\_SERVER\_EXTERNALDB\_DB**): The database name to use on the external database server
  - **JDBC Connection Checker class** (**KIE\_SERVER\_EXTERNALDB\_CONNECTION\_CHECKER**): The name of the JDBC connection checker class for the database server. Without this information, a database server connection cannot be restored after it is lost, for example, if the database server is rebooted.
  - **JDBC Exception Sorter class** (**KIE\_SERVER\_EXTERNALDB\_EXCEPTION\_SORTER**): The name of the JDBC exception sorter class for the database server. Without this information, a database server connection cannot be restored after it is lost, for example, if the database server is rebooted.
2. If you created a custom image for using an external database server other than MySQL or PostgreSQL, as described in [Section 2.5, "Building a custom Process Server extension image for an external database"](#), set the following parameters:
- **Drivers Extension Image** (**EXTENSIONS\_IMAGE**): The ImageStreamTag definition of the extension image, for example, **jboss-kie-db2-extension-openshift-image:11.1.4.4**



- **Drivers ImageStream Namespace (`EXTENSIONS_IMAGE_NAMESPACE`)**: The namespace to which you uploaded the extension image, for example, **openshift** or your project namespace.

### Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.4.10, “Completing deployment of the template for an immutable Process Server from KJAR services”](#).

### 3.4.9. Enabling Prometheus metric collection for an immutable Process Server from KJAR services

If you want to configure your Process Server deployment to use Prometheus to collect and store metrics, enable support for this feature in Process Server at deployment time.

#### Prerequisites

- You started the configuration of the template, as described in [Section 3.4.1, “Starting configuration of the template for an immutable Process Server from KJAR services”](#).

#### Procedure

To enable support for Prometheus metric collection, set the **Prometheus Server Extension Disabled (`PROMETHEUS_SERVER_EXT_DISABLED`)** parameter to **false**.

### Next steps

If necessary, set additional parameters.

To complete the deployment, follow the procedure in [Section 3.4.10, “Completing deployment of the template for an immutable Process Server from KJAR services”](#).

For instructions about configuring Prometheus metrics collection, see [Managing and monitoring Process Server](#).

### 3.4.10. Completing deployment of the template for an immutable Process Server from KJAR services

After setting all the required parameters in the OpenShift Web UI or in the command line, complete deployment of the template.

#### Procedure

Depending on the method that you are using, complete the following steps:

- In the OpenShift Web UI, click **Create**.
  - If the **This will create resources that may have security or project behavior implications** message appears, click **Create Anyway**.
- Complete the command line and press Enter.

## 3.5. (OPTIONAL) PROVIDING THE LDAP ROLE MAPPING FILE

If you configure the **AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES** parameter, you must provide a file that defines the role mapping. Mount this file on all affected deployment configurations.

## Procedure

1. Create the role mapping properties file, for example, **my-role-map**. The file must contain entries in the following format:

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

For example:

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

2. Create an OpenShift configuration map from the file by entering the following command:

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

Replace **<new\_name>** with the name that the file is to have on the pods (it must be the same as the name specified in the **AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES** file) and **<existing\_name>** with the name of the file that you created. Example:

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

3. Mount the configuration map on every deployment configuration that is configured for role mapping.

The following deployment configurations can be affected in this environment:

- **myapp-rhpamcentrmon**: Business Central Monitoring
- **myapp-kieserver**: Process Server

Replace **myapp** with the application name. Sometimes, several Process Server deployments can be present under different application names.

For every deployment configuration, run the command:

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

Replace **<mapping\_dir>** with the directory name (without file name) set in the **AUTH\_ROLE\_MAPPER\_ROLES\_PROPERTIES** parameter, for example, **/opt/eap/standalone/configuration/rolemapping**.

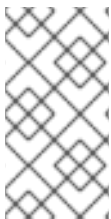
## CHAPTER 4. RED HAT PROCESS AUTOMATION MANAGER ROLES AND USERS

To access Business Central or Process Server, you must create users and assign them appropriate roles before the servers are started.

The Business Central and Process Server use Java Authentication and Authorization Service (JAAS) login module to authenticate the users. If both Business Central and Process Server are running on a single instance, then they share the same JAAS subject and security domain. Therefore, a user, who is authenticated for Business Central can also access Process Server.

However, if Business Central and Process Server are running on different instances, then the JAAS login module is triggered for both individually. Therefore, a user, who is authenticated for Business Central, needs to be authenticated separately to access the Process Server (for example, to view or manage process definitions in Business Central). In case, the user is not authenticated on the Process Server, then 401 error is logged in the log file, displaying **Invalid credentials to load data from remote server. Contact your system administrator.** message in Business Central.

This section describes available Red Hat Process Automation Manager user roles.



### NOTE

The **admin**, **analyst**, **developer**, **manager**, **process-admin**, **user**, and **rest-all** roles are reserved for Business Central. The **kie-server** role is reserved for Process Server. For this reason, the available roles can differ depending on whether Business Central, Process Server, or both are installed.

- **admin:** Users with the **admin** role are the Business Central administrators. They can manage users and create, clone, and manage the repositories. They have full access to make required changes in the application. Users with the **admin** role have access to all areas within Red Hat Process Automation Manager.
- **analyst:** Users with the **analyst** role have access to all high-level features. They can model and execute their projects. However, these users cannot add contributors to spaces or delete spaces in the **Design → Projects** view. Access to the **Deploy → Execution Servers** view, which is intended for administrators, is not available to users with the **analyst** role. However, the **Deploy** button is available to these users when they access the Library perspective.
- **developer:** Users with the **developer** role have access to almost all features and can manage rules, models, process flows, forms, and dashboards. They can manage the asset repository, they can create, build, and deploy projects, and they can use Red Hat CodeReady Studio to view processes. Only certain administrative functions such as creating and cloning a new repository are hidden from users with the **developer** role.
- **manager:** Users with the **manager** role can view reports. These users are usually interested in statistics about the business processes and their performance, business indicators, and other business-related reporting. A user with this role has access only to process and task reports.
- **process-admin:** Users with the **process-admin** role are business process administrators. They have full access to business processes, business tasks, and execution errors. These users can also view business reports and have access to the Task Inbox list.
- **user:** Users with the **user** role can work on the Task Inbox list, which contains business tasks that are part of currently running processes. Users with this role can view process and task reports and manage processes.

- **rest-all**: Users with the **rest-all** role can access Business Central REST capabilities.
- **kie-server**: Users with the **kie-server** role can access Process Server (KIE Server) REST capabilities. This role is mandatory for users to have access to **Manage** and **Track** views in Business Central.

## CHAPTER 5. OPENSIFT TEMPLATE REFERENCE INFORMATION

Red Hat Process Automation Manager provides the following OpenShift templates. To access the templates, download and extract the **rhcam-7.5.1-openshift-templates.zip** product deliverable file from the [Software Downloads](#) page of the Red Hat customer portal.

- **rhcam75-prod-immutable-monitor.yaml** provides a Business Central Monitoring instance and a Smart Router that you can use with immutable Process Servers. When you deploy this template, OpenShift displays the settings that you must then use for deploying the **rhcam75-prod-immutable-kieserver.yaml** template. For details about this template, see [Section 5.1, “rhcam75-prod-immutable-monitor.yaml template”](#).
- **rhcam75-prod-immutable-kieserver.yaml** provides an immutable Process Server. When you deploy this template, a source-to-image (S2I) build is triggered for one or several services that are to run on the Process Server. The Process Server can optionally be configured to connect to the Business Central Monitoring and Smart Router provided by **rhcam75-prod-immutable-monitor.yaml**. For details about this template, see [Section 5.2, “rhcam75-prod-immutable-kieserver.yaml template”](#).
- **rhcam75-prod-immutable-kieserver-amq.yaml** provides an immutable Process Server. When you deploy this template, a source-to-image (S2I) build is triggered for one or several services that are to run on the Process Server. The Process Server can optionally be configured to connect to the Business Central Monitoring and Smart Router provided by **rhcam75-prod-immutable-monitor.yaml**. This version of the template includes JMS integration. For details about this template, see [Section 5.3, “rhcam75-prod-immutable-kieserver-amq.yaml template”](#).
- **rhcam75-kieserver-externaldb.yaml** provides a Process Server that uses an external database. You can configure the Process Server to connect to a Business Central. Also, you can copy sections from this template into another template to configure a Process Server in the other template to use an external database. For details about this template, see [Section 5.4, “rhcam75-kieserver-externaldb.yaml template”](#).
- **rhcam75-kieserver-mysql.yaml** provides a Process Server and a MySQL instance that the Process Server uses. You can configure the Process Server to connect to a Business Central. Also, you can copy sections from this template into another template to configure a Process Server in the other template to use MySQL and to provide the MySQL instance. For details about this template, see [Section 5.5, “rhcam75-kieserver-mysql.yaml template”](#).
- **rhcam75-kieserver-postgresql.yaml** provides a Process Server and a PostgreSQL instance that the Process Server uses. You can configure the Process Server to connect to a Business Central. Also, you can copy sections from this template into another template to configure a Process Server in the other template to use PostgreSQL and to provide the PostgreSQL instance. For details about this template, see [Section 5.5, “rhcam75-kieserver-mysql.yaml template”](#).

### 5.1. RHPAM75-PROD-IMMUTABLE-MONITOR.YAML TEMPLATE

Application template for a router and monitoring console in a production environment, for Red Hat Process Automation Manager 7.5 - Deprecated

#### 5.1.1. Parameters

Templates allow you to define parameters which take on a value. That value is then substituted wherever the parameter is referenced. References can be defined in any text field in the objects list field. Refer to the [OpenShift documentation](#) for more information.

Variable name	Image Environment Variable	Description	Example value	Required
<b>APPLICATION_NAME</b>	–	The name for the application.	myapp	True
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository, if set. Default is generated randomly.	repo-custom	False
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<a href="http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/">http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/</a>	False
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	–	False
<b>BUSINESS_CENTRAL_SERVICE</b>	<b>RHPAMCENTRAL_MAVEN_REPO_SERVICE</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	myapp-rhpamcentr	False
<b>BUSINESS_CENTRAL_MAVEN_USERNAME</b>	<b>RHPAMCENTRAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>BUSINESS_CENTRAL_MAVEN_PASSWORD</b>	<b>RHPAMCENTRAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	maven!!	False
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE administrator username	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE administrator password	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE server username (Sets the org.kie.server.user system property)	executionUser	False
<b>KIE_SERVER_PASSWORD</b>	<b>KIE_SERVER_PASSWORD</b>	KIE server password, used to connect to KIE servers. If this parameter is not set, the password is automatically generated. (Sets the org.kie.server.pwd system property)	–	False
<b>KIE_SERVER_CONTROLLER_GLOBAL_DISCOVERY_ENABLED</b>	<b>KIE_SERVER_CONTROLLER_GLOBAL_DISCOVERY_ENABLED</b>	If set to true, turns on KIE server global discovery feature (Sets the org.kie.server.controller.openshift.global.discovery.enabled system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE</b>	<b>KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE</b>	If OpenShift integration of Business Central is turned on, setting this parameter to true enables connection to KIE Server via an OpenShift internal Service endpoint. (Sets the <code>org.kie.server.controller.openshift.prefer.kieserver.service</code> system property)	true	False
<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	KIE ServerTemplate Cache TTL in milliseconds (Sets the <code>org.kie.server.controller.template.cache.ttl</code> system property)	60000	False
<b>IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStreams for Red Hat Process Automation Manager images are installed. These ImageStreams are normally installed in the <code>openshift</code> namespace. You should only need to modify this if you installed the ImageStreams in a different namespace/project.	openshift	True



Variable name	Image Environment Variable	Description	Example value	Required
<b>IMAGE_STREAM_TAG</b>	–	A named pointer to an image in an image stream. Default is "7.5.0".	7.5.0	False
<b>SMART_ROUTER_HOSTNAME_HTTP</b>	–	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure- <application-name>-smartrouter- <project>.<default-domain-suffix>	–	False
<b>SMART_ROUTER_HOSTNAME_HTTPS</b>	–	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-smartrouter- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_ROUTER_ID</b>	<b>KIE_SERVER_ROUTER_ID</b>	Router ID used in API communication. (Router property org.kie.server.router.id)	kie-server-router	True
<b>KIE_SERVER_ROUTER_PROTOCOL</b>	<b>KIE_SERVER_ROUTER_PROTOCOL</b>	KIE server router protocol. (Used to build the org.kie.server.router.url.external property)	http	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_ROUTER_URL_EXTERNAL</b>	<b>KIE_SERVER_ROUTER_URL_EXTERNAL</b>	Public URL where the router can be found. Format <a href="#">http://&lt;host&gt;:&lt;port&gt;</a> (Router property <code>org.kie.server.router.url.external</code> )	–	False
<b>KIE_SERVER_ROUTER_NAME</b>	<b>KIE_SERVER_ROUTER_NAME</b>	Router name used in the Business Central user interface. (Router property <code>org.kie.server.router.name</code> )	KIE Server Router	True
<b>KIE_SERVER_ROUTER_HTTPS_SECRET</b>	–	The name of the secret containing the keystore file.	smartrouter-app-secret	True
<b>KIE_SERVER_ROUTER_HTTPS_KEYSTORE</b>	–	The name of the keystore file within the secret.	keystore.jks	False
<b>KIE_SERVER_ROUTER_HTTPS_NAME</b>	<b>KIE_SERVER_ROUTER_TLS_KEYSTORE_KEY_ALIAS</b>	The name associated with the server certificate.	jboss	False
<b>KIE_SERVER_ROUTER_HTTPS_PASSWORD</b>	<b>KIE_SERVER_ROUTER_TLS_KEYSTORE_PASSWORD</b>	The password for the keystore and certificate.	mykeystorepass	False
<b>KIE_SERVER_MONITOR_USER</b>	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE server monitor username. (Sets the <code>org.kie.server.controller.user.system</code> property)	monitorUser	False
<b>KIE_SERVER_MONITOR_PWD</b>	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE server monitor password. (Sets the <code>org.kie.server.controller.pwd.system</code> property)	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_MONITOR_TOKEN</b>	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	KIE server monitor token for bearer authentication. (Sets the org.kie.server.controller.token.system property)	–	False
<b>BUSINESS_CENTRAL_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure- <application-name>- rhpamcentrmon- <project>.<default-domain-suffix>	–	False
<b>BUSINESS_CENTRAL_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>- rhpamcentrmon- <project>.<default-domain-suffix>	–	False
<b>BUSINESS_CENTRAL_HTTPS_SECRET</b>	–	The name of the secret containing the keystore file.	businesscentral-app-secret	True
<b>BUSINESS_CENTRAL_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	keystore.jks	False
<b>BUSINESS_CENTRAL_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	The name associated with the server certificate.	jboss	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>BUSINESS_CENTRAL_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	mykeystorepass	False
<b>BUSINESS_CENTRAL_MEMORY_LIMIT</b>	–	Business Central Container memory limit.	2Gi	False
<b>SMART_ROUTER_MEMORY_LIMIT</b>	–	Smart Router Container memory limit.	512Mi	False
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL.	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO Realm name.	–	False
<b>BUSINESS_CENTRAL_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	Business Central Monitoring RH-SSO Client name.	–	False
<b>BUSINESS_CENTRAL_SSO_SECRET</b>	<b>SSO_SECRET</b>	Business Central Monitoring RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	–	False
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	Password	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	(uid={0})	False
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>SUBTREE_SCOPE</b>	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	10000	False
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	distinguishedName	False
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	true	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<code>memberOf</code>	False
<b>AUTH_LDAP_ROLE_CONTEXT_DN</b>	<b>AUTH_LDAP_ROLE_CONTEXT_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<code>ou=groups,ou=example,ou=com</code>	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	(memberOf={1})	False
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users.	user	False



Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	name	False
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttribute ID. If set to true, the DN is checked for the roleNameAttribute ID. If set to false, the DN is not checked for the roleNameAttribute ID. This flag can improve the performance of LDAP queries.	false	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	–	False
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	–	False

## 5.1.2. Objects

The CLI supports various object types. A list of these object types as well as their abbreviations can be found in the [Openshift documentation](#).

### 5.1.2.1. Services

A service is an abstraction which defines a logical set of pods and a policy by which to access them. Refer to the [container-engine documentation](#) for more information.

Service	Port	Name	Description
<b>\${APPLICATION_NAME}-rhpamcentrmon</b>	8080	http	All the Business Central Monitoring web server's ports.
	8443	https	
<b>\${APPLICATION_NAME}-rhpamcentrmon-ping</b>	8888	ping	The JGroups ping port for clustering.
<b>\${APPLICATION_NAME}-smartrouter</b>	9000	http	The smart router server http and https ports.
	9443	https	

### 5.1.2.2. Routes

A route is a way to expose a service by giving it an externally-reachable hostname such as **www.example.com**. A defined route and the endpoints identified by its service can be consumed by a router to provide named connectivity from external clients to your applications. Each route consists of a route name, service selector, and (optionally) security configuration. Refer to the [Openshift documentation](#) for more information.

Service	Security	Hostname
insecure- <b>\${APPLICATION_NAME}-rhpamcentrmon-http</b>	none	<b>\${BUSINESS_CENTRAL_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-rhpamcentrmon-https</b>	TLS passthrough	<b>\${BUSINESS_CENTRAL_HOSTNAME_HTTPS}</b>
insecure- <b>\${APPLICATION_NAME}-smartrouter-http</b>	none	<b>\${SMART_ROUTER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-smartrouter-https</b>	TLS passthrough	<b>\${SMART_ROUTER_HOSTNAME_HTTPS}</b>

### 5.1.2.3. Deployment Configurations

A deployment in OpenShift is a replication controller based on a user defined template called a deployment configuration. Deployments are created manually or in response to triggered events. Refer to the [OpenShift documentation](#) for more information.

### 5.1.2.3.1. Triggers

A trigger drives the creation of new deployments in response to events, both inside and outside OpenShift. Refer to the [OpenShift documentation](#) for more information.

Deployment	Triggers
<b><code>\${APPLICATION_NAME}-rhpamcentrmon</code></b>	ImageChange
<b><code>\${APPLICATION_NAME}-smartrouter</code></b>	ImageChange

### 5.1.2.3.2. Replicas

A replication controller ensures that a specified number of pod "replicas" are running at any one time. If there are too many, the replication controller kills some pods. If there are too few, it starts more. Refer to the [container-engine documentation](#) for more information.

Deployment	Replicas
<b><code>\${APPLICATION_NAME}-rhpamcentrmon</code></b>	1
<b><code>\${APPLICATION_NAME}-smartrouter</code></b>	2

### 5.1.2.3.3. Pod Template

#### 5.1.2.3.3.1. Service Accounts

Service accounts are API objects that exist within each project. They can be created or deleted like any other API object. Refer to the [OpenShift documentation](#) for more information.

Deployment	Service Account
<b><code>\${APPLICATION_NAME}-rhpamcentrmon</code></b>	<b><code>\${APPLICATION_NAME}-rhpamsvc</code></b>
<b><code>\${APPLICATION_NAME}-smartrouter</code></b>	<b><code>\${APPLICATION_NAME}-smartrouter</code></b>

#### 5.1.2.3.3.2. Image

Deployment	Image
<b><code>\${APPLICATION_NAME}-rhpamcentrmon</code></b>	<code>rhpam-businesscentral-monitoring-rhel8</code>
<b><code>\${APPLICATION_NAME}-smartrouter</code></b>	<code>rhpam-smartrouter-rhel8</code>

## 5.1.2.3.3.3. Readiness Probe

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

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

## 5.1.2.3.3.4. Liveness Probe

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

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

## 5.1.2.3.3.5. Exposed Ports

Deployments	Name	Port	Protocol
<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}-smartrouter</b>	http	9000	<b>TCP</b>

## 5.1.2.3.3.6. Image Environment Variables

Deployment	Variable name	Description	Example value
<b>\${APPLICATION_NAME}-rhpamcentrmon</b>	<b>APPLICATION_USE_RS_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_PWD</b>	KIE administrator password	<b>\${KIE_ADMIN_PWD}</b>
	<b>KIE_ADMIN_USER</b>	KIE administrator username	<b>\${KIE_ADMIN_USER}</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_PWD</b>	KIE server password, used to connect to KIE servers. If this parameter is not set, the password is automatically generated. (Sets the org.kie.server.pwd system property)	<b>`\${KIE_SERVER_PWD}`</b>
	<b>KIE_SERVER_USER</b>	KIE server username (Sets the org.kie.server.user system property)	<b>`\${KIE_SERVER_USER}`</b>
	<b>MAVEN_REPOS</b>	–	RHPAMCENTR,EXTERNAL
	<b>RHPAMCENTR_MAVEN_REPO_ID</b>	–	repo-rhpamcentr
	<b>RHPAMCENTR_MAVEN_REPO_SERVICE</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>`\${BUSINESS_CENTRAL_SERVICE}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>
	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_USERNAME}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_PASSWORD}`</b>
	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository, if set. Default is generated randomly.	<b>`\${MAVEN_REPO_ID}`</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<b>`\${MAVEN_REPO_URL}`</b>

Deployment	Variable name	Description	Example value
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	<b>`\${MAVEN_REPO_USERNAME}`</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	<b>`\${MAVEN_REPO_PASSWORD}`</b>
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED</b>	If set to true, turns on KIE server global discovery feature (Sets the <code>org.kie.server.controller.openshift.global.discovery.enabled</code> system property)	<b>`\${KIE_SERVER_CONTROLLER_OPENSIFT_GLOBAL_DISCOVERY_ENABLED}`</b>
	<b>KIE_SERVER_CONTROLLER_OPENSIFT_PREFER_KIESERVER_SERVICE</b>	If OpenShift integration of Business Central is turned on, setting this parameter to true enables connection to KIE Server via an OpenShift internal Service endpoint. (Sets the <code>org.kie.server.controller.openshift.prefer.kieserver.service</code> system property)	<b>`\${KIE_SERVER_CONTROLLER_OPENSIFT_PREFER_KIESERVER_SERVICE}`</b>
	<b>KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL</b>	KIE ServerTemplate Cache TTL in milliseconds (Sets the <code>org.kie.server.controller.template.cache.ttl</code> system property)	<b>`\${KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL}`</b>
	<b>KIE_WORKBENCH_CONTROLLER_OPENSIFT_ENABLED</b>	–	true
	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE server monitor username. (Sets the <code>org.kie.server.controller.user</code> system property)	<b>`\${KIE_SERVER_MONITOR_USER}`</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE server monitor password. (Sets the org.kie.server.controller.pwd system property)	<b>\${KIE_SERVER_MONITOR_PWD}</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	KIE server monitor token for bearer authentication. (Sets the org.kie.server.controller.token system property)	<b>\${KIE_SERVER_MONITOR_TOKEN}</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/businesscentral-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	<b>\${BUSINESS_CENTRAL_HTTPS_KEYSTORE}</b>
	<b>HTTPS_NAME</b>	The name associated with the server certificate.	<b>\${BUSINESS_CENTRAL_HTTPS_NAME}</b>
	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	<b>\${BUSINESS_CENTRAL_HTTPS_PASSWORD}</b>
	<b>JGROUPS_PING_PROTOCOL</b>	–	openshift.DNS_PING
	<b>OPENSIFT_DNS_PING_SERVICE_NAME</b>	–	<b>\${APPLICATION_NAME}-rhcamcentrmon-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 Realm name.	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	Business Central Monitoring RH-SSO Client Secret.	<b>\${BUSINESS_CENTRAL_SSO_SECRET}</b>



Deployment	Variable name	Description	Example value
	<b>SSO_CLIENT</b>	Business Central Monitoring RH-SSO Client name.	<b>`\${BUSINESS_CENTRAL_SSO_CLIENT}`</b>
	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	<b>`\${SSO_USERNAME}`</b>
	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	<b>`\${SSO_PASSWORD}`</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	<b>`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	<b>`\${SSO_PRINCIPAL_ATTRIBUTE}`</b>
	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-rhpamcentrmon-<project>.<default-domain-suffix>	<b>`\${BUSINESS_CENTRAL_HOSTNAME_HTTP}`</b>
	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-rhpamcentrmon-<project>.<default-domain-suffix>	<b>`\${BUSINESS_CENTRAL_HOSTNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	<b>`\${AUTH_LDAP_BIND_DN}`</b>
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	<b>`\${AUTH_LDAP_BIND_CREDENTIAL}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	<b><code>\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}</code></b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	<b><code>\${AUTH_LDAP_BASE_CTX_DN}</code></b>
	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a <code>{0}</code> expression is used. A common example for the search filter is <code>(uid={0})</code> .	<b><code>\${AUTH_LDAP_BASE_FILTER}</code></b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b><code>\${AUTH_LDAP_SEARCH_SCOPE}</code></b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	<b><code>\${AUTH_LDAP_SEARCH_TIME_LIMIT}</code></b>
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	<b><code>\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}</code></b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	<b><code>\${AUTH_LDAP_PARSE_USERNAME}</code></b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_BEGIN_STRING}</code></b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_END_STRING}</code></b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<b><code>\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}</code></b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<b>`\${AUTH_LDAP_ROLE_S_CTX_DN}`</b>
	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users.	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	<b>`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeID attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	<b><code>\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}</code></b>
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	<b><code>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</code></b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	<b><code>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</code></b>
<b><code>\${APPLICATION_NAME}</code>-smartrouter</b>	<b>KIE_SERVER_ROUTER_HOST</b>	–	–
	<b>KIE_SERVER_ROUTER_PORT</b>	–	9000
	<b>KIE_SERVER_ROUTER_PORT_TLS</b>	–	9443

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_ROUTER_URL_EXTERNAL</b>	Public URL where the router can be found. Format <a href="http://&lt;host&gt;:&lt;port&gt;">http://&lt;host&gt;:&lt;port&gt;</a> (Router property <code>org.kie.server.router.url.external</code> )	<b><code>\${KIE_SERVER_ROUTER_URL_EXTERNAL}</code></b>
	<b>KIE_SERVER_ROUTER_ID</b>	Router ID used in API communication. (Router property <code>org.kie.server.router.id</code> )	<b><code>\${KIE_SERVER_ROUTER_ID}</code></b>
	<b>KIE_SERVER_ROUTER_NAME</b>	Router name used in the Business Central user interface. (Router property <code>org.kie.server.router.name</code> )	<b><code>\${KIE_SERVER_ROUTER_NAME}</code></b>
	<b>KIE_SERVER_ROUTER_ROUTE_NAME</b>	–	<b><code>\${APPLICATION_NAME}-smartrouter</code></b>
	<b>KIE_SERVER_ROUTER_SERVICE</b>	–	<b><code>\${APPLICATION_NAME}-smartrouter</code></b>
	<b>KIE_SERVER_ROUTER_PROTOCOL</b>	KIE server router protocol. (Used to build the <code>org.kie.server.router.url.external</code> property)	<b><code>\${KIE_SERVER_ROUTER_PROTOCOL}</code></b>
	<b>KIE_SERVER_ROUTER_TLS_KEYSTORE_KEYALIAS</b>	The name associated with the server certificate.	<b><code>\${KIE_SERVER_ROUTER_HTTPS_NAME}</code></b>
	<b>KIE_SERVER_ROUTER_TLS_KEYSTORE_PASSWORD</b>	The password for the keystore and certificate.	<b><code>\${KIE_SERVER_ROUTER_HTTPS_PASSWORD}</code></b>
	<b>KIE_SERVER_ROUTER_TLS_KEYSTORE</b>	–	<b><code>/etc/smartrouter-secret-volume/\${KIE_SERVER_ROUTER_HTTPS_KEYSTORE}</code></b>
	<b>KIE_SERVER_CONTROLLER_USER</b>	KIE server monitor username. (Sets the <code>org.kie.server.controller.user</code> system property)	<b><code>\${KIE_SERVER_MONITOR_USER}</code></b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_CONTROLLER_PWD</b>	KIE server monitor password. (Sets the org.kie.server.controller.pwd system property)	<b>\${KIE_SERVER_MONITOR_PWD}</b>
	<b>KIE_SERVER_CONTROLLER_TOKEN</b>	KIE server monitor token for bearer authentication. (Sets the org.kie.server.controller.token system property)	<b>\${KIE_SERVER_MONITOR_TOKEN}</b>
	<b>KIE_SERVER_CONTROLLER_SERVICE</b>	–	<b>\${APPLICATION_NAME}-rhpamcentrmon</b>
	<b>KIE_SERVER_CONTROLLER_PROTOCOL</b>	–	http
	<b>KIE_SERVER_ROUTER_REPO</b>	–	<b>/opt/rhpam-smartrouter/data</b>
	<b>KIE_SERVER_ROUTER_CONFIG_WATCHER_ENABLED</b>	–	true

#### 5.1.2.3.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
<b>\${APPLICATION_NAME}-rhpamcentrmon</b>	businesscentral-keystore-volume	<b>/etc/businesscentral-secret-volume</b>	ssl certs	True
<b>\${APPLICATION_NAME}-smartrouter</b>	<b>\${APPLICATION_NAME}-smartrouter</b>	<b>/opt/rhpam-smartrouter/data</b>	–	false

#### 5.1.2.4. External Dependencies

##### 5.1.2.4.1. Volume Claims

A **PersistentVolume** object is a storage resource in an OpenShift cluster. Storage is provisioned by an administrator by creating **PersistentVolume** objects from sources such as GCE Persistent Disks, AWS Elastic Block Stores (EBS), and NFS mounts. Refer to the [OpenShift documentation](#) for more information.



Name	Access Mode
<b>\${APPLICATION_NAME}-smartrouter-claim</b>	ReadWriteMany
<b>\${APPLICATION_NAME}-rhpamcentr-claim</b>	ReadWriteMany

#### 5.1.2.4.2. Secrets

This template requires the following secrets to be installed for the application to run.

smartrouter-app-secret businesscentral-app-secret

## 5.2. RHPAM75-PROD-IMMUTABLE-KIESERVER.YAML TEMPLATE

Application template for an immutable KIE server in a production environment, for Red Hat Process Automation Manager 7.5 - Deprecated

### 5.2.1. Parameters

Templates allow you to define parameters which take on a value. That value is then substituted wherever the parameter is referenced. References can be defined in any text field in the objects list field. Refer to the [Openshift documentation](#) for more information.

Variable name	Image Environment Variable	Description	Example value	Required
<b>APPLICATION_NAME</b>	–	The name for the application.	myapp	True
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE administrator username.	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE administrator password.	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_PWD</b>	<b>KIE_SERVER_PWD</b>	KIE server password, used to connect to KIE servers. If this parameter is not set, the password is automatically generated. (Sets the <code>org.kie.server.pwd</code> system property)	–	False
<b>IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStreams for Red Hat Process Automation Manager images are installed. These ImageStreams are normally installed in the <code>openshift</code> namespace. You should only need to modify this if you installed the ImageStreams in a different namespace/project.	<code>openshift</code>	True
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	The name of the image stream to use for KIE server. Default is <code>"rhpam-kieserver-rhel8"</code> .	<code>rhpam-kieserver-rhel8</code>	True
<b>IMAGE_STREAM_TAG</b>	–	A named pointer to an image in an image stream. Default is <code>"7.5.0"</code> .	<code>7.5.0</code>	True

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_PERSISTENCE_DS</b>	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	java:/jboss/datasources/rhpam	False
<b>POSTGRESQL_IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStream for the PostgreSQL image is installed. The ImageStream is already installed in the openshift namespace. You should only need to modify this if you installed the ImageStream in a different namespace/project. Default is "openshift".	openshift	False
<b>POSTGRESQL_IMAGE_STREAM_TAG</b>	–	The PostgreSQL image version, which is intended to correspond to the PostgreSQL version. Default is "10".	10	False
<b>KIE_SERVER_POSTGRESQL_USER</b>	<b>RHPAM_USERNAME</b>	KIE server PostgreSQL database username.	rhpam	False
<b>KIE_SERVER_POSTGRESQL_PASSWORD</b>	<b>RHPAM_PASSWORD</b>	KIE server PostgreSQL database password.	–	False
<b>KIE_SERVER_POSTGRESQL_DATABASE</b>	<b>RHPAM_DATABASE</b>	KIE server PostgreSQL database name.	rhpam7	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	Allows the PostgreSQL to handle XA transactions.	100	True
<b>DB_VOLUME_CAPACITY</b>	–	Size of persistent storage for the database volume.	1Gi	True
<b>KIE_SERVER_POSTGRESQL_DIALECT</b>	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server PostgreSQL Hibernate dialect.	org.hibernate.dialect.PostgreSQLDialect	True
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	true	False
<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	false	False
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	The name of the secret containing the keystore file.	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	The name associated with the server certificate.	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	mykeystorepass	False
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	false	False
<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	rhpam-kieserver-library=org.openshift.quickstarts:rhpam-kieserver-library:1.5.0-SNAPSHOT	True

Variable name	Image Environment Variable	Description	Example value	Required
<b>SOURCE_REPO_SITORY_URL</b>	–	Git source URI for application.	<a href="https://github.com/jboss-container-images/rhpam-7-openshift-image.git">https://github.com/jboss-container-images/rhpam-7-openshift-image.git</a>	True
<b>SOURCE_REPO_SITORY_REF</b>	–	Git branch/tag reference.	7.5.x	False
<b>CONTEXT_DIR</b>	–	Path within Git project to build; empty for root project directory.	quickstarts/library-process/library	False
<b>GITHUB_WEBHOOK_SECRET</b>	–	GitHub trigger secret.	–	True
<b>GENERIC_WEBHOOK_SECRET</b>	–	Generic build trigger secret.	–	True
<b>MAVEN_MIRROR_URL</b>	<b>MAVEN_MIRROR_URL</b>	Maven mirror to use for S2I builds. If enabled, the mirror must contain all the artifacts necessary for building and running the required services.	–	False
<b>MAVEN_MIRROR_OF</b>	<b>MAVEN_MIRROR_OF</b>	Maven mirror configuration for KIE server.	external:*	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	repo-custom	False
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository.	–	False
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	–	False
<b>BUSINESS_CENTRAL_SERVICE</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	myapp-rhpamcentr	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>BUSINESS_CENTRAL_MAVEN_USERNAME</b>	<b>RHPAMCENTRAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
<b>BUSINESS_CENTRAL_MAVEN_PASSWORD</b>	<b>RHPAMCENTRAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	maven!!	False
<b>ARTIFACT_DIR</b>	–	List of directories from which archives will be copied into the deployment folder. If unspecified, all archives in /target will be copied.	–	False
<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer service database-data-store.	30000	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	KIE server Container memory limit.	1Gi	False
<b>KIE_SERVER_MGMT_DISABLED</b>	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped. (Sets the property org.kie.server.management.api.disabled to true)	true	True
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL.	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False



Variable name	Image Environment Variable	Description	Example value	Required
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO Realm name.	–	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	–	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	–	False
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	Password	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	(uid={0})	False
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>SUBTREE_SCOPE</b>	False
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	10000	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	distinguishedName	False
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	true	False
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<code>memberOf</code>	False
<b>AUTH_LDAP_ROLE_CTX_DN</b>	<b>AUTH_LDAP_ROLE_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<code>ou=groups,ou=example,ou=com</code>	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	(memberOf={1})	False
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users	user	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	name	False
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttribute ID. If set to true, the DN is checked for the roleNameAttribute ID. If set to false, the DN is not checked for the roleNameAttribute ID. This flag can improve the performance of LDAP queries.	false	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	–	False
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	–	False

## 5.2.2. Objects

The CLI supports various object types. A list of these object types as well as their abbreviations can be found in the [OpenShift documentation](#).

### 5.2.2.1. Services

A service is an abstraction which defines a logical set of pods and a policy by which to access them. Refer to the [container-engine documentation](#) for more information.

Service	Port	Name	Description
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	All the KIE server web server's ports.
	8443	https	
<b>\${APPLICATION_NAME}-kieserver-ping</b>	8888	ping	The JGroups ping port for clustering.
<b>\${APPLICATION_NAME}-postgresql</b>	5432	–	The database server's port.

### 5.2.2.2. Routes

A route is a way to expose a service by giving it an externally-reachable hostname such as **www.example.com**. A defined route and the endpoints identified by its service can be consumed by a router to provide named connectivity from external clients to your applications. Each route consists of a route name, service selector, and (optionally) security configuration. Refer to the [OpenShift documentation](#) for more information.

Service	Security	Hostname
insecure- <b>\${APPLICATION_NAME}-kieserver-http</b>	none	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS passthrough	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

### 5.2.2.3. Build Configurations

A **buildConfig** describes a single build definition and a set of triggers for when a new build should be created. A **buildConfig** is a REST object, which can be used in a POST to the API server to create a new instance. Refer to the [OpenShift documentation](#) for more information.



S2I image	link	Build output	BuildTriggers and Settings
rhpm-kieserver-rhel8:7.5.0	<a href="#">rhpm-7/rhpm-kieserver-rhel8</a>	<b><code>\${APPLICATION_NAME}-kieserver:latest</code></b>	GitHub, Generic, ImageChange, ConfigChange

#### 5.2.2.4. Deployment Configurations

A deployment in OpenShift is a replication controller based on a user defined template called a deployment configuration. Deployments are created manually or in response to triggered events. Refer to the [OpenShift documentation](#) for more information.

##### 5.2.2.4.1. Triggers

A trigger drives the creation of new deployments in response to events, both inside and outside OpenShift. Refer to the [OpenShift documentation](#) for more information.

Deployment	Triggers
<b><code>\${APPLICATION_NAME}-kieserver</code></b>	ImageChange
<b><code>\${APPLICATION_NAME}-postgresql</code></b>	ImageChange

##### 5.2.2.4.2. Replicas

A replication controller ensures that a specified number of pod "replicas" are running at any one time. If there are too many, the replication controller kills some pods. If there are too few, it starts more. Refer to the [container-engine documentation](#) for more information.

Deployment	Replicas
<b><code>\${APPLICATION_NAME}-kieserver</code></b>	2
<b><code>\${APPLICATION_NAME}-postgresql</code></b>	1

##### 5.2.2.4.3. Pod Template

###### 5.2.2.4.3.1. Service Accounts

Service accounts are API objects that exist within each project. They can be created or deleted like any other API object. Refer to the [OpenShift documentation](#) for more information.

Deployment	Service Account
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>

#### 5.2.2.4.3.2. Image

Deployment	Image
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>
<code>\${APPLICATION_NAME}-postgresql</code>	postgresql

#### 5.2.2.4.3.3. Readiness Probe

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

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

##### `${APPLICATION_NAME}-postgresql`

`/usr/libexec/check-container`

#### 5.2.2.4.3.4. Liveness Probe

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

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

##### `${APPLICATION_NAME}-postgresql`

`/usr/libexec/check-container --live`

#### 5.2.2.4.3.5. Exposed Ports

Deployments	Name	Port	Protocol
<code>\${APPLICATION_NAME}-kieserver</code>	jolokia	8778	TCP
	http	8080	TCP
	https	8443	TCP
	ping	8888	TCP

Deployments	Name	Port	Protocol
<b>\${APPLICATION_NAME}-postgresql</b>	–	5432	<b>TCP</b>

#### 5.2.2.4.3.6. Image Environment Variables

Deployment	Variable name	Description	Example value
<b>\${APPLICATION_NAME}-kieserver</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>KIE_ADMIN_USER</b>	KIE administrator username.	<b>\${KIE_ADMIN_USER}</b>
	<b>KIE_ADMIN_PWD</b>	KIE administrator password.	<b>\${KIE_ADMIN_PWD}</b>
	<b>KIE_SERVER_MODE</b>	–	<b>DEVELOPMENT</b>
	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	<b>\${KIE_MBEANS}</b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	<b>\${DROOLS_SERVER_FILTER_CLASSES}</b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	<b>\${PROMETHEUS_SERVER_EXT_DISABLED}</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	<b>`\${KIE_SERVER_BYPASS_AUTH_USER}`</b>
	<b>KIE_SERVER_ID</b>	–	–
	<b>KIE_SERVER_ROUTE_NAME</b>	–	insecure- `\${APPLICATION_NAME}`-kieserver
	<b>KIE_SERVER_ROUTE_SERVICE</b>	–	<b>`\${APPLICATION_NAME}`-smartrouter</b>
	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	<b>`\${KIE_SERVER_USER}`</b>
	<b>KIE_SERVER_PWD</b>	KIE server password, used to connect to KIE servers. If this parameter is not set, the password is automatically generated. (Sets the org.kie.server.pwd system property)	<b>`\${KIE_SERVER_PWD}`</b>
	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	<b>`\${KIE_SERVER_CONTAINER_DEPLOYMENT}`</b>
	<b>MAVEN_MIRROR_URL</b>	Maven mirror to use for S2I builds. If enabled, the mirror must contain all the artifacts necessary for building and running the required services.	<b>`\${MAVEN_MIRROR_URL}`</b>

Deployment	Variable name	Description	Example value
	<b>MAVEN_MIRROR_OF</b>	Maven mirror configuration for KIE server.	<b>`\${MAVEN_MIRROR_OF}`</b>
	<b>MAVEN_REPOS</b>	–	RHPAMCENTR,EXTERNAL
	<b>RHPAMCENTR_MAVEN_REPO_ID</b>	–	repo-rhpamcentr
	<b>RHPAMCENTR_MAVEN_REPO_SERVICE</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>`\${BUSINESS_CENTRAL_SERVICE}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>
	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_USERNAME}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_PASSWORD}`</b>

Deployment	Variable name	Description	Example value
	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	<b>`\${MAVEN_REPO_ID}`</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository.	<b>`\${MAVEN_REPO_URL}`</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	<b>`\${MAVEN_REPO_USERNAME}`</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	<b>`\${MAVEN_REPO_PASSWORD}`</b>
	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	<b>`\${KIE_SERVER_PERSISTENCE_DS}`</b>
	<b>DATASOURCES</b>	–	<b>RHPAM</b>
	<b>RHPAM_DATABASE</b>	KIE server PostgreSQL database name.	<b>`\${KIE_SERVER_POSTGRES_DB}`</b>
	<b>RHPAM_JNDI</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	<b>`\${KIE_SERVER_PERSISTENCE_DS}`</b>
	<b>RHPAM_JTA</b>	–	true
	<b>RHPAM_DRIVER</b>	–	postgresql

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server PostgreSQL Hibernate dialect.	<b>`\${KIE_SERVER_POSTGRESQL_DIALECT}`</b>
	<b>RHPAM_USERNAME</b>	KIE server PostgreSQL database username.	<b>`\${KIE_SERVER_POSTGRESQL_USER}`</b>
	<b>RHPAM_PASSWORD</b>	KIE server PostgreSQL database password.	<b>`\${KIE_SERVER_POSTGRESQL_PWD}`</b>
	<b>RHPAM_SERVICE_HOST</b>	–	<b>`\${APPLICATION_NAME}-postgresql`</b>
	<b>RHPAM_SERVICE_PORT</b>	–	5432
	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer service database-data-store.	<b>`\${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}`</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/kieserver-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	<b>`\${KIE_SERVER_HTTPS_KEYSTORE}`</b>
	<b>HTTPS_NAME</b>	The name associated with the server certificate.	<b>`\${KIE_SERVER_HTTPS_NAME}`</b>
	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	<b>`\${KIE_SERVER_HTTPS_PASSWORD}`</b>
	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped. (Sets the property org.kie.server.mgmt.api.disabled to true)	<b>`\${KIE_SERVER_MGMT_DISABLED}`</b>
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	–	OpenShiftStartupStrategy
	<b>JGROUPS_PING_PROTOCOL</b>	–	openshift.DNS_PING

Deployment	Variable name	Description	Example value
	<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 Realm name.	<b>`\${SSO_REALM}`</b>
	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	<b>`\${KIE_SERVER_SSO_SECRET}`</b>
	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	<b>`\${KIE_SERVER_SSO_CLIENT}`</b>
	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	<b>`\${SSO_USERNAME}`</b>
	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	<b>`\${SSO_PASSWORD}`</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	<b>`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	<b>`\${SSO_PRINCIPAL_ATTRIBUTE}`</b>
	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	<b>`\${KIE_SERVER_HOSTNAME_HTTP}`</b>



Deployment	Variable name	Description	Example value
	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	<b>`\${KIE_SERVER_HOSTNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	<b>`\${AUTH_LDAP_BIND_DN}`</b>
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	<b>`\${AUTH_LDAP_BIND_CREDENTIAL}`</b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	<b>`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`</b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	<b>`\${AUTH_LDAP_BASE_CTX_DN}`</b>
	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	<b>`\${AUTH_LDAP_BASE_FILTER}`</b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>`\${AUTH_LDAP_SEARCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	<b>`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	<b><code>\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}</code></b>
	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	<b><code>\${AUTH_LDAP_PARSE_USERNAME}</code></b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_BEGIN_STRING}</code></b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_END_STRING}</code></b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<b><code>\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}</code></b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<b>`\${AUTH_LDAP_ROLE_S_CTX_DN}`</b>
	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	<b>`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeID attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	<b>\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}</b>
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	<b>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	<b>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</b>
<b>\${APPLICATION_NAME}-postgresql</b>	<b>POSTGRESQL_USER</b>	KIE server PostgreSQL database username.	<b>\${KIE_SERVER_POSTGRESQL_USER}</b>
	<b>POSTGRESQL_PASSWORD</b>	KIE server PostgreSQL database password.	<b>\${KIE_SERVER_POSTGRESQL_PWD}</b>
	<b>POSTGRESQL_DATABASE</b>	KIE server PostgreSQL database name.	<b>\${KIE_SERVER_POSTGRESQL_DB}</b>

Deployment	Variable name	Description	Example value
	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	Allows the PostgreSQL to handle XA transactions.	<b>\${POSTGRESQL_MAX_PREPARED_TRANSACTIONS}</b>

#### 5.2.2.4.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
<b>\${APPLICATION_NAME}-kieserver</b>	kieserver-keystore-volume	<b>/etc/kieserver-secret-volume</b>	ssl certs	True
<b>\${APPLICATION_NAME}-postgresql</b>	<b>\${APPLICATION_NAME}-postgresql-pvol</b>	<b>/var/lib/pgsql/data</b>	postgresql	false

#### 5.2.2.5. External Dependencies

##### 5.2.2.5.1. Volume Claims

A **PersistentVolume** object is a storage resource in an OpenShift cluster. Storage is provisioned by an administrator by creating **PersistentVolume** objects from sources such as GCE Persistent Disks, AWS Elastic Block Stores (EBS), and NFS mounts. Refer to the [OpenShift documentation](#) for more information.

Name	Access Mode
<b>\${APPLICATION_NAME}-postgresql-claim</b>	ReadWriteOnce

##### 5.2.2.5.2. Secrets

This template requires the following secrets to be installed for the application to run.

kieserver-app-secret

## 5.3. RHPAM75-PROD-IMMUTABLE-KIESERVER-AMQ.YAML TEMPLATE

Application template for an immutable KIE server in a production environment integrated with ActiveMQ, for Red Hat Process Automation Manager 7.5 - Deprecated

### 5.3.1. Parameters

Templates allow you to define parameters which take on a value. That value is then substituted wherever the parameter is referenced. References can be defined in any text field in the objects list field. Refer to the [OpenShift documentation](#) for more information.

Variable name	Image Environment Variable	Description	Example value	Required
<b>APPLICATION_NAME</b>	–	The name for the application.	myapp	True
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE administrator username.	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE administrator password.	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE server username (Sets the org.kie.server.user system property)	executionUser	False
<b>KIE_SERVER_PASSWORD</b>	<b>KIE_SERVER_PASSWORD</b>	KIE server password. If this parameter is not set, the password is automatically generated. (Sets the org.kie.server.pwd system property)	–	False
<b>IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStreams for Red Hat Process Automation Manager images are installed. These ImageStreams are normally installed in the openshift namespace. You should only need to modify this if you installed the ImageStreams in a different namespace/project.	openshift	True

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	The name of the image stream to use for KIE server. Default is "rhpam-kieserver-rhel8".	rhpam-kieserver-rhel8	True
<b>IMAGE_STREAM_TAG</b>	–	A named pointer to an image in an image stream. Default is "7.5.0".	7.5.0	True
<b>KIE_SERVER_PERSISTENCE_DS</b>	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource (Sets the org.kie.server.persistence.ds system property)	java:/jboss/datasources/rhpam	False
<b>POSTGRESQL_IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStream for the PostgreSQL image is installed. The ImageStream is already installed in the openshift namespace. You should only need to modify this if you installed the ImageStream in a different namespace/project. Default is "openshift".	openshift	False
<b>POSTGRESQL_IMAGE_STREAM_TAG</b>	–	The PostgreSQL image version, which is intended to correspond to the PostgreSQL version. Default is "10".	10	False
<b>KIE_SERVER_POSTGRESQL_USERNAME</b>	<b>RHPAM_USERNAME</b>	KIE server PostgreSQL database username	rhpam	False



Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_POSTGRESQL_PASSWORD</b>	<b>RHPAM_PASSWORD</b>	KIE server PostgreSQL database password	–	False
<b>KIE_SERVER_POSTGRESQL_DATABASE</b>	<b>RHPAM_DATABASE</b>	KIE server PostgreSQL database name	rhpm7	False
<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	Allows the PostgreSQL to handle XA transactions.	100	True
<b>DB_VOLUME_CAPACITY</b>	–	Size of persistent storage for the database volume.	1Gi	True
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbeans system properties)	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering (Sets the org.drools.server.filter.classes system property)	true	False
<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	The name of the secret containing the keystore file	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	The name associated with the server certificate	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate	mykeystorepass	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the <code>org.kie.server.bypass.auth.user</code> system property)	false	False
<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: <code>containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2</code>	<code>rhpm-kieserver-library=org.openshift.quickstarts:rhpm-kieserver-library:1.5.0-SNAPSHOT</code>	True
<b>SOURCE_REPOSITORY_URL</b>	–	Git source URI for application	<a href="https://github.com/jboss-container-images/rhpm-7-openshift-image.git">https://github.com/jboss-container-images/rhpm-7-openshift-image.git</a>	True
<b>SOURCE_REPOSITORY_REF</b>	–	Git branch/tag reference	7.5.x	False
<b>CONTEXT_DIR</b>	–	Path within Git project to build; empty for root project directory.	<code>quickstarts/library-process/library</code>	False
<b>GITHUB_WEBHOOK_SECRET</b>	–	GitHub trigger secret	–	True
<b>GENERIC_WEBHOOK_SECRET</b>	–	Generic build trigger secret	–	True
<b>MAVEN_MIRROR_URL</b>	–	Maven mirror to use for S2I builds	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository, if set. Default is generated randomly.	my-repo-id	False
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository.	–	False
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	–	False
<b>BUSINESS_CENTRAL_SERVICE</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	myapp-rhpamcentr	False
<b>BUSINESS_CENTRAL_MAVEN_USERNAME</b>	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
<b>BUSINESS_CENTRAL_MAVEN_PASSWORD</b>	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	maven!!	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>ARTIFACT_DIR</b>	–	List of directories from which archives will be copied into the deployment folder. If unspecified, all archives in /target will be copied.	–	False
<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer service database-data-store.	30000	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	KIE server Container memory limit	1Gi	False
<b>KIE_SERVER_MGMT_DISABLED</b>	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped. (Sets the property org.kie.server.management.api.disabled to true)	true	True
<b>KIE_SERVER_EXECUTOR_JMS</b>	<b>KIE_SERVER_EXECUTOR_JMS</b>	Enables the JMS executor, set false to disable it.	true	False
<b>KIE_SERVER_EXECUTOR_JMS_TRANSACTED</b>	<b>KIE_SERVER_EXECUTOR_JMS_TRANSACTED</b>	Enable transactions for JMS executor, disabled by default	false	False
<b>KIE_SERVER_JMS_QUEUE_REQUEST</b>	<b>KIE_SERVER_JMS_QUEUE_REQUEST</b>	JNDI name of request queue for JMS. The default value is queue/KIE.SERVER.REQUEST	queue/KIE.SERVER.REQUEST	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_JMS_QUEUE_RESPONSE</b>	<b>KIE_SERVER_JMS_QUEUE_RESPONSE</b>	JNDI name of response queue for JMS. The default value is queue/KIE.SERVER.RESPONSE	queue/KIE.SERVER.RESPONSE	False
<b>KIE_SERVER_JMS_QUEUE_EXECUTOR</b>	<b>KIE_SERVER_JMS_QUEUE_EXECUTOR</b>	JNDI name of response queue for JMS. The default value is queue/KIE.SERVER.RESPONSE	queue/KIE.SERVER.EXECUTOR	False
<b>KIE_SERVER_JMS_ENABLE_SIGNAL</b>	<b>KIE_SERVER_JMS_ENABLE_SIGNAL</b>	JMS queue for signals	true	False
<b>KIE_SERVER_JMS_QUEUE_SIGNAL</b>	<b>KIE_SERVER_JMS_QUEUE_SIGNAL</b>	Enable the Signal configuration through JMS	queue/KIE.SERVER.SIGNAL	False
<b>KIE_SERVER_JMS_ENABLE_AUDIT</b>	<b>KIE_SERVER_JMS_ENABLE_AUDIT</b>	Enable the Audit logging through JMS	true	False
<b>KIE_SERVER_JMS_QUEUE_AUDIT</b>	<b>KIE_SERVER_JMS_QUEUE_AUDIT</b>	JMS queue for audit logging	queue/KIE.SERVER.AUDIT	False
<b>KIE_SERVER_JMS_AUDIT_TRANSACTIONACTED</b>	<b>KIE_SERVER_JMS_AUDIT_TRANSACTIONACTED</b>	determines if JMS session is transacted or not - default true.	false	False
<b>AMQ_USERNAME</b>	<b>AMQ_USERNAME</b>	User name for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AMQ_PASSWORD</b>	<b>AMQ_PASSWORD</b>	Password for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	–	False
<b>AMQ_ROLE</b>	<b>AMQ_ROLE</b>	User role for standard broker user.	admin	True
<b>AMQ_QUEUES</b>	<b>AMQ_QUEUES</b>	Queue names, separated by commas. These queues will be automatically created when the broker starts. Also, they will be made accessible as JNDI resources in EAP. These are the default queues needed by KIE Server. If using custom Queues, use the same values here as in the KIE_SERVER_JMS_QUEUE_RESPONSE, KIE_SERVER_JMS_QUEUE_REQUEST, KIE_SERVER_JMS_QUEUE_SIGNAL, KIE_SERVER_JMS_QUEUE_AUDIT and KIE_SERVER_JMS_QUEUE_EXECUTOR parameters.	queue/KIE.SERVER.REQUEST,queue/KIE.SERVER.RESPONSE,queue/KIE.SERVER.EXECUTOR,queue/KIE.SERVER.SIGNAL,queue/KIE.SERVER.AUDIT	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AMQ_GLOBAL_MAX_SIZE</b>	<b>AMQ_GLOBAL_MAX_SIZE</b>	Specifies the maximum amount of memory that message data can consume. If no value is specified, half of the system's memory is allocated.	10 gb	False
<b>AMQ_SECRET</b>	–	The name of a secret containing AMQ SSL related files.	broker-app-secret	True
<b>AMQ_TRUSTSTORE</b>	<b>AMQ_TRUSTSTORE</b>	The name of the AMQ SSL Trust Store file.	broker.ts	False
<b>AMQ_TRUSTSTORE_PASSWORD</b>	<b>AMQ_TRUSTSTORE_PASSWORD</b>	The password for the AMQ Trust Store.	changeit	False
<b>AMQ_KEYSTORE</b>	<b>AMQ_KEYSTORE</b>	The name of the AMQ keystore file.	broker.ks	False
<b>AMQ_KEYSTORE_PASSWORD</b>	<b>AMQ_KEYSTORE_PASSWORD</b>	The password for the AMQ keystore and certificate.	changeit	False
<b>AMQ_PROTOCOL</b>	<b>AMQ_PROTOCOL</b>	Broker protocols to configure, separated by commas. Allowed values are: <b>openwire</b> , <b>amqp</b> , <b>stomp</b> and <b>mqtt</b> . Only <b>openwire</b> is supported by EAP.	openwire	False
<b>AMQ_BROKER_IMAGESTREAM_NAME</b>	–	AMQ Broker Image	amq-broker:7.4	True



Variable name	Image Environment Variable	Description	Example value	Required
<b>AMQ_IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStreams for Red Hat AMQ images are installed. These ImageStreams are normally installed in the openshift namespace. You should only need to modify this if you installed the ImageStreams in a different namespace/project.	openshift	True
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO Realm name	–	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name	–	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist	–	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication	Password	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=example,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_B ASE_FILTER</b>	<b>AUTH_LDAP_B ASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	(uid={0})	False
<b>AUTH_LDAP_S EARCH_SCOPE</b>	<b>AUTH_LDAP_S EARCH_SCOPE</b>	The search scope to use.	<b>SUBTREE_SCO PE</b>	False
<b>AUTH_LDAP_S EARCH_TIME_L IMIT</b>	<b>AUTH_LDAP_S EARCH_TIME_L IMIT</b>	The timeout in milliseconds for user or role searches.	10000	False
<b>AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE</b>	<b>AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	distinguishedNam e	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	true	False
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	memberOf	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLES_CTX_DN</b>	<b>AUTH_LDAP_ROLES_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	ou=groups,ou=example,ou=com	False
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	(memberOf={1})	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users	user	False
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	name	False
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttribute ID. If set to true, the DN is checked for the roleNameAttribute ID. If set to false, the DN is not checked for the roleNameAttribute ID. This flag can improve the performance of LDAP queries.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	false	False
<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This property defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	–	False

### 5.3.2. Objects

The CLI supports various object types. A list of these object types as well as their abbreviations can be found in the [OpenShift documentation](#).

#### 5.3.2.1. Services

A service is an abstraction which defines a logical set of pods and a policy by which to access them. Refer to the [container-engine documentation](#) for more information.

Service	Port	Name	Description
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	All the KIE server web server's ports.
	8443	https	
<b>\${APPLICATION_NAME}-kieserver-ping</b>	8888	ping	The JGroups ping port for clustering.
<b>\${APPLICATION_NAME}-amq-jolokia</b>	8161	amq-jolokia	The broker's console and Jolokia port.



Service	Port	Name	Description
<b>\${APPLICATION_NAME}-amq-amqp</b>	5672	amq-amqp	The broker's AMQP port.
<b>\${APPLICATION_NAME}-amq-amqp-ssl</b>	5671	amq-amqp-ssl	The broker's AMQP SSL port.
<b>\${APPLICATION_NAME}-amq-mqtt</b>	1883	amq-mqtt	The broker's MQTT port.
<b>\${APPLICATION_NAME}-amq-mqtt-ssl</b>	8883	amq-mqtt-ssl	The broker's MQTT SSL port.
<b>\${APPLICATION_NAME}-amq-stomp</b>	61613	amq-stomp	The broker's STOMP port.
<b>\${APPLICATION_NAME}-amq-stomp-ssl</b>	61612	amq-stomp-ssl	The broker's STOMP SSL port.
<b>\${APPLICATION_NAME}-amq-tcp</b>	61616	amq-tcp	The broker's OpenWire port.
<b>\${APPLICATION_NAME}-amq-tcp-ssl</b>	61617	amq-tcp-ssl	The broker's OpenWire (SSL) port.
<b>\${APPLICATION_NAME}-postgresql</b>	5432	–	The database server's port.

### 5.3.2.2. Routes

A route is a way to expose a service by giving it an externally-reachable hostname such as **www.example.com**. A defined route and the endpoints identified by its service can be consumed by a router to provide named connectivity from external clients to your applications. Each route consists of a route name, service selector, and (optionally) security configuration. Refer to the [OpenShift documentation](#) for more information.

Service	Security	Hostname
<b>\${APPLICATION_NAME}-kieserver-http</b>	none	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS passthrough	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>
<b>\${APPLICATION_NAME}-amq-jolokia-console</b>	TLS passthrough	<default>

Service	Security	Hostname
<b>\${APPLICATION_NAME}-amq-tcp-ssl</b>	TLS passthrough	<default>

### 5.3.2.3. Build Configurations

A **buildConfig** describes a single build definition and a set of triggers for when a new build should be created. A **buildConfig** is a REST object, which can be used in a POST to the API server to create a new instance. Refer to the [OpenShift documentation](#) for more information.

S2I image	link	Build output	BuildTriggers and Settings
rhpm-kieserver-rhel8:7.5.0	<a href="#">rhpm-7/rhpm-kieserver-rhel8</a>	<b>\${APPLICATION_NAME}-kieserver:latest</b>	GitHub, Generic, ImageChange, ConfigChange

### 5.3.2.4. Deployment Configurations

A deployment in OpenShift is a replication controller based on a user defined template called a deployment configuration. Deployments are created manually or in response to triggered events. Refer to the [OpenShift documentation](#) for more information.

#### 5.3.2.4.1. Triggers

A trigger drives the creation of new deployments in response to events, both inside and outside OpenShift. Refer to the [OpenShift documentation](#) for more information.

Deployment	Triggers
<b>\${APPLICATION_NAME}-kieserver</b>	ImageChange
<b>\${APPLICATION_NAME}-postgresql</b>	ImageChange
<b>\${APPLICATION_NAME}-amq</b>	ImageChange

#### 5.3.2.4.2. Replicas

A replication controller ensures that a specified number of pod "replicas" are running at any one time. If there are too many, the replication controller kills some pods. If there are too few, it starts more. Refer to the [container-engine documentation](#) for more information.

Deployment	Replicas
<b>\${APPLICATION_NAME}-kieserver</b>	2

Deployment	Replicas
<code>\${APPLICATION_NAME}-postgresql</code>	1
<code>\${APPLICATION_NAME}-amq</code>	1

### 5.3.2.4.3. Pod Template

#### 5.3.2.4.3.1. Service Accounts

Service accounts are API objects that exist within each project. They can be created or deleted like any other API object. Refer to the [Openshift documentation](#) for more information.

Deployment	Service Account
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>

#### 5.3.2.4.3.2. Image

Deployment	Image
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>
<code>\${APPLICATION_NAME}-postgresql</code>	postgresql
<code>\${APPLICATION_NAME}-amq</code>	<code>\${AMQ_BROKER_IMAGESTREAM_NAME}</code>

#### 5.3.2.4.3.3. Readiness Probe

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

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

##### `${APPLICATION_NAME}-postgresql`

```
/usr/libexec/check-container
```

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

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

#### 5.3.2.4.3.4. Liveness Probe

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

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

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

```
/usr/libexec/check-container --live
```

**5.3.2.4.3.5. Exposed Ports**

Deployments	Name	Port	Protocol
<b>`\${APPLICATION_NAME}`-kieserver</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	ping	8888	<b>TCP</b>
<b>`\${APPLICATION_NAME}`-postgresql</b>	–	5432	<b>TCP</b>
<b>`\${APPLICATION_NAME}`-amq</b>	console-jolokia	8161	<b>TCP</b>
	amqp	5672	<b>TCP</b>
	amqp-ssl	5671	<b>TCP</b>
	mqtt	1883	<b>TCP</b>
	mqtt-ssl	8883	<b>TCP</b>
	stomp	61613	<b>TCP</b>
	stomp-ssl	61612	<b>TCP</b>
	artemis	61616	<b>TCP</b>
	amq-tcp-ssl	61617	<b>TCP</b>

**5.3.2.4.3.6. Image Environment Variables**

Deployment	Variable name	Description	Example value
------------	---------------	-------------	---------------

Deployment	Variable name	Description	Example value
<b>\${APPLICATION_NAME}-kieserver</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>KIE_ADMIN_USER</b>	KIE administrator username.	<b>\${KIE_ADMIN_USER}</b>
	<b>KIE_ADMIN_PWD</b>	KIE administrator password.	<b>\${KIE_ADMIN_PWD}</b>
	<b>KIE_SERVER_MODE</b>	–	<b>DEVELOPMENT</b>
	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbeans system properties)	<b>\${KIE_MBEANS}</b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering (Sets the org.drools.server.filter.classes system property)	<b>\${DROOLS_SERVER_FILTER_CLASSES}</b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	<b>\${PROMETHEUS_SERVER_EXT_DISABLED}</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	<b>\${KIE_SERVER_BYPASS_AUTH_USER}</b>
	<b>KIE_SERVER_ID</b>	–	–
<b>KIE_SERVER_ROUTE_NAME</b>	–	insecure- \${APPLICATION_NAME} -kieserver	

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_ROUTER_SERVICE</b>	–	<b>\${APPLICATION_NAME}-smartrouter</b>
	<b>KIE_SERVER_USER</b>	KIE server username (Sets the org.kie.server.user system property)	<b>\${KIE_SERVER_USER}</b>
	<b>KIE_SERVER_PWD</b>	KIE server password. If this parameter is not set, the password is automatically generated. (Sets the org.kie.server.pwd system property)	<b>\${KIE_SERVER_PWD}</b>
	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	<b>\${KIE_SERVER_CONTAINER_DEPLOYMENT}</b>
	<b>MAVEN_REPOS</b>	–	RHPAMCENTR,EXTERNAL
	<b>RHPAMCENTR_MAVEN_REPO_SERVICE</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>RHPAMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>
	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	<b>\${BUSINESS_CENTRAL_MAVEN_USERNAME}</b>
	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	<b>\${BUSINESS_CENTRAL_MAVEN_PASSWORD}</b>

Deployment	Variable name	Description	Example value
	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository, if set. Default is generated randomly.	<b>`\${MAVEN_REPO_ID}`</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository.	<b>`\${MAVEN_REPO_URL}`</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	<b>`\${MAVEN_REPO_USERNAME}`</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	<b>`\${MAVEN_REPO_PASSWORD}`</b>
	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource (Sets the org.kie.server.persistence.ds system property)	<b>`\${KIE_SERVER_PERSISTENCE_DS}`</b>
	<b>DATASOURCES</b>	–	<b>RHPAM</b>
	<b>RHPAM_DATABASE</b>	KIE server PostgreSQL database name	<b>`\${KIE_SERVER_POSTGRES_DB}`</b>
	<b>RHPAM_JNDI</b>	KIE server persistence datasource (Sets the org.kie.server.persistence.ds system property)	<b>`\${KIE_SERVER_PERSISTENCE_DS}`</b>
	<b>RHPAM_JTA</b>	–	true
	<b>RHPAM_DRIVER</b>	–	postgresql
	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	–	org.hibernate.dialect.PostgreSQLDialect
	<b>RHPAM_USERNAME</b>	KIE server PostgreSQL database username	<b>`\${KIE_SERVER_POSTGRES_USER}`</b>
	<b>RHPAM_PASSWORD</b>	KIE server PostgreSQL database password	<b>`\${KIE_SERVER_POSTGRES_PWD}`</b>

Deployment	Variable name	Description	Example value
	<b>RHPAM_SERVICE_HOST</b>	–	<b>\${APPLICATION_NAME}-postgresql</b>
	<b>RHPAM_SERVICE_PORT</b>	–	5432
	<b>TIMER_SERVICE_DATA_STORE</b>	–	<b>\${APPLICATION_NAME}-postgresql</b>
	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer service database-data-store.	<b>\${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}</b>
	<b>KIE_SERVER_EXECUTOR_JMS</b>	Enables the JMS executor, set false to disable it.	<b>\${KIE_SERVER_EXECUTOR_JMS}</b>
	<b>KIE_SERVER_EXECUTOR_JMS_TRANSACTIONAL</b>	Enable transactions for JMS executor, disabled by default	<b>\${KIE_SERVER_EXECUTOR_JMS_TRANSACTIONAL}</b>
	<b>KIE_SERVER_JMS_QUEUE_REQUEST</b>	JNDI name of request queue for JMS. The default value is queue/KIE.SERVER.REQUEST	<b>\${KIE_SERVER_JMS_QUEUE_REQUEST}</b>
	<b>KIE_SERVER_JMS_QUEUE_RESPONSE</b>	JNDI name of response queue for JMS. The default value is queue/KIE.SERVER.RESPONSE	<b>\${KIE_SERVER_JMS_QUEUE_RESPONSE}</b>
	<b>KIE_SERVER_JMS_QUEUE_EXECUTOR</b>	JNDI name of response queue for JMS. The default value is queue/KIE.SERVER.RESPONSE	<b>\${KIE_SERVER_JMS_QUEUE_EXECUTOR}</b>
	<b>KIE_SERVER_JMS_ENABLE_SIGNAL</b>	JMS queue for signals	<b>\${KIE_SERVER_JMS_ENABLE_SIGNAL}</b>
	<b>KIE_SERVER_JMS_QUEUE_SIGNAL</b>	Enable the Signal configuration through JMS	<b>\${KIE_SERVER_JMS_QUEUE_SIGNAL}</b>
	<b>KIE_SERVER_JMS_ENABLE_AUDIT</b>	Enable the Audit logging through JMS	<b>\${KIE_SERVER_JMS_ENABLE_AUDIT}</b>



Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_JMS_QUEUE_AUDIT</b>	JMS queue for audit logging	<b>\${KIE_SERVER_JMS_QUEUE_AUDIT}</b>
	<b>KIE_SERVER_JMS_AUDIT_TRANSACTED</b>	determines if JMS session is transacted or not - default true.	<b>\${KIE_SERVER_JMS_AUDIT_TRANSACTED}</b>
	<b>MQ_SERVICE_PREFERENCE_MAPPING</b>	–	<b>\${APPLICATION_NAME}-amq7=AMQ</b>
	<b>AMQ_USERNAME</b>	User name for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	<b>\${AMQ_USERNAME}</b>
	<b>AMQ_PASSWORD</b>	Password for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	<b>\${AMQ_PASSWORD}</b>
	<b>AMQ_PROTOCOL</b>	Broker protocols to configure, separated by commas. Allowed values are: <b>openwire</b> , <b>amqp</b> , <b>stomp</b> and <b>mqtt</b> . Only <b>openwire</b> is supported by EAP.	tcp

Deployment	Variable name	Description	Example value
	<b>AMQ_QUEUES</b>	Queue names, separated by commas. These queues will be automatically created when the broker starts. Also, they will be made accessible as JNDI resources in EAP. These are the default queues needed by KIE Server. If using custom Queues, use the same values here as in the KIE_SERVER_JMS_QUEUE_RESPONSE, KIE_SERVER_JMS_QUEUE_REQUEST, KIE_SERVER_JMS_QUEUE_SIGNAL, KIE_SERVER_JMS_QUEUE_AUDIT and KIE_SERVER_JMS_QUEUE_EXECUTOR parameters.	<b>\${AMQ_QUEUES}</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/kieserver-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret	<b>\${KIE_SERVER_HTTPS_KEYSTORE}</b>
	<b>HTTPS_NAME</b>	The name associated with the server certificate	<b>\${KIE_SERVER_HTTPS_NAME}</b>
	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate	<b>\${KIE_SERVER_HTTPS_PASSWORD}</b>
	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped. (Sets the property org.kie.server.mgmt.api.disabled to true)	<b>\${KIE_SERVER_MGMT_DISABLED}</b>
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	–	OpenShiftStartupStrategy

Deployment	Variable name	Description	Example value
	<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 Realm name	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret	<b>\${KIE_SERVER_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name	<b>\${KIE_SERVER_SSO_CLIENT}</b>
	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist	<b>\${SSO_USERNAME}</b>
	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client	<b>\${SSO_PASSWORD}</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation	<b>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	<b>\${SSO_PRINCIPAL_ATTRIBUTE}</b>
	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>

Deployment	Variable name	Description	Example value
	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>. <default-domain-suffix>	<b>`\${KIE_SERVER_HOSTNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication	<b>`\${AUTH_LDAP_BIND_DN}`</b>
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication	<b>`\${AUTH_LDAP_BIND_CREDENTIAL}`</b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	<b>`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`</b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	<b>`\${AUTH_LDAP_BASE_CTX_DN}`</b>
	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	<b>`\${AUTH_LDAP_BASE_FILTER}`</b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>`\${AUTH_LDAP_SEARCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	<b>`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	<b><code>\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}</code></b>
	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	<b><code>\${AUTH_LDAP_PARSE_USERNAME}</code></b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_BEGIN_STRING}</code></b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_END_STRING}</code></b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<b><code>\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}</code></b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<b>`\${AUTH_LDAP_ROLE_S_CTX_DN}`</b>
	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	<b>`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeID attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	<b>`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`</b>
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This property defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	<b>`\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}`</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	<b>`\${AUTH_ROLE_MAPPER_REPLACE_ROLE}`</b>
<b>`\${APPLICATION_NAME}`-postgresql</b>	<b>POSTGRESQL_USER</b>	KIE server PostgreSQL database username	<b>`\${KIE_SERVER_POSTGRESQL_USER}`</b>
	<b>POSTGRESQL_PASSWORD</b>	KIE server PostgreSQL database password	<b>`\${KIE_SERVER_POSTGRESQL_PWD}`</b>
	<b>POSTGRESQL_DATABASE</b>	KIE server PostgreSQL database name	<b>`\${KIE_SERVER_POSTGRESQL_DB}`</b>



Deployment	Variable name	Description	Example value
	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	Allows the PostgreSQL to handle XA transactions.	<b>\${POSTGRESQL_MAX_PREPARED_TRANSACTIONS}</b>
<b>\${APPLICATION_NAME}-amq</b>	<b>AMQ_USER</b>	User name for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	<b>\${AMQ_USERNAME}</b>
	<b>AMQ_PASSWORD</b>	Password for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	<b>\${AMQ_PASSWORD}</b>
	<b>AMQ_ROLE</b>	User role for standard broker user.	<b>\${AMQ_ROLE}</b>
	<b>AMQ_NAME</b>	–	<b>\${APPLICATION_NAME}-broker</b>
	<b>AMQ_TRANSPORTS</b>	Broker protocols to configure, separated by commas. Allowed values are: <b>openwire</b> , <b>amqp</b> , <b>stomp</b> and <b>mqtt</b> . Only <b>openwire</b> is supported by EAP.	<b>\${AMQ_PROTOCOL}</b>

Deployment	Variable name	Description	Example value
	<b>AMQ_QUEUES</b>	Queue names, separated by commas. These queues will be automatically created when the broker starts. Also, they will be made accessible as JNDI resources in EAP. These are the default queues needed by KIE Server. If using custom Queues, use the same values here as in the KIE_SERVER_JMS_QUEUE_RESPONSE, KIE_SERVER_JMS_QUEUE_REQUEST, KIE_SERVER_JMS_QUEUE_SIGNAL, KIE_SERVER_JMS_QUEUE_AUDIT and KIE_SERVER_JMS_QUEUE_EXECUTOR parameters.	<b>\${AMQ_QUEUES}</b>
	<b>AMQ_GLOBAL_MAX_SIZE</b>	Specifies the maximum amount of memory that message data can consume. If no value is specified, half of the system's memory is allocated.	<b>\${AMQ_GLOBAL_MAX_SIZE}</b>
	<b>AMQ_REQUIRE_LOGIN</b>	–	true
	<b>AMQ_ANYCAST_PREFIX</b>	–	–
	<b>AMQ_MULTICAST_PREFIX</b>	–	–
	<b>AMQ_KEYSTORE_TRUSTSTORE_DIR</b>	–	<b>/etc/amq-secret-volume</b>
	<b>AMQ_TRUSTSTORE</b>	The name of the AMQ SSL Trust Store file.	<b>\${AMQ_TRUSTSTORE}</b>
	<b>AMQ_TRUSTSTORE_PASSWORD</b>	The password for the AMQ Trust Store.	<b>\${AMQ_TRUSTSTORE_PASSWORD}</b>

Deployment	Variable name	Description	Example value
	<b>AMQ_KEYSTORE</b>	The name of the AMQ keystore file.	<b>\${AMQ_KEYSTORE}</b>
	<b>AMQ_KEYSTORE_PASSWORD</b>	The password for the AMQ keystore and certificate.	<b>\${AMQ_KEYSTORE_PASSWORD}</b>

### 5.3.2.4.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
<b>\${APPLICATION_NAME}-kieserver</b>	kieserver-keystore-volume	<b>/etc/kieserver-secret-volume</b>	ssl certs	True
<b>\${APPLICATION_NAME}-postgresql</b>	<b>\${APPLICATION_NAME}-postgresql-pvol</b>	<b>/var/lib/pgsql/data</b>	postgresql	false
<b>\${APPLICATION_NAME}-amq</b>	broker-secret-volume	<b>/etc/amq-secret-volume</b>	ssl certs	True

### 5.3.2.5. External Dependencies

#### 5.3.2.5.1. Volume Claims

A **PersistentVolume** object is a storage resource in an OpenShift cluster. Storage is provisioned by an administrator by creating **PersistentVolume** objects from sources such as GCE Persistent Disks, AWS Elastic Block Stores (EBS), and NFS mounts. Refer to the [Openshift documentation](#) for more information.

Name	Access Mode
<b>\${APPLICATION_NAME}-postgresql-claim</b>	ReadWriteOnce

#### 5.3.2.5.2. Secrets

This template requires the following secrets to be installed for the application to run.

kieserver-app-secret broker-app-secret

## 5.4. RHPAM75-KIESERVER-EXTERNALDB.YAML TEMPLATE

Application template for a managed KIE Server with an external database, for Red Hat Process Automation Manager 7.5 - Deprecated

### 5.4.1. Parameters

Templates allow you to define parameters which take on a value. That value is then substituted wherever the parameter is referenced. References can be defined in any text field in the objects list field. Refer to the [Openshift documentation](#) for more information.

Variable name	Image Environment Variable	Description	Example value	Required
<b>APPLICATION_NAME</b>	–	The name for the application.	myapp	True
<b>MAVEN_MIRROR_URL</b>	<b>MAVEN_MIRROR_URL</b>	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for deploying your services.	–	False
<b>MAVEN_MIRROR_OF</b>	<b>MAVEN_MIRROR_OF</b>	Maven mirror configuration for KIE server.	external:*	False
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	repo-custom	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<a href="http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/">http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/</a>	True
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	–	False
<b>BUSINESS_CENTRAL_SERVICE</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	myapp-rhpamcentr	False
<b>BUSINESS_CENTRAL_MAVEN_USERNAME</b>	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
<b>BUSINESS_CENTRAL_MAVEN_PASSWORD</b>	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	maven!!	False
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE administrator username.	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE administrator password.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False
<b>KIE_SERVER_PWD</b>	<b>KIE_SERVER_PWD</b>	KIE server password. (Sets the org.kie.server.pwd system property)	–	False
<b>IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStreams for Red Hat Process Automation Manager images are installed. These ImageStreams are normally installed in the openshift namespace. You should only need to modify this if you installed the ImageStreams in a different namespace/project.	openshift	True
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	The name of the image stream to use for KIE server. Default is "rhpam-kieserver-rhel8".	rhpam-kieserver-rhel8	True
<b>IMAGE_STREAM_TAG</b>	–	A named pointer to an image in an image stream. Default is "7.5.0".	7.5.0	True
<b>KIE_SERVER_PERSISTENCE_SCHEMA</b>	<b>KIE_SERVER_PERSISTENCE_SCHEMA</b>	Hibernate persistence schema.	bd.schema	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_EXTERNALDB_DIALECT</b>	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server external database Hibernate dialect.	org.hibernate.dialect.MySQL57Dialect	True
<b>KIE_SERVER_EXTERNALDB_SERVICE_HOST</b>	<b>RHPAM_SERVICE_HOST</b>	Sets the datasource service host. Use this if you want to use the predefined mysql or postgresql datasource properties. Leave blank if the KIE_SERVER_EXTERNALDB_URL parameter is set.	10.10.10.1	False
<b>KIE_SERVER_EXTERNALDB_SERVICE_PORT</b>	<b>RHPAM_SERVICE_PORT</b>	Sets the datasource service port. Use this if you want to use the predefined mysql or postgresql datasource properties. Leave blank if the KIE_SERVER_EXTERNALDB_URL parameter is set.	4321	False
<b>KIE_SERVER_EXTERNALDB_NONXA</b>	<b>RHPAM_NONXA</b>	Sets the datasources type. It can be XA or NONXA. For non XA set it to true. Default value is true.	True	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_EXTERNALDB_URL</b>	<b>RHPAM_URL</b>	Sets the datasource jdbc connection url. Note that, if you are using PostgreSQL do not use this field, use the SERVICE_HOST and PORT. If using SERVICE_PORT and HOST there is no need to fill this parameter.	jdbc:mysql://127.0.0.1:3306/rhpam	False
<b>KIE_SERVER_EXTERNALDB_DRIVER</b>	<b>RHPAM_DRIVER</b>	The predefined driver name, available values are mysql, postgresql or the preferred name for the external driver.	mariadb	True
<b>KIE_SERVER_EXTERNALDB_JNDI</b>	<b>KIE_SERVER_PERSISTENCE_DS</b>	Database JNDI name used by application to resolve the datasource, e.g. java:/jboss/datasources/ExampleDS.	java:jboss/datasources/jbpmDS	True
<b>KIE_SERVER_EXTERNALDATABASE</b>	<b>RHPAM_DATABASE</b>	KIE server external database name. Leave blank if the KIE_SERVER_EXTERNALDB_URL is set.	rhpam	False
<b>KIE_SERVER_EXTERNALDB_USER</b>	<b>RHPAM_USERNAME</b>	KIE server external database username.	rhpam	True
<b>KIE_SERVER_EXTERNALDB_PASSWORD</b>	<b>RHPAM_PASSWORD</b>	KIE server external database password.	–	True



Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_EXTERNALDB_MIN_POOL_SIZE</b>	<b>RHPAM_MIN_POOL_SIZE</b>	Sets xa-pool/min-pool-size for the configured datasource.	–	False
<b>KIE_SERVER_EXTERNALDB_MAX_POOL_SIZE</b>	<b>RHPAM_MAX_POOL_SIZE</b>	Sets xa-pool/max-pool-size for the configured datasource.	–	False
<b>KIE_SERVER_EXTERNALDB_CONNECTION_CHECKER</b>	<b>RHPAM_CONNECTION_CHECKER</b>	An org.jboss.jca.adapters.jdbc.ValidConnectionChecker that provides a SQLException isValidConnection(Connection c) method to validate if a connection is valid.	org.jboss.jca.adapters.jdbc.extensions.mysql.MySQLValidConnectionChecker	False
<b>KIE_SERVER_EXTERNALDB_EXCEPTION_SORTER</b>	<b>RHPAM_EXCEPTION_SORTER</b>	An org.jboss.jca.adapters.jdbc.ExceptionSorter that provides a boolean isExceptionFatal(SQLException e) method to validate if an exception should be broadcast to all javax.resource.spi.ConnectionEventListener as a connectionError occurred.	org.jboss.jca.adapters.jdbc.extensions.mysql.MySQLExceptionSorter	False
<b>KIE_SERVER_EXTERNALDB_BACKGROUND_VALIDATION</b>	<b>RHPAM_BACKGROUND_VALIDATION</b>	Sets the sql validation method to background-validation, if set to false the validate-on-match method will be used.	true	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_EXTERNALDB_BACKGROUND_VALIDATION_MILLIS</b>	<b>RHPAM_VALIDATION_MILLIS</b>	Defines the interval for the background-validation check for the jdbc connections.	10000	False
<b>KIE_SERVER_EXTERNALDB_DRIVER_TYPE</b>	<b>RHPAM_DRIVER_TYPE</b>	KIE server external database driver type, applicable only for DB2, possible values are 4 (default) or 2.	4	False
<b>EXTENSIONS_IMAGE</b>	–	ImageStreamTag definition for the image containing the drivers and configuration. For example, custom-driver-image:1.0.	custom-driver-extension:1.0	True
<b>EXTENSIONS_IMAGE_NAMESPACE</b>	–	Namespace within which the ImageStream definition for the image containing the drivers and configuration is located.	openshift	True
<b>EXTENSIONS_INSTALL_DIR</b>	–	Full path to the directory within the extensions image where the extensions are located (e.g. install.sh, modules/, etc.).	<b>/extensions</b>	True

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_MODE</b>	<b>KIE_SERVER_MODE</b>	The KIE Server mode. Valid values are 'DEVELOPMENT' or 'PRODUCTION'. In production mode, you can not deploy SNAPSHOT versions of artifacts on the KIE server and can not change the version of an artifact in an existing container. (Sets the org.kie.server.mode system property).	<b>PRODUCTION</b>	False
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbeans system properties).	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering (Sets the org.drools.server.filter.classes system property).	true	False
<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	The name of the secret containing the keystore file.	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	The name associated with the server certificate.	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	mykeystorepass	False
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer database data-store service.	30000	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	KIE server Container memory limit.	1Gi	False
<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	rhpm-kieserver-library=org.openshift.quickstarts:rhpm-kieserver-library:1.5.0-SNAPSHOT	False
<b>KIE_SERVER_MGMT_DISABLED</b>	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped. Sets the property org.kie.server.management.api.disabled to true and org.kie.server.startup.strategy to LocalContainersStartupStrategy.	true	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL.	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO Realm name.	–	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	–	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	–	False
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	Password	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	(uid={0})	False
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>SUBTREE_SCOPE</b>	False
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	10000	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	distinguishedName	False
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	true	False
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False



Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<code>memberOf</code>	False
<b>AUTH_LDAP_ROLE_CTX_DN</b>	<b>AUTH_LDAP_ROLE_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<code>ou=groups,ou=example,ou=com</code>	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	(memberOf={1})	False
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users.	user	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	name	False
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttribute ID. If set to true, the DN is checked for the roleNameAttribute ID. If set to false, the DN is not checked for the roleNameAttribute ID. This flag can improve the performance of LDAP queries.	false	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	–	False
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This property defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	–	False

## 5.4.2. Objects

The CLI supports various object types. A list of these object types as well as their abbreviations can be found in the [Openshift documentation](#).

### 5.4.2.1. Services

A service is an abstraction which defines a logical set of pods and a policy by which to access them. Refer to the [container-engine documentation](#) for more information.

Service	Port	Name	Description
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	All the KIE server web server's ports.
	8443	https	
<b>\${APPLICATION_NAME}-kieserver-ping</b>	8888	ping	The JGroups ping port for clustering.

### 5.4.2.2. Routes

A route is a way to expose a service by giving it an externally-reachable hostname such as **www.example.com**. A defined route and the endpoints identified by its service can be consumed by a router to provide named connectivity from external clients to your applications. Each route consists of a route name, service selector, and (optionally) security configuration. Refer to the [Openshift documentation](#) for more information.

Service	Security	Hostname
insecure- <b>\${APPLICATION_NAME}-kieserver-http</b>	none	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS passthrough	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

### 5.4.2.3. Build Configurations

A **buildConfig** describes a single build definition and a set of triggers for when a new build should be created. A **buildConfig** is a REST object, which can be used in a POST to the API server to create a new instance. Refer to the [Openshift documentation](#) for more information.

S2I image	link	Build output	BuildTriggers and Settings
rhpam-kieserver-rhel8:7.5.0	<a href="#">rhpam-7/rhpam-kieserver-rhel8</a>	<b>\${APPLICATION_NAME}-kieserver:latest</b>	ImageChange, ImageChange, ConfigChange

#### 5.4.2.4. Deployment Configurations

A deployment in OpenShift is a replication controller based on a user defined template called a deployment configuration. Deployments are created manually or in response to triggered events. Refer to the [OpenShift documentation](#) for more information.

##### 5.4.2.4.1. Triggers

A trigger drives the creation of new deployments in response to events, both inside and outside OpenShift. Refer to the [OpenShift documentation](#) for more information.

Deployment	Triggers
<code>\${APPLICATION_NAME}-kieserver</code>	ImageChange

##### 5.4.2.4.2. Replicas

A replication controller ensures that a specified number of pod "replicas" are running at any one time. If there are too many, the replication controller kills some pods. If there are too few, it starts more. Refer to the [container-engine documentation](#) for more information.

Deployment	Replicas
<code>\${APPLICATION_NAME}-kieserver</code>	1

##### 5.4.2.4.3. Pod Template

###### 5.4.2.4.3.1. Service Accounts

Service accounts are API objects that exist within each project. They can be created or deleted like any other API object. Refer to the [OpenShift documentation](#) for more information.

Deployment	Service Account
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${APPLICATION_NAME}-kieserver</code>

###### 5.4.2.4.3.2. Image

Deployment	Image
<code>\${APPLICATION_NAME}-kieserver</code>	<code>\${KIE_SERVER_IMAGE_STREAM_NAME}</code>

###### 5.4.2.4.3.3. Readiness Probe

`${APPLICATION_NAME}-kieserver`

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

## 5.4.2.4.3.4. Liveness Probe

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

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

## 5.4.2.4.3.5. Exposed Ports

Deployments	Name	Port	Protocol
<b>\${APPLICATION_NAME}-kieserver</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	ping	8888	<b>TCP</b>

## 5.4.2.4.3.6. Image Environment Variables

Deployment	Variable name	Description	Example value
<b>\${APPLICATION_NAME}-kieserver</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>KIE_ADMIN_USER</b>	KIE administrator username.	<b>\${KIE_ADMIN_USER}</b>
	<b>KIE_ADMIN_PWD</b>	KIE administrator password.	<b>\${KIE_ADMIN_PWD}</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_MODE</b>	The KIE Server mode. Valid values are 'DEVELOPMENT' or 'PRODUCTION'. In production mode, you can not deploy SNAPSHOT versions of artifacts on the KIE server and can not change the version of an artifact in an existing container. (Sets the org.kie.server.mode system property).	<b>`\${KIE_SERVER_MODE}`</b>
	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbeans system properties).	<b>`\${KIE_MBEANS}`</b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering (Sets the org.drools.server.filter.classes system property).	<b>`\${DROOLS_SERVER_FILTER_CLASSES}`</b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	<b>`\${PROMETHEUS_SERVER_EXT_DISABLED}`</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	<b>`\${KIE_SERVER_BYPASS_AUTH_USER}`</b>
	<b>KIE_SERVER_ID</b>	–	–
	<b>KIE_SERVER_ROUTE_NAME</b>	–	<b>`\${APPLICATION_NAME}`-kieserver</b>



Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	<b>\${KIE_SERVER_USER}</b>
	<b>KIE_SERVER_PWD</b>	KIE server password. (Sets the org.kie.server.pwd system property)	<b>\${KIE_SERVER_PWD}</b>
	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	<b>\${KIE_SERVER_CONTAINER_DEPLOYMENT}</b>
	<b>MAVEN_MIRROR_URL</b>	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for deploying your services.	<b>\${MAVEN_MIRROR_URL}</b>
	<b>MAVEN_MIRROR_OF</b>	Maven mirror configuration for KIE server.	<b>\${MAVEN_MIRROR_OF}</b>
	<b>MAVEN_REPOS</b>	–	RHPAMCENTR,EXTERNAL
	<b>RHPAMCENTR_MAVEN_REPO_ID</b>	–	repo-rhpamcentr
	<b>RHPAMCENTR_MAVEN_REPO_SERVICE</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>RHPAMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>

Deployment	Variable name	Description	Example value
	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_USERNAME}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_PASSWORD}`</b>
	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	<b>`\${MAVEN_REPO_ID}`</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<b>`\${MAVEN_REPO_URL}`</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	<b>`\${MAVEN_REPO_USERNAME}`</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	<b>`\${MAVEN_REPO_PASSWORD}`</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped. Sets the property org.kie.server.mgmt.api.disabled to true and org.kie.server.startup.strategy to LocalContainersStartupStrategy.	<b>`\${KIE_SERVER_MGMT_DISABLED}`</b>
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	–	OpenShiftStartupStrategy
	<b>KIE_SERVER_PERSISTENCE_DS</b>	Database JNDI name used by application to resolve the datasource, e.g. java:/jboss/datasources/ExampleDS.	<b>`\${KIE_SERVER_EXTERNALDB_JNDI}`</b>
	<b>KIE_SERVER_PERSISTENCE_SCHEMA</b>	Hibernate persistence schema.	<b>`\${KIE_SERVER_PERSISTENCE_SCHEMA}`</b>
	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server external database Hibernate dialect.	<b>`\${KIE_SERVER_EXTERNALDB_DIALECT}`</b>
	<b>DATASOURCES</b>	–	<b>RHPAM</b>
	<b>RHPAM_DATABASE</b>	KIE server external database name. Leave blank if the KIE_SERVER_EXTERNALDB_URL is set.	<b>`\${KIE_SERVER_EXTERNALDB_DB}`</b>
	<b>RHPAM_SERVICE_HOST</b>	Sets the datasource service host. Use this if you want to use the predefined mysql or postgresql datasource properties. Leave blank if the KIE_SERVER_EXTERNALDB_URL parameter is set.	<b>`\${KIE_SERVER_EXTERNALDB_SERVICE_HOST}`</b>

Deployment	Variable name	Description	Example value
	<b>RHPAM_SERVICE_PORT</b>	Sets the datasource service port. Use this if you want to use the predefined mysql or postgresql datasource properties. Leave blank if the KIE_SERVER_EXTERNALDB_URL parameter is set.	<b>`\${KIE_SERVER_EXTERNALDB_SERVICE_PORT}`</b>
	<b>RHPAM_JNDI</b>	Database JNDI name used by application to resolve the datasource, e.g. java:/jboss/datasources/ExampleDS.	<b>`\${KIE_SERVER_EXTERNALDB_JNDI}`</b>
	<b>RHPAM_DRIVER</b>	The predefined driver name, available values are mysql, postgresql or the preferred name for the external driver.	<b>`\${KIE_SERVER_EXTERNALDB_DRIVER}`</b>
	<b>RHPAM_USERNAME</b>	KIE server external database username.	<b>`\${KIE_SERVER_EXTERNALDB_USER}`</b>
	<b>RHPAM_PASSWORD</b>	KIE server external database password.	<b>`\${KIE_SERVER_EXTERNALDB_PWD}`</b>
	<b>RHPAM_NONXA</b>	Sets the datasources type. It can be XA or NONXA. For non XA set it to true. Default value is true.	<b>`\${KIE_SERVER_EXTERNALDB_NONXA}`</b>
	<b>RHPAM_URL</b>	Sets the datasource jdbc connection url. Note that, if you are using PostgreSQL do not use this field, use the SERVICE_HOST and PORT. If using SERVICE_PORT and HOST there is no need to fill this parameter.	<b>`\${KIE_SERVER_EXTERNALDB_URL}`</b>

Deployment	Variable name	Description	Example value
	<b>RHPAM_XA_CONNECTION_PROPERTY_URL</b>	Sets the datasource jdbc connection url. Note that, if you are using PostgreSQL do not use this field, use the SERVICE_HOST and PORT. If using SERVICE_PORT and HOST there is no need to fill this parameter.	<b>`\${KIE_SERVER_EXTERNALDB_URL}`</b>
	<b>RHPAM_MIN_POOL_SIZE</b>	Sets xa-pool/min-pool-size for the configured datasource.	<b>`\${KIE_SERVER_EXTERNALDB_MIN_POOL_SIZE}`</b>
	<b>RHPAM_MAX_POOL_SIZE</b>	Sets xa-pool/max-pool-size for the configured datasource.	<b>`\${KIE_SERVER_EXTERNALDB_MAX_POOL_SIZE}`</b>
	<b>RHPAM_CONNECTION_CHECKER</b>	An org.jboss.jca.adapters.jdbc.ValidConnectionChecker that provides a SQLException isValidConnection(Connection c) method to validate if a connection is valid.	<b>`\${KIE_SERVER_EXTERNALDB_CONNECTION_CHECKER}`</b>
	<b>RHPAM_EXCEPTION_SORTER</b>	An org.jboss.jca.adapters.jdbc.ExceptionSorter that provides a boolean isExceptionFatal(SQLException e) method to validate if an exception should be broadcast to all javax.resource.spi.ConnectionEventListener as a connectionErrorOccurred.	<b>`\${KIE_SERVER_EXTERNALDB_EXCEPTION_SORTER}`</b>
	<b>RHPAM_BACKGROUND_VALIDATION</b>	Sets the sql validation method to background-validation, if set to false the validate-on-match method will be used.	<b>`\${KIE_SERVER_EXTERNALDB_BACKGROUND_VALIDATION}`</b>

Deployment	Variable name	Description	Example value
	<b>RHPAM_VALIDATION_MILLIS</b>	Defines the interval for the background-validation check for the jdbc connections.	<b>`\${KIE_SERVER_EXTERNALDB_BACKGROUND_VALIDATION_MILLIS}`</b>
	<b>RHPAM_DRIVER_TYPE</b>	KIE server external database driver type, applicable only for DB2, possible values are 4 (default) or 2.	<b>`\${KIE_SERVER_EXTERNALDB_DRIVER_TYPE}`</b>
	<b>RHPAM_JTA</b>	–	true
	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer database data-store service.	<b>`\${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}`</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/kieserver-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	<b>`\${KIE_SERVER_HTTPS_KEYSTORE}`</b>
	<b>HTTPS_NAME</b>	The name associated with the server certificate.	<b>`\${KIE_SERVER_HTTPS_NAME}`</b>
	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	<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 Realm name.	<b>`\${SSO_REALM}`</b>

Deployment	Variable name	Description	Example value
	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	<b>`\${KIE_SERVER_SSO_SECRET}`</b>
	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	<b>`\${KIE_SERVER_SSO_CLIENT}`</b>
	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	<b>`\${SSO_USERNAME}`</b>
	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	<b>`\${SSO_PASSWORD}`</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	<b>`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	<b>`\${SSO_PRINCIPAL_ATTRIBUTE}`</b>
	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	<b>`\${KIE_SERVER_HOSTNAME_HTTP}`</b>
	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	<b>`\${KIE_SERVER_HOSTNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	<b>`\${AUTH_LDAP_BIND_DN}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	<b>`\${AUTH_LDAP_BIND_CREDENTIAL}`</b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	<b>`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`</b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	<b>`\${AUTH_LDAP_BASE_CTX_DN}`</b>
	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	<b>`\${AUTH_LDAP_BASE_FILTER}`</b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>`\${AUTH_LDAP_SEARCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	<b>`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`</b>
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	<b>`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`</b>



Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	<b><code>\${AUTH_LDAP_PARSE_USERNAME}</code></b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_BEGIN_STRING}</code></b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_END_STRING}</code></b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<b><code>\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}</code></b>
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<b><code>\${AUTH_LDAP_ROLE_S_CTX_DN}</code></b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users.	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	<b>`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeID attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`</b>
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	<b>`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This property defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	<b>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	<b>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</b>

#### 5.4.2.4.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
<b>\${APPLICATION_NAME}-kieserver</b>	kieserver-keystore-volume	<b>/etc/kieserver-secret-volume</b>	ssl certs	True

#### 5.4.2.5. External Dependencies

##### 5.4.2.5.1. Secrets

This template requires the following secrets to be installed for the application to run.

kieserver-app-secret

## 5.5. RHPAM75-KIESERVER-MYSQL.YAML TEMPLATE

Application template for a managed KIE Server with a MySQL database, for Red Hat Process Automation Manager 7.5 - Deprecated

### 5.5.1. Parameters

Templates allow you to define parameters which take on a value. That value is then substituted wherever the parameter is referenced. References can be defined in any text field in the objects list field. Refer to the [OpenShift documentation](#) for more information.

Variable name	Image Environment Variable	Description	Example value	Required
<b>APPLICATION_NAME</b>	–	The name for the application.	myapp	True
<b>MAVEN_MIRROR_URL</b>	<b>MAVEN_MIRROR_URL</b>	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for deploying your services.	–	False
<b>MAVEN_MIRROR_OF</b>	<b>MAVEN_MIRROR_OF</b>	Maven mirror configuration for KIE server.	external:*	False
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to <b>MAVEN_MIRROR_OF</b> . For example: external:*,!repo-rhcamcentr,!repo-custom. If <b>MAVEN_MIRROR_URL</b> is set but <b>MAVEN_MIRROR_ID</b> is not set, an id will be generated randomly, but won't be usable in <b>MAVEN_MIRROR_OF</b> .	repo-custom	False
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<a href="http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/">http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/</a>	True

Variable name	Image Environment Variable	Description	Example value	Required
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	–	False
<b>BUSINESS_CENTRAL_SERVICE</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	myapp-rhpamcentr	False
<b>BUSINESS_CENTRAL_MAVEN_USERNAME</b>	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
<b>BUSINESS_CENTRAL_MAVEN_PASSWORD</b>	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	maven!!	False
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE administrator username.	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE administrator password.	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_PWD</b>	<b>KIE_SERVER_PWD</b>	KIE server password. (Sets the org.kie.server.pwd system property)	–	False
<b>IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStreams for Red Hat Process Automation Manager images are installed. These ImageStreams are normally installed in the openshift namespace. You should only need to modify this if you installed the ImageStreams in a different namespace/project.	openshift	True
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	The name of the image stream to use for KIE server. Default is "rhpam-kieserver-rhel8".	rhpam-kieserver-rhel8	True
<b>IMAGE_STREAM_TAG</b>	–	A named pointer to an image in an image stream. Default is "7.5.0".	7.5.0	True
<b>KIE_SERVER_PERSISTENCE_DS</b>	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	java:/jboss/datasources/rhpam	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>MYSQL_IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStream for the MySQL image is installed. The ImageStream is already installed in the openshift namespace. You should only need to modify this if you installed the ImageStream in a different namespace/project. Default is "openshift".	openshift	False
<b>MYSQL_IMAGE_STREAM_TAG</b>	–	The MySQL image version, which is intended to correspond to the MySQL version. Default is "5.7".	5.7	False
<b>KIE_SERVER_MYSQL_USER</b>	<b>RHPAM_USERNAME</b>	KIE server MySQL database username.	rhpm	False
<b>KIE_SERVER_MYSQL_PWD</b>	<b>RHPAM_PASSWORD</b>	KIE server MySQL database password.	–	False
<b>KIE_SERVER_MYSQL_DB</b>	<b>RHPAM_DATABASE</b>	KIE server MySQL database name.	rhpm7	False
<b>DB_VOLUME_CAPACITY</b>	–	Size of persistent storage for the database volume.	1Gi	True
<b>KIE_SERVER_MYSQL_DIALECT</b>	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server MySQL Hibernate dialect.	org.hibernate.dialect.MySQL57Dialect	True



Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_MODE</b>	<b>KIE_SERVER_MODE</b>	The KIE Server mode. Valid values are 'DEVELOPMENT' or 'PRODUCTION'. In production mode, you can not deploy SNAPSHOT versions of artifacts on the KIE server and can not change the version of an artifact in an existing container. (Sets the org.kie.server.mode system property).	<b>PRODUCTION</b>	False
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	true	False
<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	The name of the secret containing the keystore file.	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	The name associated with the server certificate.	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	mykeystorepass	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the <code>org.kie.server.bypass.auth.user</code> system property)	false	False
<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer database data-store service.	30000	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	KIE server Container memory limit.	1Gi	False
<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: <code>containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2</code>	<code>rhpm-kieserver-library=org.openshift.quickstarts:rhpm-kieserver-library:1.5.0-SNAPSHOT</code>	False
<b>KIE_SERVER_MGMT_DISABLE</b>	<b>KIE_SERVER_MGMT_DISABLE</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped sets the property <code>org.kie.server.management.api.disabled</code> to true and <code>org.kie.server.startup.strategy</code> to <code>LocalContainersStartupStrategy</code> .	true	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL.	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO Realm name.	–	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	–	False
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	–	False
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	Password	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BASE_FILTER</b>	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	(uid={0})	False
<b>AUTH_LDAP_SEARCH_SCOPE</b>	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>SUBTREE_SCOPE</b>	False
<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	10000	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	distinguishedName	False
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	true	False
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<code>memberOf</code>	False
<b>AUTH_LDAP_ROLE_CTX_DN</b>	<b>AUTH_LDAP_ROLE_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<code>ou=groups,ou=example,ou=com</code>	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	(memberOf={1})	False
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users.	user	False



Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	name	False
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttribute ID. If set to true, the DN is checked for the roleNameAttribute ID. If set to false, the DN is not checked for the roleNameAttribute ID. This flag can improve the performance of LDAP queries.	false	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	–	False
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	–	False

## 5.5.2. Objects

The CLI supports various object types. A list of these object types as well as their abbreviations can be found in the [Openshift documentation](#).

### 5.5.2.1. Services

A service is an abstraction which defines a logical set of pods and a policy by which to access them. Refer to the [container-engine documentation](#) for more information.

Service	Port	Name	Description
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	All the KIE server web server's ports.
	8443	https	
<b>\${APPLICATION_NAME}-kieserver-ping</b>	8888	ping	The JGroups ping port for clustering.
<b>\${APPLICATION_NAME}-mysql</b>	3306	–	The database server's port.

### 5.5.2.2. Routes

A route is a way to expose a service by giving it an externally-reachable hostname such as **www.example.com**. A defined route and the endpoints identified by its service can be consumed by a router to provide named connectivity from external clients to your applications. Each route consists of a route name, service selector, and (optionally) security configuration. Refer to the [Openshift documentation](#) for more information.

Service	Security	Hostname
insecure- <b>\${APPLICATION_NAME}-kieserver-http</b>	none	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS passthrough	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

### 5.5.2.3. Deployment Configurations

A deployment in OpenShift is a replication controller based on a user defined template called a deployment configuration. Deployments are created manually or in response to triggered events. Refer to the [Openshift documentation](#) for more information.

#### 5.5.2.3.1. Triggers

A trigger drives the creation of new deployments in response to events, both inside and outside OpenShift. Refer to the [Openshift documentation](#) for more information.

Deployment	Triggers
<b>\${APPLICATION_NAME}-kieserver</b>	ImageChange
<b>\${APPLICATION_NAME}-mysql</b>	ImageChange

#### 5.5.2.3.2. Replicas

A replication controller ensures that a specified number of pod "replicas" are running at any one time. If there are too many, the replication controller kills some pods. If there are too few, it starts more. Refer to the [container-engine documentation](#) for more information.

Deployment	Replicas
<b>\${APPLICATION_NAME}-kieserver</b>	1
<b>\${APPLICATION_NAME}-mysql</b>	1

#### 5.5.2.3.3. Pod Template

##### 5.5.2.3.3.1. Service Accounts

Service accounts are API objects that exist within each project. They can be created or deleted like any other API object. Refer to the [OpenShift documentation](#) for more information.

Deployment	Service Account
<b>\${APPLICATION_NAME}-kieserver</b>	<b>\${APPLICATION_NAME}-kieserver</b>

##### 5.5.2.3.3.2. Image

Deployment	Image
<b>\${APPLICATION_NAME}-kieserver</b>	<b>\${KIE_SERVER_IMAGE_STREAM_NAME}</b>
<b>\${APPLICATION_NAME}-mysql</b>	mysql

##### 5.5.2.3.3.3. Readiness Probe

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

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

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

```
/bin/sh -i -c MYSQL_PWD="$MYSQL_PASSWORD" mysql -h 127.0.0.1 -u $MYSQL_USER -D
$MYSQL_DATABASE -e 'SELECT 1'
```

#### 5.5.2.3.3.4. Liveness Probe

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

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

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

tcpSocket on port 3306

#### 5.5.2.3.3.5. Exposed Ports

Deployments	Name	Port	Protocol
<b>\${APPLICATION_NAME}-kieserver</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	ping	8888	<b>TCP</b>
<b>\${APPLICATION_NAME}-mysql</b>	–	3306	<b>TCP</b>

#### 5.5.2.3.3.6. Image Environment Variables

Deployment	Variable name	Description	Example value
<b>\${APPLICATION_NAME}-kieserver</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>KIE_ADMIN_USER</b>	KIE administrator username.	<b>\${KIE_ADMIN_USER}</b>
	<b>KIE_ADMIN_PWD</b>	KIE administrator password.	<b>\${KIE_ADMIN_PWD}</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_MODE</b>	The KIE Server mode. Valid values are 'DEVELOPMENT' or 'PRODUCTION'. In production mode, you can not deploy SNAPSHOT versions of artifacts on the KIE server and can not change the version of an artifact in an existing container. (Sets the org.kie.server.mode system property).	<b>`\${KIE_SERVER_MODE}`</b>
	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	<b>`\${KIE_MBEANS}`</b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	<b>`\${DROOLS_SERVER_FILTER_CLASSES}`</b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	<b>`\${PROMETHEUS_SERVER_EXT_DISABLED}`</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	<b>`\${KIE_SERVER_BYPASS_AUTH_USER}`</b>
	<b>KIE_SERVER_ID</b>	–	–
	<b>KIE_SERVER_ROUTE_NAME</b>	–	<b>`\${APPLICATION_NAME}`-kieserver</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	<b>`\${KIE_SERVER_USER}`</b>
	<b>KIE_SERVER_PWD</b>	KIE server password. (Sets the org.kie.server.pwd system property)	<b>`\${KIE_SERVER_PWD}`</b>
	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	<b>`\${KIE_SERVER_CONTAINER_DEPLOYMENT}`</b>
	<b>MAVEN_MIRROR_URL</b>	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for deploying your services.	<b>`\${MAVEN_MIRROR_URL}`</b>
	<b>MAVEN_MIRROR_OFF</b>	Maven mirror configuration for KIE server.	<b>`\${MAVEN_MIRROR_OFF}`</b>
	<b>MAVEN_REPOS</b>	–	RHPAMCENTR,EXTERNAL
	<b>RHPAMCENTR_MAVEN_REPO_ID</b>	–	repo-rhpamcentr
	<b>RHPAMCENTR_MAVEN_REPO_SERVICE</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>`\${BUSINESS_CENTRAL_SERVICE}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>

Deployment	Variable name	Description	Example value
	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_USERNAME}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_PASSWORD}`</b>
	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	<b>`\${MAVEN_REPO_ID}`</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<b>`\${MAVEN_REPO_URL}`</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	<b>`\${MAVEN_REPO_USERNAME}`</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	<b>`\${MAVEN_REPO_PASSWORD}`</b>



Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped sets the property org.kie.server.mgmt.api.disabled to true and org.kie.server.startup.strategy to LocalContainersStartupStrategy.	<b>\${KIE_SERVER_MGMT_DISABLED}</b>
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	–	OpenShiftStartupStrategy
	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	<b>\${KIE_SERVER_PERSISTENCE_DS}</b>
	<b>DATASOURCES</b>	–	<b>RHPAM</b>
	<b>RHPAM_JNDI</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	<b>\${KIE_SERVER_PERSISTENCE_DS}</b>
	<b>RHPAM_CONNECTION_CHECKER</b>	–	org.jboss.jca.adapters.jdbc.extensions.mysql.MySQLValidConnectionChecker
	<b>RHPAM_EXCEPTION_SORTER</b>	–	org.jboss.jca.adapters.jdbc.extensions.mysql.MySQLExceptionSorter
	<b>RHPAM_DATABASE</b>	KIE server MySQL database name.	<b>\${KIE_SERVER_MYSQL_DB}</b>
	<b>RHPAM_DRIVER</b>	–	mariadb
	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server MySQL Hibernate dialect.	<b>\${KIE_SERVER_MYSQL_DIALECT}</b>
	<b>RHPAM_USERNAME</b>	KIE server MySQL database username.	<b>\${KIE_SERVER_MYSQL_USER}</b>

Deployment	Variable name	Description	Example value
	<b>RHPAM_PASSWORD</b>	KIE server MySQL database password.	<b>\${KIE_SERVER_MYSQL_PWD}</b>
	<b>RHPAM_SERVICE_HOST</b>	–	<b>\${APPLICATION_NAME}-mysql</b>
	<b>RHPAM_SERVICE_PORT</b>	–	3306
	<b>RHPAM_JTA</b>	–	true
	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer database data-store service.	<b>\${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/kieserver-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	<b>\${KIE_SERVER_HTTPS_KEYSTORE}</b>
	<b>HTTPS_NAME</b>	The name associated with the server certificate.	<b>\${KIE_SERVER_HTTPS_NAME}</b>
	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	<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 Realm name.	<b>\${SSO_REALM}</b>

Deployment	Variable name	Description	Example value
	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	<b>`\${KIE_SERVER_SSO_SECRET}`</b>
	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	<b>`\${KIE_SERVER_SSO_CLIENT}`</b>
	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	<b>`\${SSO_USERNAME}`</b>
	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	<b>`\${SSO_PASSWORD}`</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	<b>`\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}`</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	<b>`\${SSO_PRINCIPAL_ATTRIBUTE}`</b>
	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	<b>`\${KIE_SERVER_HOSTNAME_HTTP}`</b>
	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	<b>`\${KIE_SERVER_HOSTNAME_HTTPS}`</b>
	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	<b>`\${AUTH_LDAP_URL}`</b>
	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	<b>`\${AUTH_LDAP_BIND_DN}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	<b>`\${AUTH_LDAP_BIND_CREDENTIAL}`</b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	<b>`\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}`</b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	<b>`\${AUTH_LDAP_BASE_CTX_DN}`</b>
	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	<b>`\${AUTH_LDAP_BASE_FILTER}`</b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b>`\${AUTH_LDAP_SEARCH_SCOPE}`</b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	<b>`\${AUTH_LDAP_SEARCH_TIME_LIMIT}`</b>
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	<b>`\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	<b><code>\${AUTH_LDAP_PARSE_USERNAME}</code></b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_BEGIN_STRING}</code></b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b><code>\${AUTH_LDAP_USERNAME_END_STRING}</code></b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<b><code>\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}</code></b>
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<b><code>\${AUTH_LDAP_ROLE_S_CTX_DN}</code></b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users.	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	<b>`\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	<b>`\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}`</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeID attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}`</b>
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	<b>`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	<b>\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	<b>\${AUTH_ROLE_MAPPER_REPLACE_ROLE}</b>
<b>\${APPLICATION_NAME}-mysql</b>	<b>MYSQL_USER</b>	KIE server MySQL database username.	<b>\${KIE_SERVER_MYSQL_USER}</b>
	<b>MYSQL_PASSWORD</b>	KIE server MySQL database password.	<b>\${KIE_SERVER_MYSQL_PWD}</b>
	<b>MYSQL_DATABASE</b>	KIE server MySQL database name.	<b>\${KIE_SERVER_MYSQL_DB}</b>

#### 5.5.2.3.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
<b>\${APPLICATION_NAME}-kieserver</b>	kieserver-keystore-volume	<b>/etc/kieserver-secret-volume</b>	ssl certs	True
<b>\${APPLICATION_NAME}-mysql</b>	<b>\${APPLICATION_NAME}-mysql-pvol</b>	<b>/var/lib/mysql/data</b>	mysql	false

#### 5.5.2.4. External Dependencies

##### 5.5.2.4.1. Volume Claims

A **PersistentVolume** object is a storage resource in an OpenShift cluster. Storage is provisioned by an administrator by creating **PersistentVolume** objects from sources such as GCE Persistent Disks, AWS



Elastic Block Stores (EBS), and NFS mounts. Refer to the [Openshift documentation](#) for more information.

Name	Access Mode
<b>\${APPLICATION_NAME}-mysql-claim</b>	ReadWriteOnce

#### 5.5.2.4.2. Secrets

This template requires the following secrets to be installed for the application to run.

kieserver-app-secret

## 5.6. RHPAM75-KIESERVER-POSTGRESQL.YAML TEMPLATE

Application template for a managed KIE Server with a PostgreSQL database, for Red Hat Process Automation Manager 7.5 - Deprecated

### 5.6.1. Parameters

Templates allow you to define parameters which take on a value. That value is then substituted wherever the parameter is referenced. References can be defined in any text field in the objects list field. Refer to the [Openshift documentation](#) for more information.

Variable name	Image Environment Variable	Description	Example value	Required
<b>APPLICATION_NAME</b>	–	The name for the application.	myapp	True
<b>MAVEN_MIRROR_URL</b>	<b>MAVEN_MIRROR_URL</b>	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for deploying your services.	–	False
<b>MAVEN_MIRROR_OF</b>	<b>MAVEN_MIRROR_OF</b>	Maven mirror configuration for KIE server.	external:*	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>MAVEN_REPO_ID</b>	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	repo-custom	False
<b>MAVEN_REPO_URL</b>	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<a href="http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/">http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/</a>	True
<b>MAVEN_REPO_USERNAME</b>	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	–	False
<b>MAVEN_REPO_PASSWORD</b>	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	–	False
<b>BUSINESS_CENTRAL_SERVICE</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	myapp-rhpamcentr	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>BUSINESS_CENTRAL_MAVEN_USERNAME</b>	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
<b>BUSINESS_CENTRAL_MAVEN_PASSWORD</b>	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	maven!!	False
<b>KIE_ADMIN_USER</b>	<b>KIE_ADMIN_USER</b>	KIE administrator username.	adminUser	False
<b>KIE_ADMIN_PASSWORD</b>	<b>KIE_ADMIN_PASSWORD</b>	KIE administrator password.	–	False
<b>KIE_SERVER_USER</b>	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False
<b>KIE_SERVER_PASSWORD</b>	<b>KIE_SERVER_PASSWORD</b>	KIE server password. (Sets the org.kie.server.pwd system property)	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStreams for Red Hat Process Automation Manager images are installed. These ImageStreams are normally installed in the openshift namespace. You should only need to modify this if you installed the ImageStreams in a different namespace/project.	openshift	True
<b>KIE_SERVER_IMAGE_STREAM_NAME</b>	–	The name of the image stream to use for KIE server. Default is "rhpam-kieserver-rhel8".	rhpam-kieserver-rhel8	True
<b>IMAGE_STREAM_TAG</b>	–	A named pointer to an image in an image stream. Default is "7.5.0".	7.5.0	True
<b>KIE_SERVER_PERSISTENCE_DS</b>	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	java:/jboss/datasources/rhpam	False
<b>KIE_SERVER_POSTGRESQL_USERNAME</b>	<b>RHPAM_USERNAME</b>	KIE server PostgreSQL database username.	rhpam	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_POSTGRESQL_PASSWORD</b>	<b>RHPAM_PASSWORD</b>	KIE server PostgreSQL database password.	–	False
<b>KIE_SERVER_POSTGRESQL_DATABASE</b>	<b>RHPAM_DATABASE</b>	KIE server PostgreSQL database name.	rhpm7	False
<b>POSTGRESQL_IMAGE_STREAM_NAMESPACE</b>	–	Namespace in which the ImageStream for the PostgreSQL image is installed. The ImageStream is already installed in the openshift namespace. You should only need to modify this if you installed the ImageStream in a different namespace/project. Default is "openshift".	openshift	False
<b>POSTGRESQL_IMAGE_STREAM_TAG</b>	–	The PostgreSQL image version, which is intended to correspond to the PostgreSQL version. Default is "10".	10	False
<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	Allows the PostgreSQL to handle XA transactions.	100	True
<b>DB_VOLUME_CAPACITY</b>	–	Size of persistent storage for the database volume.	1Gi	True
<b>KIE_SERVER_POSTGRESQL_DIALECT</b>	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server PostgreSQL Hibernate dialect.	org.hibernate.dialect.PostgreSQLDialect	True

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_MODE</b>	<b>KIE_SERVER_MODE</b>	The KIE Server mode. Valid values are 'DEVELOPMENT' or 'PRODUCTION'. In production mode, you can not deploy SNAPSHOT versions of artifacts on the KIE server and can not change the version of an artifact in an existing container. (Sets the org.kie.server.mode system property).	<b>PRODUCTION</b>	False
<b>KIE_MBEANS</b>	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	enabled	False
<b>DROOLS_SERVER_FILTER_CLASSES</b>	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	true	False
<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_HOSTNAME_HTTP</b>	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure- <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HOSTNAME_HTTPS</b>	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver- <project>.<default-domain-suffix>	–	False
<b>KIE_SERVER_HTTPS_SECRET</b>	–	The name of the secret containing the keystore file.	kieserver-app-secret	True
<b>KIE_SERVER_HTTPS_KEYSTORE</b>	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	keystore.jks	False
<b>KIE_SERVER_HTTPS_NAME</b>	<b>HTTPS_NAME</b>	The name associated with the server certificate.	jboss	False
<b>KIE_SERVER_HTTPS_PASSWORD</b>	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	mykeystorepass	False
<b>KIE_SERVER_BYPASS_AUTH_USER</b>	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer database data-store service.	30000	False
<b>KIE_SERVER_MEMORY_LIMIT</b>	–	KIE server Container memory limit.	1Gi	False
<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version  c2(alias2)=g2:a2:v2	rhpm-kieserver-library=org.openshift.quickstarts:rhpm-kieserver-library:1.5.0-SNAPSHOT	False
<b>KIE_SERVER_MGMT_DISABLED</b>	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped sets the property org.kie.server.management.api.disabled to true and org.kie.server.startup.strategy to LocalContainersStartupStrategy.	true	False
<b>SSO_URL</b>	<b>SSO_URL</b>	RH-SSO URL.	<a href="https://rh-sso.example.com/auth">https://rh-sso.example.com/auth</a>	False
<b>SSO_REALM</b>	<b>SSO_REALM</b>	RH-SSO Realm name.	–	False
<b>KIE_SERVER_SSO_CLIENT</b>	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	–	False



Variable name	Image Environment Variable	Description	Example value	Required
<b>KIE_SERVER_SSO_SECRET</b>	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False
<b>SSO_USERNAME</b>	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False
<b>SSO_PASSWORD</b>	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	–	False
<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	false	False
<b>SSO_PRINCIPAL_ATTRIBUTE</b>	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	preferred_username	False
<b>AUTH_LDAP_URL</b>	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	ldap://myldap.example.com	False
<b>AUTH_LDAP_BIND_DN</b>	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	uid=admin,ou=users,ou=example,ou=com	False
<b>AUTH_LDAP_BIND_CREDENTIAL</b>	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	Password	False
<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
<b>AUTH_LDAP_BASE_CTX_DN</b>	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=example,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_B ASE_FILTER</b>	<b>AUTH_LDAP_B ASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid={0}).	(uid={0})	False
<b>AUTH_LDAP_S EARCH_SCOPE</b>	<b>AUTH_LDAP_S EARCH_SCOPE</b>	The search scope to use.	<b>SUBTREE_SCO PE</b>	False
<b>AUTH_LDAP_S EARCH_TIME_L IMIT</b>	<b>AUTH_LDAP_S EARCH_TIME_L IMIT</b>	The timeout in milliseconds for user or role searches.	10000	False
<b>AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE</b>	<b>AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	distinguishedNam e	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_PARSE_USERNAME</b>	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	true	False
<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False
<b>AUTH_LDAP_USERNAME_END_STRING</b>	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	memberOf	False
<b>AUTH_LDAP_ROLES_CTX_DN</b>	<b>AUTH_LDAP_ROLES_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	ou=groups,ou=example,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_FILTER</b>	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member={0}). An alternative that matches on the authenticated userDN is (member={1}).	(memberOf={1})	False
<b>AUTH_LDAP_ROLE_RECURSION</b>	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
<b>AUTH_LDAP_DEFAULT_ROLE</b>	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users	user	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	name	False
<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttribute ID. If set to true, the DN is checked for the roleNameAttribute ID. If set to false, the DN is not checked for the roleNameAttribute ID. This flag can improve the performance of LDAP queries.	false	False
<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttribute Id attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	<b>AUTH_LDAP_REFERRAL_USE_R_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	–	False
<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	–	False
<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	–	False

## 5.6.2. Objects

The CLI supports various object types. A list of these object types as well as their abbreviations can be found in the [OpenShift documentation](#).

### 5.6.2.1. Services

A service is an abstraction which defines a logical set of pods and a policy by which to access them. Refer to the [container-engine documentation](#) for more information.

Service	Port	Name	Description
<b>\${APPLICATION_NAME}-kieserver</b>	8080	http	All the KIE server web server's ports.
	8443	https	
<b>\${APPLICATION_NAME}-kieserver-ping</b>	8888	ping	The JGroups ping port for clustering.
<b>\${APPLICATION_NAME}-postgresql</b>	5432	–	The database server's port.

### 5.6.2.2. Routes

A route is a way to expose a service by giving it an externally-reachable hostname such as **www.example.com**. A defined route and the endpoints identified by its service can be consumed by a router to provide named connectivity from external clients to your applications. Each route consists of a route name, service selector, and (optionally) security configuration. Refer to the [OpenShift documentation](#) for more information.

Service	Security	Hostname
insecure- <b>\${APPLICATION_NAME}-kieserver-http</b>	none	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
<b>\${APPLICATION_NAME}-kieserver-https</b>	TLS passthrough	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>

### 5.6.2.3. Deployment Configurations

A deployment in OpenShift is a replication controller based on a user defined template called a deployment configuration. Deployments are created manually or in response to triggered events. Refer to the [OpenShift documentation](#) for more information.

#### 5.6.2.3.1. Triggers

A trigger drives the creation of new deployments in response to events, both inside and outside OpenShift. Refer to the [OpenShift documentation](#) for more information.



Deployment	Triggers
<b><code>\${APPLICATION_NAME}-kieserver</code></b>	ImageChange
<b><code>\${APPLICATION_NAME}-postgresql</code></b>	ImageChange

#### 5.6.2.3.2. Replicas

A replication controller ensures that a specified number of pod "replicas" are running at any one time. If there are too many, the replication controller kills some pods. If there are too few, it starts more. Refer to the [container-engine documentation](#) for more information.

Deployment	Replicas
<b><code>\${APPLICATION_NAME}-kieserver</code></b>	1
<b><code>\${APPLICATION_NAME}-postgresql</code></b>	1

#### 5.6.2.3.3. Pod Template

##### 5.6.2.3.3.1. Service Accounts

Service accounts are API objects that exist within each project. They can be created or deleted like any other API object. Refer to the [Openshift documentation](#) for more information.

Deployment	Service Account
<b><code>\${APPLICATION_NAME}-kieserver</code></b>	<b><code>\${APPLICATION_NAME}-kieserver</code></b>

##### 5.6.2.3.3.2. Image

Deployment	Image
<b><code>\${APPLICATION_NAME}-kieserver</code></b>	<b><code>\${KIE_SERVER_IMAGE_STREAM_NAME}</code></b>
<b><code>\${APPLICATION_NAME}-postgresql</code></b>	postgresql

##### 5.6.2.3.3.3. Readiness Probe

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

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

###### `${APPLICATION_NAME}-postgresql`

`/usr/libexec/check-container`

## 5.6.2.3.3.4. Liveness Probe

`${APPLICATION_NAME}-kieserver``Http Get on http://localhost:8080/services/rest/server/healthcheck``${APPLICATION_NAME}-postgresql``/usr/libexec/check-container --live`

## 5.6.2.3.3.5. Exposed Ports

Deployments	Name	Port	Protocol
<b>\${APPLICATION_NAME}-kieserver</b>	jolokia	8778	<b>TCP</b>
	http	8080	<b>TCP</b>
	https	8443	<b>TCP</b>
	ping	8888	<b>TCP</b>
<b>\${APPLICATION_NAME}-postgresql</b>	–	5432	<b>TCP</b>

## 5.6.2.3.3.6. Image Environment Variables

Deployment	Variable name	Description	Example value
<b>\${APPLICATION_NAME}-kieserver</b>	<b>WORKBENCH_SERVICE_NAME</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>\${BUSINESS_CENTRAL_SERVICE}</b>
	<b>KIE_ADMIN_USER</b>	KIE administrator username.	<b>\${KIE_ADMIN_USER}</b>
	<b>KIE_ADMIN_PWD</b>	KIE administrator password.	<b>\${KIE_ADMIN_PWD}</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_MODE</b>	The KIE Server mode. Valid values are 'DEVELOPMENT' or 'PRODUCTION'. In production mode, you can not deploy SNAPSHOT versions of artifacts on the KIE server and can not change the version of an artifact in an existing container. (Sets the org.kie.server.mode system property).	<b>\${KIE_SERVER_MODE}</b>
	<b>KIE_MBEANS</b>	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	<b>\${KIE_MBEANS}</b>
	<b>DROOLS_SERVER_FILTER_CLASSES</b>	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	<b>\${DROOLS_SERVER_FILTER_CLASSES}</b>
	<b>PROMETHEUS_SERVER_EXT_DISABLED</b>	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	<b>\${PROMETHEUS_SERVER_EXT_DISABLED}</b>
	<b>KIE_SERVER_BYPASS_AUTH_USER</b>	Allows the KIE server to bypass the authenticated user for task-related operations, for example, queries. (Sets the org.kie.server.bypass.auth.user system property)	<b>\${KIE_SERVER_BYPASS_AUTH_USER}</b>
	<b>KIE_SERVER_ID</b>	–	–
	<b>KIE_SERVER_ROUTE_NAME</b>	–	<b>\${APPLICATION_NAME}-kieserver</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_USER</b>	KIE server username. (Sets the org.kie.server.user system property)	<b>`\${KIE_SERVER_USER}`</b>
	<b>KIE_SERVER_PWD</b>	KIE server password. (Sets the org.kie.server.pwd system property)	<b>`\${KIE_SERVER_PWD}`</b>
	<b>KIE_SERVER_CONTAINER_DEPLOYMENT</b>	KIE Server Container deployment configuration with optional alias. Format: containerId=groupId:artifactId:version c2(alias2)=g2:a2:v2	<b>`\${KIE_SERVER_CONTAINER_DEPLOYMENT}`</b>
	<b>MAVEN_MIRROR_URL</b>	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for deploying your services.	<b>`\${MAVEN_MIRROR_URL}`</b>
	<b>MAVEN_MIRROR_OFF</b>	Maven mirror configuration for KIE server.	<b>`\${MAVEN_MIRROR_OFF}`</b>
	<b>MAVEN_REPOS</b>	–	RHPAMCENTR,EXTERNAL
	<b>RHPAMCENTR_MAVEN_REPO_ID</b>	–	repo-rhpamcentr
	<b>RHPAMCENTR_MAVEN_REPO_SERVICE</b>	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	<b>`\${BUSINESS_CENTRAL_SERVICE}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PATH</b>	–	<b>/maven2/</b>

Deployment	Variable name	Description	Example value
	<b>RHPAMCENTR_MAVEN_REPO_USERNAME</b>	Username to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_USERNAME}`</b>
	<b>RHPAMCENTR_MAVEN_REPO_PASSWORD</b>	Password to access the Maven service hosted by Business Central inside EAP.	<b>`\${BUSINESS_CENTRAL_MAVEN_PASSWORD}`</b>
	<b>EXTERNAL_MAVEN_REPO_ID</b>	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	<b>`\${MAVEN_REPO_ID}`</b>
	<b>EXTERNAL_MAVEN_REPO_URL</b>	Fully qualified URL to a Maven repository or service.	<b>`\${MAVEN_REPO_URL}`</b>
	<b>EXTERNAL_MAVEN_REPO_USERNAME</b>	Username to access the Maven repository, if required.	<b>`\${MAVEN_REPO_USERNAME}`</b>
	<b>EXTERNAL_MAVEN_REPO_PASSWORD</b>	Password to access the Maven repository, if required.	<b>`\${MAVEN_REPO_PASSWORD}`</b>

Deployment	Variable name	Description	Example value
	<b>KIE_SERVER_MGMT_DISABLED</b>	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped sets the property org.kie.server.mgmt.api.disabled to true and org.kie.server.startup.strategy to LocalContainersStartupStrategy.	<b>`\${KIE_SERVER_MGMT_DISABLED}`</b>
	<b>KIE_SERVER_STARTUP_STRATEGY</b>	–	OpenShiftStartupStrategy
	<b>KIE_SERVER_PERSISTENCE_DS</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	<b>`\${KIE_SERVER_PERSISTENCE_DS}`</b>
	<b>DATASOURCES</b>	–	<b>RHPAM</b>
	<b>RHPAM_DATABASE</b>	KIE server PostgreSQL database name.	<b>`\${KIE_SERVER_POSTGRES_DB}`</b>
	<b>RHPAM_DRIVER</b>	–	postgresql
	<b>RHPAM_USERNAME</b>	KIE server PostgreSQL database username.	<b>`\${KIE_SERVER_POSTGRES_USER}`</b>
	<b>RHPAM_PASSWORD</b>	KIE server PostgreSQL database password.	<b>`\${KIE_SERVER_POSTGRES_PWD}`</b>
	<b>RHPAM_SERVICE_HOST</b>	–	<b>`\${APPLICATION_NAME}`-postgresql</b>
	<b>RHPAM_SERVICE_PORT</b>	–	5432
	<b>KIE_SERVER_PERSISTENCE_DIALECT</b>	KIE server PostgreSQL Hibernate dialect.	<b>`\${KIE_SERVER_POSTGRES_DIALECT}`</b>
	<b>RHPAM_JTA</b>	–	true

Deployment	Variable name	Description	Example value
	<b>RHPAM_JNDI</b>	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	<b>`\${KIE_SERVER_PERSISTENCE_DS}`</b>
	<b>RHPAM_CONNECTION_CHECKER</b>	–	org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLValidConnectionChecker
	<b>RHPAM_EXCEPTION_SORTER</b>	–	org.jboss.jca.adapters.jdbc.extensions.postgres.PostgreSQLExceptionHandler
	<b>TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL</b>	Sets refresh-interval for the EJB timer database data-store service.	<b>`\${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}`</b>
	<b>HTTPS_KEYSTORE_DIR</b>	–	<b>/etc/kieserver-secret-volume</b>
	<b>HTTPS_KEYSTORE</b>	The name of the keystore file within the secret.	<b>`\${KIE_SERVER_HTTPS_KEYSTORE}`</b>
	<b>HTTPS_NAME</b>	The name associated with the server certificate.	<b>`\${KIE_SERVER_HTTPS_NAME}`</b>
	<b>HTTPS_PASSWORD</b>	The password for the keystore and certificate.	<b>`\${KIE_SERVER_HTTPS_PASSWORD}`</b>
	<b>JGROUPS_PING_PROTOCOL</b>	–	opensift.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

Deployment	Variable name	Description	Example value
	<b>SSO_REALM</b>	RH-SSO Realm name.	<b>\${SSO_REALM}</b>
	<b>SSO_SECRET</b>	KIE Server RH-SSO Client Secret.	<b>\${KIE_SERVER_SSO_SECRET}</b>
	<b>SSO_CLIENT</b>	KIE Server RH-SSO Client name.	<b>\${KIE_SERVER_SSO_CLIENT}</b>
	<b>SSO_USERNAME</b>	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	<b>\${SSO_USERNAME}</b>
	<b>SSO_PASSWORD</b>	RH-SSO Realm Admin Password used to create the Client.	<b>\${SSO_PASSWORD}</b>
	<b>SSO_DISABLE_SSL_CERTIFICATE_VALIDATION</b>	RH-SSO Disable SSL Certificate Validation.	<b>\${SSO_DISABLE_SSL_CERTIFICATE_VALIDATION}</b>
	<b>SSO_PRINCIPAL_ATTRIBUTE</b>	RH-SSO Principal Attribute to use as username.	<b>\${SSO_PRINCIPAL_ATTRIBUTE}</b>
	<b>HOSTNAME_HTTP</b>	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	<b>\${KIE_SERVER_HOSTNAME_HTTP}</b>
	<b>HOSTNAME_HTTPS</b>	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	<b>\${KIE_SERVER_HOSTNAME_HTTPS}</b>
	<b>AUTH_LDAP_URL</b>	LDAP Endpoint to connect for authentication.	<b>\${AUTH_LDAP_URL}</b>



Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_BIND_DN</b>	Bind DN used for authentication.	<b><code>\${AUTH_LDAP_BIND_DN}</code></b>
	<b>AUTH_LDAP_BIND_CREDENTIAL</b>	LDAP Credentials used for authentication.	<b><code>\${AUTH_LDAP_BIND_CREDENTIAL}</code></b>
	<b>AUTH_LDAP_JAAS_SECURITY_DOMAIN</b>	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	<b><code>\${AUTH_LDAP_JAAS_SECURITY_DOMAIN}</code></b>
	<b>AUTH_LDAP_BASE_CTX_DN</b>	LDAP Base DN of the top-level context to begin the user search.	<b><code>\${AUTH_LDAP_BASE_CTX_DN}</code></b>
	<b>AUTH_LDAP_BASE_FILTER</b>	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a <code>{0}</code> expression is used. A common example for the search filter is <code>(uid={0})</code> .	<b><code>\${AUTH_LDAP_BASE_FILTER}</code></b>
	<b>AUTH_LDAP_SEARCH_SCOPE</b>	The search scope to use.	<b><code>\${AUTH_LDAP_SEARCH_SCOPE}</code></b>
	<b>AUTH_LDAP_SEARCH_TIME_LIMIT</b>	The timeout in milliseconds for user or role searches.	<b><code>\${AUTH_LDAP_SEARCH_TIME_LIMIT}</code></b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE</b>	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	<b>\${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}</b>
	<b>AUTH_LDAP_PARSE_USERNAME</b>	A flag indicating if the DN is to be parsed for the username. If set to true, the DN is parsed for the username. If set to false the DN is not parsed for the username. This option is used together with <code>usernameBeginString</code> and <code>usernameEndString</code> .	<b>\${AUTH_LDAP_PARSE_USERNAME}</b>
	<b>AUTH_LDAP_USERNAME_BEGIN_STRING</b>	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b>\${AUTH_LDAP_USERNAME_BEGIN_STRING}</b>
	<b>AUTH_LDAP_USERNAME_END_STRING</b>	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with <code>usernameEndString</code> and only taken into account if <code>parseUsername</code> is set to true.	<b>\${AUTH_LDAP_USERNAME_END_STRING}</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_ID</b>	Name of the attribute containing the user roles.	<b>`\${AUTH_LDAP_ROLE_ATTRIBUTE_ID}`</b>
	<b>AUTH_LDAP_ROLE_S_CTX_DN</b>	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	<b>`\${AUTH_LDAP_ROLE_S_CTX_DN}`</b>
	<b>AUTH_LDAP_ROLE_FILTER</b>	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a <code>{0}</code> expression is used. The authenticated userDN is substituted into the filter anywhere a <code>{1}</code> is used. An example search filter that matches on the input username is <code>(member={0})</code> . An alternative that matches on the authenticated userDN is <code>(member={1})</code> .	<b>`\${AUTH_LDAP_ROLE_FILTER}`</b>
	<b>AUTH_LDAP_ROLE_RECURSION</b>	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	<b>`\${AUTH_LDAP_ROLE_RECURSION}`</b>
	<b>AUTH_LDAP_DEFAULT_ROLE</b>	A role included for all authenticated users	<b>`\${AUTH_LDAP_DEFAULT_ROLE}`</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID</b>	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributesDN property is set to true, this property is used to find the role object's name attribute.	<b>\${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}</b>
	<b>AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN</b>	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	<b>\${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}</b>
	<b>AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN</b>	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeID attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	<b>\${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}</b>

Deployment	Variable name	Description	Example value
	<b>AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK</b>	If you are not using referrals, you can ignore this option. When using referrals, this option denotes the attribute name which contains users defined for a certain role, for example member, if the role object is inside the referral. Users are checked against the content of this attribute name. If this option is not set, the check will always fail, so role objects cannot be stored in a referral tree.	<b>`\${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}`</b>
	<b>AUTH_ROLE_MAPPER_ROLES_PROPERTIES</b>	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,role3	<b>`\${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}`</b>
	<b>AUTH_ROLE_MAPPER_REPLACE_ROLE</b>	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	<b>`\${AUTH_ROLE_MAPPER_REPLACE_ROLE}`</b>
<b>`\${APPLICATION_NAME}`-postgresql</b>	<b>POSTGRESQL_USER</b>	KIE server PostgreSQL database username.	<b>`\${KIE_SERVER_POSTGRESQL_USER}`</b>
	<b>POSTGRESQL_PASSWORD</b>	KIE server PostgreSQL database password.	<b>`\${KIE_SERVER_POSTGRESQL_PWD}`</b>
	<b>POSTGRESQL_DATABASE</b>	KIE server PostgreSQL database name.	<b>`\${KIE_SERVER_POSTGRESQL_DB}`</b>

Deployment	Variable name	Description	Example value
	<b>POSTGRESQL_MAX_PREPARED_TRANSACTIONS</b>	Allows the PostgreSQL to handle XA transactions.	<b>\${POSTGRESQL_MAX_PREPARED_TRANSACTIONS}</b>

#### 5.6.2.3.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
<b>\${APPLICATION_NAME}-kieserver</b>	kieserver-keystore-volume	<b>/etc/kieserver-secret-volume</b>	ssl certs	True
<b>\${APPLICATION_NAME}-postgresql</b>	<b>\${APPLICATION_NAME}-postgresql-pvol</b>	<b>/var/lib/pgsql/data</b>	postgresql	false

#### 5.6.2.4. External Dependencies

##### 5.6.2.4.1. Volume Claims

A **PersistentVolume** object is a storage resource in an OpenShift cluster. Storage is provisioned by an administrator by creating **PersistentVolume** objects from sources such as GCE Persistent Disks, AWS Elastic Block Stores (EBS), and NFS mounts. Refer to the [OpenShift documentation](#) for more information.

Name	Access Mode
<b>\${APPLICATION_NAME}-postgresql-claim</b>	ReadWriteOnce

##### 5.6.2.4.2. Secrets

This template requires the following secrets to be installed for the application to run.

kieserver-app-secret

## 5.7. OPENSIFT USAGE QUICK REFERENCE

To deploy, monitor, manage, and undeploy Red Hat Process Automation Manager templates on Red Hat OpenShift Container Platform, you can use the OpenShift Web console or the **oc** command.

For instructions about using the Web console, see [Create and build an image using the Web console](#).

For detailed instructions about using the **oc** command, see [CLI Reference](#). The following commands are likely to be required:

- To create a project, use the following command:

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

For more information, see [Creating a project using the CLI](#).

- To deploy a template (create an application from a template), use the following command:

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

For more information, see [Creating an application using the CLI](#).

- To view a list of the active pods in the project, use the following command:

```
$ oc get pods
```

- To view the current status of a pod, including information whether or not the pod deployment has completed and it is now in a running state, use the following command:

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

You can also use the **oc describe** command to view the current status of other objects. For more information, see [Application modification operations](#).

- To view the logs for a pod, use the following command:

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

- To view deployment logs, look up a **DeploymentConfig** name in the template reference and enter the following command:

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

For more information, see [Viewing deployment logs](#).

- To view build logs, look up a **BuildConfig** name in the template reference and enter the command:

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

For more information, see [Accessing build logs](#).

- To scale a pod in the application, look up a **DeploymentConfig** name in the template reference and enter the command:

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

For more information, see [Manual scaling](#).

- To undeploy the application, you can delete the project by using the command:

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

Alternatively, you can use the **oc delete** command to remove any part of the application, such as a pod or replication controller. For details, see [Application modification operations](#).

## APPENDIX A. VERSIONING INFORMATION

Documentation last updated on Friday, June 25, 2021.