Red Hat Process Automation Manager 7.4

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

Red Hat Process Automation Manager 7.4 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

Legal Notice

Abstract

This document describes how to deploy a Red Hat Process Automation Manager 7.4 immutable server environment on Red Hat OpenShift Container Platform.

Table of Contents

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

- 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.

CHAPTER 1. OVERVIEW OF RED HAT PROCESS AUTOMATION MANAGER ON RED HAT OPENSHIFT 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 connects 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 OPENSHIFT 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 rhpam74-businesscentral
   $ oc get imagestreamtag -n openshift | grep rhpam74-kieserver
   ```

   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 **rhpam-7.4.0-openshift-templates.zip** product deliverable file from the Software Downloads page and extract the **rhpam74-image-streams.yaml** file.

g. Complete one of the following actions:

- Enter the following command:

```
$ oc create -f rhpam74-image-streams.yaml
```

- In the OpenShift Web UI, select **Add to Project → Import YAML / JSON**and then choose the file or paste its contents.

> **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 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 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 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 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. CHANGING GLUSTERFS CONFIGURATION

You must check whether your OpenShift environment uses GlusterFS to provide permanent storage volumes. If it uses GlusterFS, to ensure optimal performance, you must tune your GlusterFS storage by changing the storage class configuration.

Procedure

1. To check whether your environment uses GlusterFS, enter the following command:

```
oc get storageclass
```

In the results, check whether the **(default)** marker is on the storage class that lists **glusterfs**. For example, in the following output the default storage class is **gluster-container**, which does list **glusterfs**:

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

If the result has a default storage class that does not list **glusterfs** or if the result is empty, you do not need to make any changes. In this case, skip the rest of this procedure.

2. To save the configuration of the default storage class into a YAML file, enter the following command:

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

Replace **<class-name>** with the name of the default storage class. Example:

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

3. Edit the **storage_config.yaml** file:

   a. Remove the lines with the following keys:

- **creationTimestamp**

- **resourceVersion**

- **selfLink**

- **uid**

b. On the line with the **volumeoptions** key, add the following two options: **features.cache-invalidation on, performance.nl-cache on**. Example:

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

4. To remove the existing default storage class, enter the following command:

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

Replace **<class-name>** with the name of the default storage class. Example:

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

5. To re-create the storage class using the new configuration, enter the following command:

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

2.6. 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 **EXTENSIONS_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

  - Cekit version 3.2

  - The following libraries and extensions for Cekit:

    - **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-7.4.0-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.

7. 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.

2.7. 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

1. Use the following command to extract the source code:

> git clone ssh://<adminUser>@<business-central-host>:8001/<MySpace>/<MyProject>

In this command, replace the following variables:

   - **<adminUser>** with the administrative user for Business Central

   - **<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

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

2.8. 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 **rhpam-7.4.0-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 rhpam-7.4.0-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. If the tool reports failed downloads, enter the following commands to download the artifacts that failed to download the first time:

   ```
   grep Path: errors.log | sed -n -e 's/^.*Path: //p' > failed-downloads.txt
   java -jar offliner-<version>.jar -r https://maven.repository.redhat.com/ga/ -r
   https://repo1.maven.org/maven2/ -d /home/user/temp failed-downloads.txt
   ```

   If failures are reported again and are a minority of the total number downloaded the first time, you can proceed.

   e. 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 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 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 **rhpam74-immutable-monitor.yaml** template file.

Procedure

1. Download the **rhpam-7.4.0-openshift-templates.zip** product deliverable file from the Software Downloads page of the Red Hat Customer Portal.

2. Extract the **rhpam74-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 **rhpam74-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>/rhpam74-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" .

   - 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" .

   - 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.

   - 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

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 **rhpam74-prod-immutable-kieserver-amq.yaml** template file if you want to enable JMS capabilities. Otherwise, use the **rhpam74-prod-immutable-kieserver.yaml** template file.

Procedure

1. Download the **rhpam-7.4.0-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>/&lt;template-file-name&gt;.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

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>**. You can provide two or more KJAR files using the **|** separator, as illustrated in the following example:

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

  If the **KIE_SERVER_CONTAINER_DEPLOYMENT** value is not defined, the server discovers the group ID, artifact ID, and version of the artifacts by inspecting the **pom.xml** file of your project and uses the artifact ID as the container ID. 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.
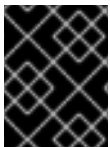
Next steps

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 2.8, "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 2.8, "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 **rhpam74-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 **rhpam74-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 2.6, "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 **rhpam74-prod-immutable-kieserver.yaml** or **rhpam74-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, staring 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 **rhpam74-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 **rhpam74-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 **rhpam74-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 **rhpam74-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**
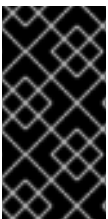
> **IMPORTANT**
>
> The standard Process Server image includes drivers for MySQL and PostgreSQL external database servers. If you want to use another database server, you must build a custom Process Server image. For instructions, see Section 2.6, "Building a custom Process Server extension image for 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:

- **rhpam74-kieserver-postgresql.yaml** to use a PostgreSQL pod for persistent storage. Use this template unless you have a specific reason to use another template.

- **rhpam74-kieserver-mysql.yaml** to use a MySQL pod for persistent storage.

- **rhpam74-kieserver-externaldb.yaml** to use an external database server for persistent storage.
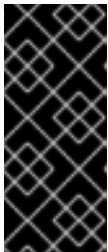
> **IMPORTANT**
>
> The standard Process Server image for an external database server includes drivers for MySQL and PostgreSQL external database servers. If you want to use another database server, you must build a custom Process Server image. For instructions, see Section 2.6, "Building a custom Process Server extension image for an external database".

Procedure

1. Download the **rhpam-7.4.0-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>/&lt;template-file-name&gt;.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>**. You can provide two or more KJAR files using the |separator, as illustrated in the following example:

> containerId=groupId:artifactId:version|c2=g2:a2:v2

- KIE Server Mode(**KIE_SERVER_MODE**): In the **rhpam74-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 froh 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 2.8, "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 2.8, "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 .

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

If you are using the **rhpam74-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 .

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 2.6, "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.
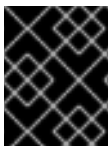
Next steps

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 JBoss Developer 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. OPENSHIFT TEMPLATE REFERENCE INFORMATION

Red Hat Process Automation Manager provides the following OpenShift templates. To access the templates, download and extract the **rhpam-7.4.0-openshift-templates.zip** product deliverable file from the Software Downloads page of the Red Hat customer portal.

- **rhpam74-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 **rhpam74-prod-immutable-kieserver.yaml** template. For details about this template, see Section 5.1, "rhpam74-prod-immutable-monitor.yaml template".

- **rhpam74-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 **rhpam74-prod-immutable-monitor.yaml**. For details about this template, see Section 5.2, "rhpam74-prod-immutable-kieserver.yaml template".

- **rhpam74-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 **rhpam74-prod-immutable-monitor.yaml**. This version of the template includes JMS integration. For details about this template, see Section 5.3, "rhpam74-prod-immutable-kieserver-amq.yaml template".

- **rhpam74-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, "rhpam74-kieserver-externaldb.yaml template".

- **rhpam74-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, "rhpam74-kieserver-mysql.yaml template".

- **rhpam74-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, "rhpam74-kieserver-mysql.yaml template".

5.1. RHPAM74-PROD-IMMUTABLE-MONITOR.YAML TEMPLATE

Application template for a router and monitoring console in a production environment, for Red Hat Process Automation Manager 7.4

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
APPLICATION_ NAME	–	The name for the application.	myapp	True
MAVEN_REPO_I D	**EXTERNAL_MA VEN_REPO_ID**	The id to use for the maven repository, if set. Default is generated randomly.	repo-custom	False
MAVEN_REPO_ URL	**EXTERNAL_MA VEN_REPO_UR L**	Fully qualified URL to a Maven repository or service.	http://nexus.nexu s-project.svc.cluster. local:8081/nexus/ content/groups/p ublic/	False
MAVEN_REPO_ USERNAME	**EXTERNAL_MA VEN_REPO_US ERNAME**	Username to access the Maven repository, if required.	–	False
MAVEN_REPO_ PASSWORD	**EXTERNAL_MA VEN_REPO_PA SSWORD**	Password to access the Maven repository, if required.	–	False
BUSINESS_CEN TRAL_SERVICE	**RHPAMCENTR_ MAVEN_REPO_ SERVICE**	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
BUSINESS_CEN TRAL_MAVEN_ USERNAME	**RHPAMCENTR_ MAVEN_REPO_ USERNAME**	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False

Variable name	Image Environment Variable	Description	Example value	Required
BUSINESS_CEN TRAL_MAVEN_ PASSWORD	**RHPAMCENTR_ MAVEN_REPO_ PASSWORD**	Password to access the Maven service hosted by Business Central inside EAP.	maven1!	False
KIE_ADMIN_US ER	**KIE_ADMIN_US ER**	KIE administrator username	adminUser	False
KIE_ADMIN_PW D	**KIE_ADMIN_PW D**	KIE administrator password	–	False
KIE_SERVER_U SER	**KIE_SERVER_U SER**	KIE server username (Sets the org.kie.server.user system property)	executionUser	False
KIE_SERVER_P WD	**KIE_SERVER_P WD**	KIE server password, used to connect to KIE servers. Value is automatically generated by default. (Sets the org.kie.server.pwd system property)	–	False
KIE_SERVER_C ONTROLLER_O PENSHIFT_GLO BAL_DISCOVE RY_ENABLED	**KIE_SERVER_C ONTROLLER_O PENSHIFT_GLO BAL_DISCOVE RY_ENABLED**	If set to true, turns on KIE server global discovery feature (Sets the org.kie.server.cont roller.openshift.glo bal.discovery.enabl ed system property)	false	False

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE	**KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE**	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 org.kie.server.controller.openshift.prefer.kieserver.service system property)	true	False
KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL	**KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL**	KIE ServerTemplate Cache TTL in milliseconds (Sets the org.kie.server.controller.template.cache.ttl system property)	60000	False
IMAGE_STREAM_NAMESPACE	–	Namespace in which the ImageStreams for Red Hat Middleware 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
IMAGE_STREAM_TAG	–	A named pointer to an image in an image stream. Default is "1.0".	1.0	False

Variable name	Image Environment Variable	Description	Example value	Required
SMART_ROUTER_HOSTNAME_HTTP	–	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-smartrouter-<project>.<default-domain-suffix>	–	False
SMART_ROUTER_HOSTNAME_HTTPS	–	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-smartrouter-<project>.<default-domain-suffix>	–	False
KIE_SERVER_ROUTER_ID	KIE_SERVER_ROUTER_ID	Router ID used when connecting to the controller. (Router property org.kie.server.router.id)	kie-server-router	True
KIE_SERVER_ROUTER_PROTOCOL	KIE_SERVER_ROUTER_PROTOCOL	KIE server router protocol. (Used to build the org.kie.server.router.url.external property)	http	False
KIE_SERVER_ROUTER_URL_EXTERNAL	KIE_SERVER_ROUTER_URL_EXTERNAL	Public URL where the router can be found. Format http://<host>:<port> (Router property org.kie.server.router.url.external)	–	False

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_ROUTER_NAME	**KIE_SERVER_ROUTER_NAME**	Router name used when connecting to the controller. (Router property org.kie.server.router.name)	KIE Server Router	True
KIE_SERVER_ROUTER_HTTPS_SECRET	–	The name of the secret containing the keystore file.	smartrouter-app-secret	True
KIE_SERVER_ROUTER_HTTPS_KEYSTORE	–	The name of the keystore file within the secret.	keystore.jks	False
KIE_SERVER_ROUTER_HTTPS_NAME	**KIE_SERVER_ROUTER_TLS_KEYSTORE_KEY ALIAS**	The name associated with the server certificate.	jboss	False
KIE_SERVER_ROUTER_HTTPS_PASSWORD	**KIE_SERVER_ROUTER_TLS_KEYSTORE_PASSWORD**	The password for the keystore and certificate.	mykeystorepass	False
KIE_SERVER_MONITOR_USER	**KIE_SERVER_CONTROLLER_USER**	KIE server monitor username. (Sets the org.kie.server.controller.user system property)	monitorUser	False
KIE_SERVER_MONITOR_PWD	**KIE_SERVER_CONTROLLER_PWD**	KIE server monitor password. (Sets the org.kie.server.controller.pwd system property)	–	False

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_M ONITOR_TOKE N	KIE_SERVER_C ONTROLLER_T OKEN	KIE server monitor token for bearer authentication. (Sets the org.kie.server.cont roller.token system property)	–	False
BUSINESS_CEN TRAL_HOSTNA ME_HTTP	HOSTNAME_HT TP	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-rhpamcentrmon-<project>.<default-domain-suffix>	–	False
BUSINESS_CEN TRAL_HOSTNA ME_HTTPS	HOSTNAME_HT TPS	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-rhpamcentrmon-<project>.<default-domain-suffix>	–	False
BUSINESS_CEN TRAL_HTTPS_S ECRET	–	The name of the secret containing the keystore file.	businesscentral-app-secret	True
BUSINESS_CEN TRAL_HTTPS_ KEYSTORE	HTTPS_KEYST ORE	The name of the keystore file within the secret.	keystore.jks	False
BUSINESS_CEN TRAL_HTTPS_ NAME	HTTPS_NAME	The name associated with the server certificate.	jboss	False
BUSINESS_CEN TRAL_HTTPS_P ASSWORD	HTTPS_PASSW ORD	The password for the keystore and certificate.	mykeystorepass	False

Variable name	Image Environment Variable	Description	Example value	Required
BUSINESS_CEN TRAL_MEMORY _LIMIT	–	Business Central Container memory limit.	2Gi	False
SMART_ROUTE R_MEMORY_LI MIT	–	Smart Router Container memory limit.	512Mi	False
SSO_URL	**SSO_URL**	RH-SSO URL.	https://rh-sso.example.com/auth	False
SSO_REALM	**SSO_REALM**	RH-SSO Realm name.	–	False
BUSINESS_CEN TRAL_SSO_CLI ENT	**SSO_CLIENT**	Business Central Monitoring RH-SSO Client name.	–	False
BUSINESS_CEN TRAL_SSO_SE CRET	**SSO_SECRET**	Business Central Monitoring RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False
SSO_USERNAM E	**SSO_USERNAM E**	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False
SSO_PASSWOR D	**SSO_PASSWOR D**	RH-SSO Realm Admin Password used to create the Client.	–	False
SSO_DISABLE_ SSL_CERTIFIC ATE_VALIDATI ON	**SSO_DISABLE_ SSL_CERTIFIC ATE_VALIDATI ON**	RH-SSO Disable SSL Certificate Validation.	false	False
SSO_PRINCIPA L_ATTRIBUTE	**SSO_PRINCIPA L_ATTRIBUTE**	RH-SSO Principal Attribute to use as username.	preferred_userna me	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_U RL	**AUTH_LDAP_U RL**	LDAP Endpoint to connect for authentication.	ldap://myldap.exa mple.com	False
AUTH_LDAP_BI ND_DN	**AUTH_LDAP_BI ND_DN**	Bind DN used for authentication.	uid=admin,ou=user s,ou=exmample,ou =com	False
AUTH_LDAP_BI ND_CREDENTI AL	**AUTH_LDAP_BI ND_CREDENTI AL**	LDAP Credentials used for authentication.	Password	False
AUTH_LDAP_J AAS_SECURITY _DOMAIN	**AUTH_LDAP_J AAS_SECURITY _DOMAIN**	The JMX ObjectName of the JaasSecurityDoma in used to decrypt the password.	–	False
AUTH_LDAP_B ASE_CTX_DN	**AUTH_LDAP_B ASE_CTX_DN**	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=exam ple,ou=com	False
AUTH_LDAP_B ASE_FILTER	**AUTH_LDAP_B ASE_FILTER**	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
AUTH_LDAP_S EARCH_SCOPE	**AUTH_LDAP_S EARCH_SCOPE**	The search scope to use.	**SUBTREE_SCO PE**	False
AUTH_LDAP_S EARCH_TIME_L IMIT	**AUTH_LDAP_S EARCH_TIME_L IMIT**	The timeout in milliseconds for user or role searches.	10000	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE	**AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE**	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
AUTH_LDAP_P ARSE_USERNA ME	**AUTH_LDAP_P ARSE_USERNA ME**	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 usernameBeginStri ng and usernameEndStrin g.	true	False
AUTH_LDAP_U SERNAME_BEG IN_STRING	**AUTH_LDAP_U SERNAME_BEG IN_STRING**	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_USERNAME_END_STRING	AUTH_LDAP_USERNAME_END_STRING	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	–	False
AUTH_LDAP_ROLE_ATTRIBUTE_ID	AUTH_LDAP_ROLE_ATTRIBUTE_ID	Name of the attribute containing the user roles.	memberOf	False
AUTH_LDAP_ROLES_CTX_DN	AUTH_LDAP_ROLES_CTX_DN	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
AUTH_LDAP_ROLE_FILTER	**AUTH_LDAP_ROLE_FILTER**	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
AUTH_LDAP_ROLE_RECURSION	**AUTH_LDAP_ROLE_RECURSION**	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
AUTH_LDAP_DEFAULT_ROLE	**AUTH_LDAP_DEFAULT_ROLE**	A role included for all authenticated users.	user	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_NAME_AT TRIBUTE_ID	**AUTH_LDAP_R OLE_NAME_AT TRIBUTE_ID**	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	name	False
AUTH_LDAP_P ARSE_ROLE_N AME_FROM_DN	**AUTH_LDAP_P ARSE_ROLE_N AME_FROM_DN**	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
AUTH_LDAP_R OLE_ATTRIBUT E_IS_DN	**AUTH_LDAP_R OLE_ATTRIBUT E_IS_DN**	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
AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK	**AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK**	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
AUTH_ROLE_M APPER_ROLES _PROPERTIES	**AUTH_ROLE_M APPER_ROLES _PROPERTIES**	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,r ole2,role3	–	False
AUTH_ROLE_M APPER_REPLA CE_ROLE	**AUTH_ROLE_M APPER_REPLA CE_ROLE**	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
${APPLICATION_NAME}-rhpamcentrmon	8080	http	All the Business Central Monitoring web server's ports.
	8443	https	
${APPLICATION_NAME}-rhpamcentrmon-ping	8888	ping	The JGroups ping port for clustering.
${APPLICATION_NAME}-smartrouter	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-${APPLICATION_NAME}-rhpamcentrmon-http	none	**${BUSINESS_CENTRAL_HOSTNAME_HTTP}**
${APPLICATION_NAME}-rhpamcentrmon-https	TLS passthrough	**${BUSINESS_CENTRAL_HOSTNAME_HTTPS}**
insecure-${APPLICATION_NAME}-smartrouter-http	none	**${SMART_ROUTER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-smartrouter-https	TLS passthrough	**${SMART_ROUTER_HOSTNAME_HTTPS}**

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
${APPLICATION_NAME}-rhpamcentrmon	ImageChange
${APPLICATION_NAME}-smartrouter	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
${APPLICATION_NAME}-rhpamcentrmon	1
${APPLICATION_NAME}-smartrouter	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
${APPLICATION_NAME}-rhpamcentrmon	${APPLICATION_NAME}-rhpamsvc

5.1.2.3.3.2. Image

Deployment	Image
${APPLICATION_NAME}-rhpamcentrmon	rhpam74-businesscentral-monitoring-openshift
${APPLICATION_NAME}-smartrouter	rhpam74-smartrouter-openshift

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
${APPLICATION_NAME}-rhpamcentrmon	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
	ping	8888	**TCP**
${APPLICATION_NAME}-smartrouter	http	9000	**TCP**

5.1.2.3.3.6. Image Environment Variables

Deployment	Variable name	Description	Example value
${APPLICATION_NAME}-rhpamcentrmon	**KIE_ADMIN_PWD**	KIE administrator password	**${KIE_ADMIN_PWD}**
	KIE_ADMIN_USER	KIE administrator username	**${KIE_ADMIN_USER}**
	KIE_SERVER_PWD	KIE server password, used to connect to KIE servers. Value is automatically generated by default. (Sets the org.kie.server.pwd system property)	**${KIE_SERVER_PWD}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_USER	KIE server username (Sets the org.kie.server.user system property)	**${KIE_SERVER_USER}**
	MAVEN_REPOS	–	RHPAMCENTR,EXTERNAL
	RHPAMCENTR_MAVEN_REPO_ID	–	repo-rhpamcentr
	RHPAMCENTR_MAVEN_REPO_SERVICE	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	**${BUSINESS_CENTRAL_SERVICE}**
	RHPAMCENTR_MAVEN_REPO_PATH	–	**/maven2/**
	RHPAMCENTR_MAVEN_REPO_USERNAME	Username to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_USERNAME}**
	RHPAMCENTR_MAVEN_REPO_PASSWORD	Password to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_PASSWORD}**
	EXTERNAL_MAVEN_REPO_ID	The id to use for the maven repository, if set. Default is generated randomly.	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Fully qualified URL to a Maven repository or service.	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Username to access the Maven repository, if required.	**${MAVEN_REPO_USERNAME}**
	EXTERNAL_MAVEN_REPO_PASSWORD	Password to access the Maven repository, if required.	**${MAVEN_REPO_PASSWORD}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED	If set to true, turns on KIE server global discovery feature (Sets the org.kie.server.controller.openshift.global.discovery.enabled system property)	**${KIE_SERVER_CONTROLLER_OPENSHIFT_GLOBAL_DISCOVERY_ENABLED}**
	KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE	If OpenShift integration of Business Central is turned on, setting this parameter to true enables connection to KIE Server via an OpenShift internal Service endpoint. (Sets the org.kie.server.controller.openshift.prefer.kieserver.service system property)	**${KIE_SERVER_CONTROLLER_OPENSHIFT_PREFER_KIESERVER_SERVICE}**
	KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL	KIE ServerTemplate Cache TTL in milliseconds (Sets the org.kie.server.controller.template.cache.ttl system property)	**${KIE_SERVER_CONTROLLER_TEMPLATE_CACHE_TTL}**
	KIE_WORKBENCH_CONTROLLER_OPENSHIFT_ENABLED	–	true
	KIE_SERVER_CONTROLLER_USER	KIE server monitor username. (Sets the org.kie.server.controller.user system property)	**${KIE_SERVER_MONITOR_USER}**
	KIE_SERVER_CONTROLLER_PWD	KIE server monitor password. (Sets the org.kie.server.controller.pwd system property)	**${KIE_SERVER_MONITOR_PWD}**
	KIE_SERVER_CONTROLLER_TOKEN	KIE server monitor token for bearer authentication. (Sets the org.kie.server.controller.token system property)	**${KIE_SERVER_MONITOR_TOKEN}**

Deployment	Variable name	Description	Example value
	HTTPS_KEYSTORE_ DIR	–	**/etc/businesscentral-secret-volume**
	HTTPS_KEYSTORE	The name of the keystore file within the secret.	**${BUSINESS_CENTR AL_HTTPS_KEYSTO RE}**
	HTTPS_NAME	The name associated with the server certificate.	**${BUSINESS_CENTR AL_HTTPS_NAME}**
	HTTPS_PASSWORD	The password for the keystore and certificate.	**${BUSINESS_CENTR AL_HTTPS_PASSW ORD}**
	JGROUPS_PING_PR OTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PI NG_SERVICE_NAME	–	**${APPLICATION_NA ME}-rhpamcentrmon-ping**
	OPENSHIFT_DNS_PI NG_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL.	**${SSO_URL}**
	SSO_OPENIDCONN ECT_DEPLOYMENT S	–	ROOT.war
	SSO_REALM	RH-SSO Realm name.	**${SSO_REALM}**
	SSO_SECRET	Business Central Monitoring RH-SSO Client Secret.	**${BUSINESS_CENTR AL_SSO_SECRET}**
	SSO_CLIENT	Business Central Monitoring RH-SSO Client name.	**${BUSINESS_CENTR AL_SSO_CLIENT}**
	SSO_USERNAME	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	**${SSO_USERNAME}**

Deployment	Variable name	Description	Example value
	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client.	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_ CERTIFICATE_VALI DATION	RH-SSO Disable SSL Certificate Validation.	**${SSO_DISABLE_SS L_CERTIFICATE_VA LIDATION}**
	SSO_PRINCIPAL_AT TRIBUTE	RH-SSO Principal Attribute to use as username.	**${SSO_PRINCIPAL_ ATTRIBUTE}**
	HOSTNAME_HTTP	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-rhpamcentrmon-<project>.<default-domain-suffix>	**${BUSINESS_CENTR AL_HOSTNAME_HT TP}**
	HOSTNAME_HTTPS	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-rhpamcentrmon-<project>.<default-domain-suffix>	**${BUSINESS_CENTR AL_HOSTNAME_HT TPS}**
	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication.	**${AUTH_LDAP_URL}**
	AUTH_LDAP_BIND_ DN	Bind DN used for authentication.	**${AUTH_LDAP_BIND _DN}**
	AUTH_LDAP_BIND_ CREDENTIAL	LDAP Credentials used for authentication.	**${AUTH_LDAP_BIND _CREDENTIAL}**
	AUTH_LDAP_JAAS_ SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	**${AUTH_LDAP_JAA S_SECURITY_DOMA IN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_BASE_ CTX_DN	LDAP Base DN of the top-level context to begin the user search.	**${AUTH_LDAP_BAS E_CTX_DN}**
	AUTH_LDAP_BASE_ FILTER	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid= {0}).	**${AUTH_LDAP_BAS E_FILTER}**
	AUTH_LDAP_SEAR CH_SCOPE	The search scope to use.	**${AUTH_LDAP_SEA RCH_SCOPE}**
	AUTH_LDAP_SEAR CH_TIME_LIMIT	The timeout in milliseconds for user or role searches.	**${AUTH_LDAP_SEA RCH_TIME_LIMIT}**
	AUTH_LDAP_DISTIN GUISHED_NAME_AT TRIBUTE	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.	**${AUTH_LDAP_DIST INGUISHED_NAME_ ATTRIBUTE}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE _USERNAME	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 usernameBeginString and usernameEndString.	**${AUTH_LDAP_PAR SE_USERNAME}**
	AUTH_LDAP_USER NAME_BEGIN_STRI NG	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_BEGIN_STR ING}**
	AUTH_LDAP_USER NAME_END_STRING	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_END_STRIN G}**
	AUTH_LDAP_ROLE_ ATTRIBUTE_ID	Name of the attribute containing the user roles.	**${AUTH_LDAP_ROL E_ATTRIBUTE_ID}**
	AUTH_LDAP_ROLE S_CTX_DN	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.	**${AUTH_LDAP_ROL ES_CTX_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE_ FILTER	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}).	**${AUTH_LDAP_ROL E_FILTER}**
	AUTH_LDAP_ROLE_ RECURSION	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	**${AUTH_LDAP_ROL E_RECURSION}**
	AUTH_LDAP_DEFA ULT_ROLE	A role included for all authenticated users.	**${AUTH_LDAP_DEF AULT_ROLE}**
	AUTH_LDAP_ROLE_ NAME_ATTRIBUTE_I D	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	**${AUTH_LDAP_ROL E_NAME_ATTRIBUT E_ID}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	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.	${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}
	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	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.	${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}
	AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK	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.	${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}

Deployment	Variable name	Description	Example value
	AUTH_ROLE_MAPP ER_ROLES_PROPE RTIES	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,r ole3	**${AUTH_ROLE_MAP PER_ROLES_PROPE RTIES}**
	AUTH_ROLE_MAPP ER_REPLACE_ROLE	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	**${AUTH_ROLE_MAP PER_REPLACE_ROL E}**
${APPLICATION_NA ME}-smartrouter	**KIE_SERVER_ROUT ER_HOST**	–	–
	KIE_SERVER_ROUT ER_PORT	–	9000
	KIE_SERVER_ROUT ER_PORT_TLS	–	9443
	KIE_SERVER_ROUT ER_URL_EXTERNAL	Public URL where the router can be found. Format http://<host>: <port> (Router property org.kie.server.router.url. external)	**${KIE_SERVER_ROU TER_URL_EXTERNA L}**
	KIE_SERVER_ROUT ER_ID	Router ID used when connecting to the controller. (Router property org.kie.server.router.id)	**${KIE_SERVER_ROU TER_ID}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_ROUTER_NAME	Router name used when connecting to the controller. (Router property org.kie.server.router.name)	**${KIE_SERVER_ROUTER_NAME}**
	KIE_SERVER_ROUTER_PROTOCOL	KIE server router protocol. (Used to build the org.kie.server.router.url. external property)	**${KIE_SERVER_ROUTER_PROTOCOL}**
	KIE_SERVER_ROUTER_TLS_KEYSTORE_KEYALIAS	The name associated with the server certificate.	**${KIE_SERVER_ROUTER_HTTPS_NAME}**
	KIE_SERVER_ROUTER_TLS_KEYSTORE_PASSWORD	The password for the keystore and certificate.	**${KIE_SERVER_ROUTER_HTTPS_PASSWORD}**
	KIE_SERVER_ROUTER_TLS_KEYSTORE	–	**/etc/smartrouter-secret-volume/${KIE_SERVER_ROUTER_HTTPS_KEYSTORE}**
	KIE_SERVER_CONTROLLER_USER	KIE server monitor username. (Sets the org.kie.server.controller.user system property)	**${KIE_SERVER_MONITOR_USER}**
	KIE_SERVER_CONTROLLER_PWD	KIE server monitor password. (Sets the org.kie.server.controller.pwd system property)	**${KIE_SERVER_MONITOR_PWD}**
	KIE_SERVER_CONTROLLER_TOKEN	KIE server monitor token for bearer authentication. (Sets the org.kie.server.controller.token system property)	**${KIE_SERVER_MONITOR_TOKEN}**
	KIE_SERVER_CONTROLLER_SERVICE	–	**${APPLICATION_NAME}-rhpamcentrmon**

Deployment	Variable name	Description	Example value
	KIE_SERVER_CONTROLLER_PROTOCOL	–	http
	KIE_SERVER_ROUTER_REPO	–	**/opt/rhpam-smartrouter/data**
	KIE_SERVER_ROUTER_CONFIG_WATCHER_ENABLED	–	true

5.1.2.3.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
${APPLICATION_NAME}-rhpamcentrmon	businesscentral-keystore-volume	**/etc/businesscentral-secret-volume**	ssl certs	True
${APPLICATION_NAME}-smartrouter	**${APPLICATION_NAME}-smartrouter**	**/opt/rhpam-smartrouter/data**	–	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
${APPLICATION_NAME}-smartrouter-claim	ReadWriteMany
${APPLICATION_NAME}-rhpamcentr-claim	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. RHPAM74-PROD-IMMUTABLE-KIESERVER.YAML TEMPLATE

Application template for an immutable KIE server in a production environment, for Red Hat Process Automation Manager 7.4

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
APPLICATION_NAME	–	The name for the application.	myapp	True
KIE_ADMIN_USER	KIE_ADMIN_USER	KIE administrator username.	adminUser	False
KIE_ADMIN_PWD	KIE_ADMIN_PWD	KIE administrator password.	–	False
KIE_SERVER_USER	KIE_SERVER_USER	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False
KIE_SERVER_PWD	KIE_SERVER_PWD	KIE server password, used to connect to KIE servers. Value is automatically generated by default. (Sets the org.kie.server.pwd system property)	–	False

Variable name	Image Environment Variable	Description	Example value	Required
IMAGE_STREA M_NAMESPACE	–	Namespace in which the ImageStreams for Red Hat Middleware 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/projec t.	openshift	True
KIE_SERVER_I MAGE_STREAM _NAME	–	The name of the image stream to use for KIE server. Default is "rhpam74-kieserver-openshift".	rhpam74-kieserver-openshift	True
IMAGE_STREA M_TAG	–	A named pointer to an image in an image stream. Default is "1.0".	1.0	True
KIE_SERVER_P ERSISTENCE_D S	**KIE_SERVER_P ERSISTENCE_D S**	KIE server persistence datasource. (Sets the org.kie.server.persi stence.ds system property)	java:/jboss/dataso urces/rhpam	False

Variable name	Image Environment Variable	Description	Example value	Required
POSTGRESQL_I MAGE_STREAM _NAMESPACE	–	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/projec t. Default is "openshift".	openshift	False
POSTGRESQL_I MAGE_STREAM _TAG	–	The PostgreSQL image version, which is intended to correspond to the PostgreSQL version. Default is "10".	10	False
KIE_SERVER_P OSTGRESQL_U SER	**RHPAM_USERN AME**	KIE server PostgreSQL database username.	rhpam	False
KIE_SERVER_P OSTGRESQL_P WD	**RHPAM_PASSW ORD**	KIE server PostgreSQL database password.	–	False
KIE_SERVER_P OSTGRESQL_D B	**RHPAM_DATAB ASE**	KIE server PostgreSQL database name.	rhpam7	False
POSTGRESQL_ MAX_PREPARE D_TRANSACTI ONS	**POSTGRESQL_ MAX_PREPARE D_TRANSACTI ONS**	Allows the PostgreSQL to handle XA transactions.	100	True
DB_VOLUME_C APACITY	–	Size of persistent storage for the database volume.	1Gi	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_P OSTGRESQL_D IALECT	**KIE_SERVER_P ERSISTENCE_D IALECT**	KIE server PostgreSQL Hibernate dialect.	org.hibernate.diale ct.PostgreSQLDial ect	True
KIE_MBEANS	**KIE_MBEANS**	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbean s system properties)	enabled	False
DROOLS_SERV ER_FILTER_CL ASSES	**DROOLS_SERV ER_FILTER_CL ASSES**	KIE server class filtering. (Sets the org.drools.server.fil ter.classes system property)	true	False
PROMETHEUS_ SERVER_EXT_D ISABLED	**PROMETHEUS_ SERVER_EXT_D ISABLED**	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheu s.server.ext.disable d system property)	false	False
KIE_SERVER_H OSTNAME_HTT P	**HOSTNAME_HT TP**	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	–	False
KIE_SERVER_H OSTNAME_HTT PS	**HOSTNAME_HT TPS**	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	–	False

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_HTTPS_SECRET	–	The name of the secret containing the keystore file.	kieserver-app-secret	True
KIE_SERVER_HTTPS_KEYSTORE	HTTPS_KEYSTORE	The name of the keystore file within the secret.	keystore.jks	False
KIE_SERVER_HTTPS_NAME	HTTPS_NAME	The name associated with the server certificate.	jboss	False
KIE_SERVER_HTTPS_PASSWORD	HTTPS_PASSWORD	The password for the keystore and certificate.	mykeystorepass	False
KIE_SERVER_BYPASS_AUTH_USER	KIE_SERVER_BYPASS_AUTH_USER	Allows the KIE server to bypass the authenticated user for task related operations e.g. queries. (Sets the org.kie.server.bypass.auth.user system property)	false	False
KIE_SERVER_CONTAINER_DEPLOYMENT	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE Server Container deployment configuration in format: containerId=groupId:artifactId:version |c2=g2:a2:v2	rhpam-kieserver-library=org.openshift.quickstarts:rhpam-kieserver-library:1.5.0-SNAPSHOT	True
SOURCE_REPOSITORY_URL	–	Git source URI for application.	https://github.com/jboss-container-images/rhpam-7-openshift-image.git	True
SOURCE_REPOSITORY_REF	–	Git branch/tag reference.	master	False

Variable name	Image Environment Variable	Description	Example value	Required
CONTEXT_DIR	–	Path within Git project to build; empty for root project directory.	quickstarts/library –process/library	False
GITHUB_WEBH OOK_SECRET	–	GitHub trigger secret.	–	True
GENERIC_WEB HOOK_SECRET	–	Generic build trigger secret.	–	True
MAVEN_MIRRO R_URL	**MAVEN_MIRRO R_URL**	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
MAVEN_MIRRO R_OF	**MAVEN_MIRRO R_OF**	Maven mirror configuration for KIE server.	external:*	False
MAVEN_REPO_I D	**EXTERNAL_MA VEN_REPO_ID**	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
MAVEN_REPO_URL	**EXTERNAL_MAVEN_REPO_URL**	Fully qualified URL to a Maven repository.	–	False
MAVEN_REPO_USERNAME	**EXTERNAL_MAVEN_REPO_USERNAME**	Username to access the Maven repository, if required.	–	False
MAVEN_REPO_PASSWORD	**EXTERNAL_MAVEN_REPO_PASSWORD**	Password to access the Maven repository, if required.	–	False
BUSINESS_CENTRAL_SERVICE	**WORKBENCH_SERVICE_NAME**	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
BUSINESS_CENTRAL_MAVEN_USERNAME	**RHPAMCENTR_MAVEN_REPO_USERNAME**	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
BUSINESS_CENTRAL_MAVEN_PASSWORD	**RHPAMCENTR_MAVEN_REPO_PASSWORD**	Password to access the Maven service hosted by Business Central inside EAP.	maven1!	False
ARTIFACT_DIR	–	List of directories from which archives will be copied into the deployment folder. If unspecified, all archives in /target will be copied.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL	TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL	Sets refresh-interval for the EJB timer service database-data-store.	30000	False
KIE_SERVER_M EMORY_LIMIT	–	KIE server Container memory limit.	1Gi	False
KIE_SERVER_M GMT_DISABLE D	KIE_SERVER_M GMT_DISABLE D	Disable management api and don't allow KIE containers to be deployed/undeplo yed or started/stopped sets the property org.kie.server.mgm t.api.disabled to true and org.kie.server.start up.strategy to LocalContainersSt artupStrategy.	true	True
SSO_URL	SSO_URL	RH-SSO URL.	https://rh-sso.example.com/ auth	False
SSO_REALM	SSO_REALM	RH-SSO Realm name.	–	False
KIE_SERVER_S SO_CLIENT	SSO_CLIENT	KIE Server RH-SSO Client name.	–	False
KIE_SERVER_S SO_SECRET	SSO_SECRET	KIE Server RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False
SSO_USERNAM E	SSO_USERNAM E	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
SSO_PASSWORD	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client.	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable SSL Certificate Validation.	false	False
SSO_PRINCIPAL_ATTRIBUTE	SSO_PRINCIPAL_ATTRIBUTE	RH-SSO Principal Attribute to use as username.	preferred_username	False
AUTH_LDAP_URL	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication.	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	AUTH_LDAP_BIND_DN	Bind DN used for authentication.	uid=admin,ou=users,ou=exmample,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	AUTH_LDAP_BIND_CREDENTIAL	LDAP Credentials used for authentication.	Password	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	AUTH_LDAP_JAAS_SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
AUTH_LDAP_BASE_CTX_DN	AUTH_LDAP_BASE_CTX_DN	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
AUTH_LDAP_BASE_FILTER	**AUTH_LDAP_BASE_FILTER**	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
AUTH_LDAP_SEARCH_SCOPE	**AUTH_LDAP_SEARCH_SCOPE**	The search scope to use.	**SUBTREE_SCOPE**	False
AUTH_LDAP_SEARCH_TIME_LIMIT	**AUTH_LDAP_SEARCH_TIME_LIMIT**	The timeout in milliseconds for user or role searches.	10000	False
AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	**AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE**	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

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_P ARSE_USERNA ME	**AUTH_LDAP_P ARSE_USERNA ME**	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 usernameBeginStri ng and usernameEndStrin g.	true	False
AUTH_LDAP_U SERNAME_BEG IN_STRING	**AUTH_LDAP_U SERNAME_BEG IN_STRING**	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False
AUTH_LDAP_U SERNAME_END _STRING	**AUTH_LDAP_U SERNAME_END _STRING**	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_ATTRIBUT E_ID	**AUTH_LDAP_R OLE_ATTRIBUT E_ID**	Name of the attribute containing the user roles.	memberOf	False
AUTH_LDAP_R OLES_CTX_DN	**AUTH_LDAP_R OLES_CTX_DN**	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=exa mple,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_FILTER	**AUTH_LDAP_R OLE_FILTER**	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
AUTH_LDAP_R OLE_RECURSI ON	**AUTH_LDAP_R OLE_RECURSI ON**	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
AUTH_LDAP_D EFAULT_ROLE	**AUTH_LDAP_D EFAULT_ROLE**	A role included for all authenticated users	user	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	**AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID**	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	**AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN**	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
AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	**AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN**	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
AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK	AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK	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
AUTH_ROLE_M APPER_ROLES _PROPERTIES	AUTH_ROLE_M APPER_ROLES _PROPERTIES	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,r ole2,role3	–	False
AUTH_ROLE_M APPER_REPLA CE_ROLE	AUTH_ROLE_M APPER_REPLA CE_ROLE	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
${APPLICATION_NAME}-kieserver	8080	http	All the KIE server web server's ports.
	8443	https	
${APPLICATION_NAME}-kieserver-ping	8888	ping	The JGroups ping port for clustering.
${APPLICATION_NAME}-postgresql	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-${APPLICATION_NAME}-kieserver-http	none	**${KIE_SERVER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-kieserver-https	TLS passthrough	**${KIE_SERVER_HOSTNAME_HTTPS}**

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
rhpam74-kieserver-openshift:1.0	**rhpam-7/rhpam74-kieserver-openshift**	**${APPLICATION_NAME}-kieserver:latest**	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
${APPLICATION_NAME}-kieserver	ImageChange
${APPLICATION_NAME}-postgresql	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
${APPLICATION_NAME}-kieserver	2
${APPLICATION_NAME}-postgresql	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
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**

5.2.2.4.3.2. Image

Deployment	Image
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**
${APPLICATION_NAME}-postgresql	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
${APPLICATION_NAME}-kieserver	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
	ping	8888	**TCP**

Deployments	Name	Port	Protocol
${APPLICATION_NAME}-postgresql	–	5432	**TCP**

5.2.2.4.3.6. Image Environment Variables

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

Deployment	Variable name	Description	Example value
	KIE_SERVER_BYPA SS_AUTH_USER	Allows the KIE server to bypass the authenticated user for task related operations e.g. queries. (Sets the org.kie.server.bypass.aut h.user system property)	${KIE_SERVER_BYP ASS_AUTH_USER}
	KIE_SERVER_ID	–	–
	KIE_SERVER_ROUT E_NAME	–	${APPLICATION_NA ME}-kieserver
	KIE_SERVER_USER	KIE server username. (Sets the org.kie.server.user system property)	${KIE_SERVER_USE R}
	KIE_SERVER_PWD	KIE server password, used to connect to KIE servers. Value is automatically generated by default. (Sets the org.kie.server.pwd system property)	${KIE_SERVER_PWD }
	KIE_SERVER_CONT AINER_DEPLOYMEN T	KIE Server Container deployment configuration in format: containerId=groupId:arti factId:version|c2=g2:a2: v2	${KIE_SERVER_CON TAINER_DEPLOYME NT}
	MAVEN_MIRROR_U RL	Maven mirror to use for S2I builds. If enabled, the mirror must contain all the artifacts necessary for building and running the required services.	${MAVEN_MIRROR_ URL}
	MAVEN_MIRROR_O F	Maven mirror configuration for KIE server.	${MAVEN_MIRROR_ OF}
	MAVEN_REPOS	–	RHPAMCENTR,EXTERN AL

Deployment	Variable name	Description	Example value
	RHPAMCENTR_MAVEN_REPO_ID	–	repo-rhpamcentr
	RHPAMCENTR_MAVEN_REPO_SERVICE	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	**${BUSINESS_CENTRAL_SERVICE}**
	RHPAMCENTR_MAVEN_REPO_PATH	–	**/maven2/**
	RHPAMCENTR_MAVEN_REPO_USERNAME	Username to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_USERNAME}**
	RHPAMCENTR_MAVEN_REPO_PASSWORD	Password to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_PASSWORD}**
	EXTERNAL_MAVEN_REPO_ID	The id to use for the maven repository. If set, it can be excluded from the optionally configured mirror by adding it to MAVEN_MIRROR_OF. For example: external:*,!repo-rhpamcentr,!repo-custom. If MAVEN_MIRROR_URL is set but MAVEN_MIRROR_ID is not set, an id will be generated randomly, but won't be usable in MAVEN_MIRROR_OF.	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Fully qualified URL to a Maven repository.	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Username to access the Maven repository, if required.	**${MAVEN_REPO_USERNAME}**

Deployment	Variable name	Description	Example value
	EXTERNAL_MAVEN_ REPO_PASSWORD	Password to access the Maven repository, if required.	**${MAVEN_REPO_PA SSWORD}**
	KIE_SERVER_PERSI STENCE_DS	KIE server persistence datasource. (Sets the org.kie.server.persistenc e.ds system property)	**${KIE_SERVER_PER SISTENCE_DS}**
	DATASOURCES	–	**RHPAM**
	RHPAM_DATABASE	KIE server PostgreSQL database name.	**${KIE_SERVER_POS TGRESQL_DB}**
	RHPAM_JNDI	KIE server persistence datasource. (Sets the org.kie.server.persistenc e.ds system property)	**${KIE_SERVER_PER SISTENCE_DS}**
	RHPAM_JTA	–	true
	RHPAM_DRIVER	–	postgresql
	KIE_SERVER_PERSI STENCE_DIALECT	KIE server PostgreSQL Hibernate dialect.	**${KIE_SERVER_POS TGRESQL_DIALECT }**
	RHPAM_USERNAME	KIE server PostgreSQL database username.	**${KIE_SERVER_POS TGRESQL_USER}**
	RHPAM_PASSWORD	KIE server PostgreSQL database password.	**${KIE_SERVER_POS TGRESQL_PWD}**
	RHPAM_SERVICE_H OST	–	**${APPLICATION_NA ME}-postgresql**
	RHPAM_SERVICE_P ORT	–	5432
	TIMER_SERVICE_DA TA_STORE_REFRES H_INTERVAL	Sets refresh-interval for the EJB timer service database-data-store.	**${TIMER_SERVICE_ DATA_STORE_REF RESH_INTERVAL}**
	HTTPS_KEYSTORE_ DIR	–	**/etc/kieserver-secret- volume**

Deployment	Variable name	Description	Example value
	HTTPS_KEYSTORE	The name of the keystore file within the secret.	**${KIE_SERVER_HTTPS_KEYSTORE}**
	HTTPS_NAME	The name associated with the server certificate.	**${KIE_SERVER_HTTPS_NAME}**
	HTTPS_PASSWORD	The password for the keystore and certificate.	**${KIE_SERVER_HTTPS_PASSWORD}**
	KIE_SERVER_MGMT_DISABLED	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped sets the property org.kie.server.mgmt.api.disabled to true and org.kie.server.startup.strategy to LocalContainersStartupStrategy.	**${KIE_SERVER_MGMT_DISABLED}**
	KIE_SERVER_STARTUP_STRATEGY	–	OpenShiftStartupStrategy
	JGROUPS_PING_PROTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PING_SERVICE_NAME	–	**${APPLICATION_NAME}-kieserver-ping**
	OPENSHIFT_DNS_PING_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL.	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO Realm name.	**${SSO_REALM}**
	SSO_SECRET	KIE Server RH-SSO Client Secret.	**${KIE_SERVER_SSO_SECRET}**

Deployment	Variable name	Description	Example value
	SSO_CLIENT	KIE Server RH-SSO Client name.	**${KIE_SERVER_SSO _CLIENT}**
	SSO_USERNAME	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	**${SSO_USERNAME}**
	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client.	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_ CERTIFICATE_VALI DATION	RH-SSO Disable SSL Certificate Validation.	**${SSO_DISABLE_SS L_CERTIFICATE_VA LIDATION}**
	SSO_PRINCIPAL_AT TRIBUTE	RH-SSO Principal Attribute to use as username.	**${SSO_PRINCIPAL_ ATTRIBUTE}**
	HOSTNAME_HTTP	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTP}**
	HOSTNAME_HTTPS	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTPS}**
	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication.	**${AUTH_LDAP_URL}**
	AUTH_LDAP_BIND_ DN	Bind DN used for authentication.	**${AUTH_LDAP_BIND _DN}**
	AUTH_LDAP_BIND_ CREDENTIAL	LDAP Credentials used for authentication.	**${AUTH_LDAP_BIND _CREDENTIAL}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_JAAS_SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	**${AUTH_LDAP_JAAS_SECURITY_DOMAIN}**
	AUTH_LDAP_BASE_CTX_DN	LDAP Base DN of the top-level context to begin the user search.	**${AUTH_LDAP_BASE_CTX_DN}**
	AUTH_LDAP_BASE_FILTER	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}).	**${AUTH_LDAP_BASE_FILTER}**
	AUTH_LDAP_SEARCH_SCOPE	The search scope to use.	**${AUTH_LDAP_SEARCH_SCOPE}**
	AUTH_LDAP_SEARCH_TIME_LIMIT	The timeout in milliseconds for user or role searches.	**${AUTH_LDAP_SEARCH_TIME_LIMIT}**
	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	**${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE _USERNAME	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 usernameBeginString and usernameEndString.	**${AUTH_LDAP_PAR SE_USERNAME}**
	AUTH_LDAP_USER NAME_BEGIN_STRI NG	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_BEGIN_STR ING}**
	AUTH_LDAP_USER NAME_END_STRING	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_END_STRIN G}**
	AUTH_LDAP_ROLE_ ATTRIBUTE_ID	Name of the attribute containing the user roles.	**${AUTH_LDAP_ROL E_ATTRIBUTE_ID}**
	AUTH_LDAP_ROLE S_CTX_DN	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.	**${AUTH_LDAP_ROL ES_CTX_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE_FILTER	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}).	**${AUTH_LDAP_ROLE_FILTER}**
	AUTH_LDAP_ROLE_RECURSION	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	**${AUTH_LDAP_ROLE_RECURSION}**
	AUTH_LDAP_DEFAULT_ROLE	A role included for all authenticated users	**${AUTH_LDAP_DEFAULT_ROLE}**
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	**${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE _ROLE_NAME_FRO M_DN	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.	**${AUTH_LDAP_PAR SE_ROLE_NAME_FR OM_DN}**
	AUTH_LDAP_ROLE_ ATTRIBUTE_IS_DN	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	**${AUTH_LDAP_ROL E_ATTRIBUTE_IS_D N}**
	AUTH_LDAP_REFER RAL_USER_ATTRIB UTE_ID_TO_CHECK	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.	**${AUTH_LDAP_REF ERRAL_USER_ATTR IBUTE_ID_TO_CHEC K}**

Deployment	Variable name	Description	Example value
	AUTH_ROLE_MAPP ER_ROLES_PROPE RTIES	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,r ole3	**${AUTH_ROLE_MAP PER_ROLES_PROPE RTIES}**
	AUTH_ROLE_MAPP ER_REPLACE_ROLE	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	**${AUTH_ROLE_MAP PER_REPLACE_ROL E}**
${APPLICATION_NA ME}-postgresql	**POSTGRESQL_USE R**	KIE server PostgreSQL database username.	**${KIE_SERVER_POS TGRESQL_USER}**
	POSTGRESQL_PAS SWORD	KIE server PostgreSQL database password.	**${KIE_SERVER_POS TGRESQL_PWD}**
	POSTGRESQL_DAT ABASE	KIE server PostgreSQL database name.	**${KIE_SERVER_POS TGRESQL_DB}**
	POSTGRESQL_MAX _PREPARED_TRANS ACTIONS	Allows the PostgreSQL to handle XA transactions.	**${POSTGRESQL_MA X_PREPARED_TRAN SACTIONS}**

5.2.2.4.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
${APPLICATION _NAME}- kieserver	kieserver- keystore-volume	**/etc/kieserver- secret-volume**	ssl certs	True
${APPLICATION _NAME}- postgresql	**${APPLICATION _NAME}- postgresql-pvol**	**/var/lib/pgsql/da ta**	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
${APPLICATION_NAME}-postgresql-claim	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. RHPAM74-PROD-IMMUTABLE-KIESERVER-AMQ.YAML TEMPLATE

Application template for an immultable KIE server in a production environment integrated with ActiveMQ, for Red Hat Process Automation Manager 7.4

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
APPLICATION_ NAME	–	The name for the application.	myapp	True
KIE_ADMIN_US ER	**KIE_ADMIN_US ER**	KIE administrator username	adminUser	False
KIE_ADMIN_PW D	**KIE_ADMIN_PW D**	KIE administrator password	–	False
KIE_SERVER_U SER	**KIE_SERVER_U SER**	KIE server username (Sets the org.kie.server.user system property)	executionUser	False

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_P WD	**KIE_SERVER_P WD**	KIE server password, used to connect to KIE servers. Value is automatically generated by default. (Sets the org.kie.server.pwd system property)	–	False
IMAGE_STREA M_NAMESPACE	–	Namespace in which the ImageStreams for Red Hat Middleware 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/projec t.	openshift	True
KIE_SERVER_I MAGE_STREAM _NAME	–	The name of the image stream to use for KIE server. Default is "rhpam74-kieserver-openshift".	rhpam74-kieserver-openshift	True
IMAGE_STREA M_TAG	–	A named pointer to an image in an image stream. Default is "1.0".	1.0	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_P ERSISTENCE_D S	**KIE_SERVER_P ERSISTENCE_D S**	KIE server persistence datasource (Sets the org.kie.server.persi stence.ds system property)	java:/jboss/dataso urces/rhpam	False
POSTGRESQL_I MAGE_STREAM _NAMESPACE	–	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/projec t. Default is "openshift".	openshift	False
POSTGRESQL_I MAGE_STREAM _TAG	–	The PostgreSQL image version, which is intended to correspond to the PostgreSQL version. Default is "10".	10	False
KIE_SERVER_P OSTGRESQL_U SER	**RHPAM_USERN AME**	KIE server PostgreSQL database username	rhpam	False
KIE_SERVER_P OSTGRESQL_P WD	**RHPAM_PASSW ORD**	KIE server PostgreSQL database password	–	False
KIE_SERVER_P OSTGRESQL_D B	**RHPAM_DATAB ASE**	KIE server PostgreSQL database name	rhpam7	False

Variable name	Image Environment Variable	Description	Example value	Required
POSTGRESQL_ MAX_PREPARE D_TRANSACTI ONS	**POSTGRESQL_ MAX_PREPARE D_TRANSACTI ONS**	Allows the PostgreSQL to handle XA transactions.	100	True
DB_VOLUME_C APACITY	–	Size of persistent storage for the database volume.	1Gi	True
KIE_MBEANS	**KIE_MBEANS**	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbean s system properties)	enabled	False
DROOLS_SERV ER_FILTER_CL ASSES	**DROOLS_SERV ER_FILTER_CL ASSES**	KIE server class filtering (Sets the org.drools.server.fil ter.classes system property)	true	False
PROMETHEUS_ SERVER_EXT_D ISABLED	**PROMETHEUS_ SERVER_EXT_D ISABLED**	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheu s.server.ext.disable d system property)	false	False
KIE_SERVER_H OSTNAME_HTT P	**HOSTNAME_HT TP**	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
KIE_SERVER_HOSTNAME_HTTPS	**HOSTNAME_HTTPS**	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	–	False
KIE_SERVER_HTTPS_SECRET	–	The name of the secret containing the keystore file	kieserver-app-secret	True
KIE_SERVER_HTTPS_KEYSTORE	**HTTPS_KEYSTORE**	The name of the keystore file within the secret	keystore.jks	False
KIE_SERVER_HTTPS_NAME	**HTTPS_NAME**	The name associated with the server certificate	jboss	False
KIE_SERVER_HTTPS_PASSWORD	**HTTPS_PASSWORD**	The password for the keystore and certificate	mykeystorepass	False
KIE_SERVER_BYPASS_AUTH_USER	**KIE_SERVER_BYPASS_AUTH_USER**	KIE server bypass auth user (Sets the org.kie.server.bypass.auth.user system property)	false	False
KIE_SERVER_CONTAINER_DEPLOYMENT	**KIE_SERVER_CONTAINER_DEPLOYMENT**	KIE Server Container deployment configuration in format: containerId=groupId:artifactId:version|c2=g2:a2:v2	rhpam-kieserver-library=org.openshift.quickstarts:rhpam-kieserver-library:1.5.0-SNAPSHOT	True
SOURCE_REPOSITORY_URL	–	Git source URI for application	https://github.com/jboss-container-images/rhpam-7-openshift-image.git	True

Variable name	Image Environment Variable	Description	Example value	Required
SOURCE_REPOSITORY_REF	–	Git branch/tag reference	master	False
CONTEXT_DIR	–	Path within Git project to build; empty for root project directory.	quickstarts/library-process/library	False
GITHUB_WEBHOOK_SECRET	–	GitHub trigger secret	–	True
GENERIC_WEBHOOK_SECRET	–	Generic build trigger secret	–	True
MAVEN_MIRROR_URL	–	Maven mirror to use for S2I builds	–	False
MAVEN_REPO_ID	**EXTERNAL_MAVEN_REPO_ID**	The id to use for the maven repository, if set. Default is generated randomly.	my-repo-id	False
MAVEN_REPO_URL	**EXTERNAL_MAVEN_REPO_URL**	Fully qualified URL to a Maven repository.	–	False
MAVEN_REPO_USERNAME	**EXTERNAL_MAVEN_REPO_USERNAME**	Username to access the Maven repository, if required.	–	False
MAVEN_REPO_PASSWORD	**EXTERNAL_MAVEN_REPO_PASSWORD**	Password to access the Maven repository, if required.	–	False
BUSINESS_CENTRAL_SERVICE	**WORKBENCH_SERVICE_NAME**	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
BUSINESS_CEN TRAL_MAVEN_ USERNAME	**RHPAMCENTR_ MAVEN_REPO_ USERNAME**	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
BUSINESS_CEN TRAL_MAVEN_ PASSWORD	**RHPAMCENTR_ MAVEN_REPO_ PASSWORD**	Password to access the Maven service hosted by Business Central inside EAP.	maven1!	False
ARTIFACT_DIR	–	List of directories from which archives will be copied into the deployment folder. If unspecified, all archives in /target will be copied.	–	False
TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL	**TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL**	Sets refresh-interval for the EJB timer service database-data-store.	30000	False
KIE_SERVER_M EMORY_LIMIT	–	KIE server Container memory limit	1Gi	False
KIE_SERVER_M GMT_DISABLE D	**KIE_SERVER_M GMT_DISABLE D**	Disable management api and don't allow KIE containers to be deployed/undeplo yed or started/stopped sets the property org.kie.server.mgm t.api.disabled to true and org.kie.server.start up.strategy to LocalContainersSt artupStrategy.	true	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_J MS_QUEUE_RE QUEST	**KIE_SERVER_J MS_QUEUE_RE QUEST**	JNDI name of request queue for JMS. The default value is queue/KIE.SERVE R.REQUEST	queue/KIE.SERVE R.REQUEST	False
KIE_SERVER_J MS_QUEUE_RE SPONSE	**KIE_SERVER_J MS_QUEUE_RE SPONSE**	JNDI name of response queue for JMS. The default value is queue/KIE.SERVE R.RESPONSE	queue/KIE.SERVE R.RESPONSE	False
KIE_SERVER_J MS_QUEUE_EX ECUTOR	**KIE_SERVER_J MS_QUEUE_EX ECUTOR**	JNDI name of response queue for JMS. The default value is queue/KIE.SERVE R.RESPONSE	queue/KIE.SERVE R.EXECUTOR	False
KIE_SERVER_J MS_ENABLE_SI GNAL	**KIE_SERVER_J MS_ENABLE_SI GNAL**	JMS queue for signals	true	False
KIE_SERVER_J MS_QUEUE_SI GNAL	**KIE_SERVER_J MS_QUEUE_SI GNAL**	Enable the Signal configuration through JMS	queue/KIE.SERVE R.SIGNAL	False
KIE_SERVER_J MS_ENABLE_A UDIT	**KIE_SERVER_J MS_ENABLE_A UDIT**	Enable the Audit logging through JMS	true	False
KIE_SERVER_J MS_QUEUE_AU DIT	**KIE_SERVER_J MS_QUEUE_AU DIT**	JMS queue for audit logging	queue/KIE.SERVE R.AUDIT	False
KIE_SERVER_J MS_AUDIT_TRA NSACTED	**KIE_SERVER_J MS_AUDIT_TRA NSACTED**	determines if JMS session is transacted or not – default true.	false	False

Variable name	Image Environment Variable	Description	Example value	Required
AMQ_USERNA ME	**AMQ_USERNA ME**	User name for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	–	False
AMQ_PASSWO RD	**AMQ_PASSWO RD**	Password for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	–	False
AMQ_ROLE	**AMQ_ROLE**	User role for standard broker user.	admin	True

Variable name	Image Environment Variable	Description	Example value	Required
AMQ_QUEUES	**AMQ_QUEUES**	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 value here than KIE_SERVER_JMS _QUEUE_RESPON SE, KIE_SERVER_JMS _QUEUE_REQUES T, KIE_SERVER_JMS _QUEUE_SIGNAL, KIE_SERVER_JMS _QUEUE_AUDIT and KIE_SERVER_JMS _QUEUE_EXECUT OR env.	queue/KIE.SERVE R.REQUEST,queu e/KIE.SERVER.RE SPONSE,queue/KI E.SERVER.EXECU TOR,queue/KIE.S ERVER.SIGNAL,qu eue/KIE.SERVER. AUDIT	False
AMQ_GLOBAL_ MAX_SIZE	**AMQ_GLOBAL_ MAX_SIZE**	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

Variable name	Image Environment Variable	Description	Example value	Required
AMQ_PROTOC OL	**AMQ_PROTOC OL**	Broker protocols to configure, separated by commas. Allowed values are: **openwire**, **amqp**, **stomp** and **mqtt**. Only **openwire** is supported by EAP.	openwire	False
AMQ_BROKER_ IMAGESTREAM _NAME	–	AMQ Broker Image	amq-broker-73-openshift:7.3	True
SSO_URL	**SSO_URL**	RH-SSO URL	https://rh-sso.example.com/auth	False
SSO_REALM	**SSO_REALM**	RH-SSO Realm name	–	False
KIE_SERVER_S SO_CLIENT	**SSO_CLIENT**	KIE Server RH-SSO Client name	–	False
KIE_SERVER_S SO_SECRET	**SSO_SECRET**	KIE Server RH-SSO Client Secret	252793ed-7118-4ca8-8dab-5622fa97d892	False
SSO_USERNAM E	**SSO_USERNAM E**	RH-SSO Realm Admin Username used to create the Client if it doesn't exist	–	False
SSO_PASSWOR D	**SSO_PASSWOR D**	RH-SSO Realm Admin Password used to create the Client	–	False
SSO_DISABLE_ SSL_CERTIFIC ATE_VALIDATI ON	**SSO_DISABLE_ SSL_CERTIFIC ATE_VALIDATI ON**	RH-SSO Disable SSL Certificate Validation	false	False
SSO_PRINCIPA L_ATTRIBUTE	**SSO_PRINCIPA L_ATTRIBUTE**	RH-SSO Principal Attribute to use as username.	preferred_userna me	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_URL	**AUTH_LDAP_URL**	LDAP Endpoint to connect for authentication	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	**AUTH_LDAP_BIND_DN**	Bind DN used for authentication	uid=admin,ou=users,ou=exmample,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	**AUTH_LDAP_BIND_CREDENTIAL**	LDAP Credentials used for authentication	Password	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	**AUTH_LDAP_JAAS_SECURITY_DOMAIN**	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
AUTH_LDAP_BASE_CTX_DN	**AUTH_LDAP_BASE_CTX_DN**	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=example,ou=com	False
AUTH_LDAP_BASE_FILTER	**AUTH_LDAP_BASE_FILTER**	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
AUTH_LDAP_SEARCH_SCOPE	**AUTH_LDAP_SEARCH_SCOPE**	The search scope to use.	**SUBTREE_SCOPE**	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_SEARCH_TIME_LIMIT	**AUTH_LDAP_SEARCH_TIME_LIMIT**	The timeout in milliseconds for user or role searches.	10000	False
AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	**AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE**	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
AUTH_LDAP_PARSE_USERNAME	**AUTH_LDAP_PARSE_USERNAME**	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 usernameBeginString and usernameEndString.	true	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_U SERNAME_BEG IN_STRING	**AUTH_LDAP_U SERNAME_BEG IN_STRING**	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False
AUTH_LDAP_U SERNAME_END _STRING	**AUTH_LDAP_U SERNAME_END _STRING**	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False
AUTH_LDAP_R OLE_ATTRIBUT E_ID	**AUTH_LDAP_R OLE_ATTRIBUT E_ID**	Name of the attribute containing the user roles.	memberOf	False
AUTH_LDAP_R OLES_CTX_DN	**AUTH_LDAP_R OLES_CTX_DN**	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=exa mple,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_FILTER	**AUTH_LDAP_R OLE_FILTER**	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
AUTH_LDAP_R OLE_RECURSI ON	**AUTH_LDAP_R OLE_RECURSI ON**	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
AUTH_LDAP_D EFAULT_ROLE	**AUTH_LDAP_D EFAULT_ROLE**	A role included for all authenticated users	user	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	**AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID**	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	**AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN**	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
AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	**AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN**	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
AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK	**AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK**	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
AUTH_ROLE_M APPER_ROLES _PROPERTIES	**AUTH_ROLE_M APPER_ROLES _PROPERTIES**	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,r ole2,role3	–	False
AUTH_ROLE_M APPER_REPLA CE_ROLE	**AUTH_ROLE_M APPER_REPLA CE_ROLE**	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
${APPLICATION_NAME}-kieserver	8080	http	All the KIE server web server's ports.
	8443	https	
${APPLICATION_NAME}-kieserver-ping	8888	ping	The JGroups ping port for clustering.
${APPLICATION_NAME}-amq-jolokia	8161	amq-jolokia	The broker's console and Jolokia port.
${APPLICATION_NAME}-amq-amqp	5672	amp-amqp	The broker's AMQP port.
${APPLICATION_NAME}-amq-mqtt	1883	amq-mqtt	The broker's MQTT port.
${APPLICATION_NAME}-amq-stomp	61613	amp-stomp	The broker's STOMP port.
${APPLICATION_NAME}-amq-tcp	61616	amq-tcp	The broker's OpenWire port.
${APPLICATION_NAME}-postgresql	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
${APPLICATION_NAME}-kieserver-http	none	${KIE_SERVER_HOSTNAME_HTTP}

Service	Security	Hostname
${APPLICATION_NAME}-kieserver-https	TLS passthrough	**${KIE_SERVER_HOSTNAME_HTTPS}**
${APPLICATION_NAME}-amq-jolokia-console	none	\<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
rhpam74-kieserver-openshift:1.0	**rhpam-7/rhpam74-kieserver-openshift**	**${APPLICATION_NAME}-kieserver:latest**	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
${APPLICATION_NAME}-kieserver	ImageChange
${APPLICATION_NAME}-postgresql	ImageChange
${APPLICATION_NAME}-amq	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
${APPLICATION_NAME}-kieserver	2
${APPLICATION_NAME}-postgresql	1
${APPLICATION_NAME}-amq	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
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**

5.3.2.4.3.2. Image

Deployment	Image
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**
${APPLICATION_NAME}-postgresql	postgresql
${APPLICATION_NAME}-amq	**${AMQ_BROKER_IMAGESTREAM_NAME}**

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
${APPLICATION_NAME}-kieserver	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
	ping	8888	**TCP**
${APPLICATION_NAME}-postgresql	–	5432	**TCP**
${APPLICATION_NAME}-amq	console–jolokia	8161	**TCP**
	amq–amqp	5672	**TCP**
	amq–mqtt	1883	**TCP**
	amq–stomp	61613	**TCP**
	amq–tcp	61616	**TCP**

5.3.2.4.3.6. Image Environment Variables

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

Deployment	Variable name	Description	Example value
	KIE_ADMIN_PWD	KIE administrator password	**${KIE_ADMIN_PWD}**
	KIE_SERVER_MODE	–	**DEVELOPMENT**
	KIE_MBEANS	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbeans system properties)	**${KIE_MBEANS}**
	DROOLS_SERVER_ FILTER_CLASSES	KIE server class filtering (Sets the org.drools.server.filter.cl asses system property)	**${DROOLS_SERVER _FILTER_CLASSES}**
	PROMETHEUS_SER VER_EXT_DISABLE D	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.serv er.ext.disabled system property)	**${PROMETHEUS_SE RVER_EXT_DISABL ED}**
	KIE_SERVER_BYPA SS_AUTH_USER	KIE server bypass auth user (Sets the org.kie.server.bypass.aut h.user system property)	**${KIE_SERVER_BYP ASS_AUTH_USER}**
	KIE_SERVER_ID	–	–
	KIE_SERVER_ROUT E_NAME	–	**${APPLICATION_NA ME}-kieserver**
	KIE_SERVER_USER	KIE server username (Sets the org.kie.server.user system property)	**${KIE_SERVER_USE R}**
	KIE_SERVER_PWD	KIE server password, used to connect to KIE servers. Value is automatically generated by default. (Sets the org.kie.server.pwd system property)	**${KIE_SERVER_PWD }**

Deployment	Variable name	Description	Example value
	KIE_SERVER_CONTAINER_DEPLOYMENT	KIE Server Container deployment configuration in format: containerId=groupId:artifactId:version|c2=g2:a2:v2	**${KIE_SERVER_CONTAINER_DEPLOYMENT}**
	MAVEN_REPOS	–	RHPAMCENTR,EXTERNAL
	RHPAMCENTR_MAVEN_REPO_SERVICE	The Service name for the optional Business Central, where it can be reached, to allow service lookups (for example, maven repo usage), if required.	**${BUSINESS_CENTRAL_SERVICE}**
	RHPAMCENTR_MAVEN_REPO_PATH	–	**/maven2/**
	RHPAMCENTR_MAVEN_REPO_USERNAME	Username to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_USERNAME}**
	RHPAMCENTR_MAVEN_REPO_PASSWORD	Password to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_PASSWORD}**
	EXTERNAL_MAVEN_REPO_ID	The id to use for the maven repository, if set. Default is generated randomly.	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Fully qualified URL to a Maven repository.	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Username to access the Maven repository, if required.	**${MAVEN_REPO_USERNAME}**
	EXTERNAL_MAVEN_REPO_PASSWORD	Password to access the Maven repository, if required.	**${MAVEN_REPO_PASSWORD}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_PERSISTENCE_DS	KIE server persistence datasource (Sets the org.kie.server.persistence.ds system property)	**${KIE_SERVER_PERSISTENCE_DS}**
	DATASOURCES	–	**RHPAM**
	RHPAM_DATABASE	KIE server PostgreSQL database name	**${KIE_SERVER_POSTGRESQL_DB}**
	RHPAM_JNDI	KIE server persistence datasource (Sets the org.kie.server.persistence.ds system property)	**${KIE_SERVER_PERSISTENCE_DS}**
	RHPAM_JTA	–	true
	RHPAM_NONXA	–	false
	RHPAM_DRIVER	–	postgresql
	KIE_SERVER_PERSISTENCE_DIALECT	–	org.hibernate.dialect.PostgreSQLDialect
	RHPAM_USERNAME	KIE server PostgreSQL database username	**${KIE_SERVER_POSTGRESQL_USER}**
	RHPAM_PASSWORD	KIE server PostgreSQL database password	**${KIE_SERVER_POSTGRESQL_PWD}**
	RHPAM_SERVICE_HOST	–	**${APPLICATION_NAME}-postgresql**
	RHPAM_SERVICE_PORT	–	5432
	TIMER_SERVICE_DATA_STORE	–	**${APPLICATION_NAME}-postgresql**
	TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL	Sets refresh-interval for the EJB timer service database-data-store.	**${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_JMS_ QUEUE_REQUEST	JNDI name of request queue for JMS. The default value is queue/KIE.SERVER.RE QUEST	**${KIE_SERVER_JMS _QUEUE_REQUEST}**
	KIE_SERVER_JMS_ QUEUE_RESPONSE	JNDI name of response queue for JMS. The default value is queue/KIE.SERVER.RES PONSE	**${KIE_SERVER_JMS _QUEUE_RESPONS E}**
	KIE_SERVER_JMS_ QUEUE_EXECUTOR	JNDI name of response queue for JMS. The default value is queue/KIE.SERVER.RES PONSE	**${KIE_SERVER_JMS _QUEUE_EXECUTO R}**
	KIE_SERVER_JMS_E NABLE_SIGNAL	JMS queue for signals	**${KIE_SERVER_JMS _ENABLE_SIGNAL}**
	KIE_SERVER_JMS_ QUEUE_SIGNAL	Enable the Signal configuration through JMS	**${KIE_SERVER_JMS _QUEUE_SIGNAL}**
	KIE_SERVER_JMS_E NABLE_AUDIT	Enable the Audit logging through JMS	**${KIE_SERVER_JMS _ENABLE_AUDIT}**
	KIE_SERVER_JMS_ QUEUE_AUDIT	JMS queue for audit logging	**${KIE_SERVER_JMS _QUEUE_AUDIT}**
	KIE_SERVER_JMS_A UDIT_TRANSACTED	determines if JMS session is transacted or not – default true.	**${KIE_SERVER_JMS _AUDIT_TRANSACT ED}**
	MQ_SERVICE_PREFI X_MAPPING	–	**${APPLICATION_NA ME}-amq7=AMQ**
	AMQ_USERNAME	User name for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	**${AMQ_USERNAME}**

Deployment	Variable name	Description	Example value
	AMQ_PASSWORD	Password for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	**${AMQ_PASSWORD}**
	AMQ_PROTOCOL	Broker protocols to configure, separated by commas. Allowed values are: **openwire**, **amqp**, **stomp** and **mqtt**. Only **openwire** is supported by EAP.	tcp
	AMQ_QUEUES	Queue names, separated by commas. These queues will be automatically created when the broker starts. Also, they will be made accessible as JNDI resources in EAP. These are the default queues needed by KIE Server. If using custom Queues use the same value here than KIE_SERVER_JMS_QUEUE_RESPONSE, KIE_SERVER_JMS_QUEUE_REQUEST, KIE_SERVER_JMS_QUEUE_SIGNAL, KIE_SERVER_JMS_QUEUE_AUDIT and KIE_SERVER_JMS_QUEUE_EXECUTOR env.	**${AMQ_QUEUES}**
	HTTPS_KEYSTORE_DIR	–	**/etc/kieserver-secret-volume**
	HTTPS_KEYSTORE	The name of the keystore file within the secret	**${KIE_SERVER_HTTPS_KEYSTORE}**
	HTTPS_NAME	The name associated with the server certificate	**${KIE_SERVER_HTTPS_NAME}**

Deployment	Variable name	Description	Example value
	HTTPS_PASSWORD	The password for the keystore and certificate	**${KIE_SERVER_HTTPS_PASSWORD}**
	KIE_SERVER_MGMT _DISABLED	Disable management api and don't allow KIE containers to be deployed/undeployed or started/stopped sets the property org.kie.server.mgmt.api. disabled to true and org.kie.server.startup.str ategy to LocalContainersStartup Strategy.	**${KIE_SERVER_MG MT_DISABLED}**
	KIE_SERVER_STAR TUP_STRATEGY	–	OpenShiftStartupStrate gy
	JGROUPS_PING_PR OTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PI NG_SERVICE_NAME	–	**${APPLICATION_NA ME}-kieserver-ping**
	OPENSHIFT_DNS_PI NG_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL	**${SSO_URL}**
	SSO_OPENIDCONN ECT_DEPLOYMENT S	–	ROOT.war
	SSO_REALM	RH-SSO Realm name	**${SSO_REALM}**
	SSO_SECRET	KIE Server RH-SSO Client Secret	**${KIE_SERVER_SSO _SECRET}**
	SSO_CLIENT	KIE Server RH-SSO Client name	**${KIE_SERVER_SSO _CLIENT}**
	SSO_USERNAME	RH-SSO Realm Admin Username used to create the Client if it doesn't exist	**${SSO_USERNAME}**

Deployment	Variable name	Description	Example value
	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_ CERTIFICATE_VALI DATION	RH-SSO Disable SSL Certificate Validation	**${SSO_DISABLE_SS L_CERTIFICATE_VA LIDATION}**
	SSO_PRINCIPAL_AT TRIBUTE	RH-SSO Principal Attribute to use as username.	**${SSO_PRINCIPAL_ ATTRIBUTE}**
	HOSTNAME_HTTP	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTP}**
	HOSTNAME_HTTPS	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTPS}**
	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication	**${AUTH_LDAP_URL}**
	AUTH_LDAP_BIND_ DN	Bind DN used for authentication	**${AUTH_LDAP_BIND _DN}**
	AUTH_LDAP_BIND_ CREDENTIAL	LDAP Credentials used for authentication	**${AUTH_LDAP_BIND _CREDENTIAL}**
	AUTH_LDAP_JAAS_ SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	**${AUTH_LDAP_JAA S_SECURITY_DOMA IN}**
	AUTH_LDAP_BASE_ CTX_DN	LDAP Base DN of the top-level context to begin the user search.	**${AUTH_LDAP_BAS E_CTX_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_BASE_FILTER	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}).	**${AUTH_LDAP_BASE_FILTER}**
	AUTH_LDAP_SEARCH_SCOPE	The search scope to use.	**${AUTH_LDAP_SEARCH_SCOPE}**
	AUTH_LDAP_SEARCH_TIME_LIMIT	The timeout in milliseconds for user or role searches.	**${AUTH_LDAP_SEARCH_TIME_LIMIT}**
	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	**${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}**
	AUTH_LDAP_PARSE_USERNAME	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 usernameBeginString and usernameEndString.	**${AUTH_LDAP_PARSE_USERNAME}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_USER NAME_BEGIN_STRI NG	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_BEGIN_STR ING}**
	AUTH_LDAP_USER NAME_END_STRING	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_END_STRIN G}**
	AUTH_LDAP_ROLE_ ATTRIBUTE_ID	Name of the attribute containing the user roles.	**${AUTH_LDAP_ROL E_ATTRIBUTE_ID}**
	AUTH_LDAP_ROLE S_CTX_DN	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	**${AUTH_LDAP_ROL ES_CTX_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE_FILTER	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}).	**${AUTH_LDAP_ROLE_FILTER}**
	AUTH_LDAP_ROLE_RECURSION	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	**${AUTH_LDAP_ROLE_RECURSION}**
	AUTH_LDAP_DEFAULT_ROLE	A role included for all authenticated users	**${AUTH_LDAP_DEFAULT_ROLE}**
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	**${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE _ROLE_NAME_FRO M_DN	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.	**${AUTH_LDAP_PAR SE_ROLE_NAME_FR OM_DN}**
	AUTH_LDAP_ROLE_ ATTRIBUTE_IS_DN	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	**${AUTH_LDAP_ROL E_ATTRIBUTE_IS_D N}**
	AUTH_LDAP_REFER RAL_USER_ATTRIB UTE_ID_TO_CHECK	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.	**${AUTH_LDAP_REF ERRAL_USER_ATTR IBUTE_ID_TO_CHEC K}**

Deployment	Variable name	Description	Example value
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	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	${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}
	AUTH_ROLE_MAPPER_REPLACE_ROLE	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	${AUTH_ROLE_MAPPER_REPLACE_ROLE}
${APPLICATION_NAME}-postgresql	POSTGRESQL_USER	KIE server PostgreSQL database username	${KIE_SERVER_POSTGRESQL_USER}
	POSTGRESQL_PASSWORD	KIE server PostgreSQL database password	${KIE_SERVER_POSTGRESQL_PWD}
	POSTGRESQL_DATABASE	KIE server PostgreSQL database name	${KIE_SERVER_POSTGRESQL_DB}
	POSTGRESQL_MAX_PREPARED_TRANSACTIONS	Allows the PostgreSQL to handle XA transactions.	${POSTGRESQL_MAX_PREPARED_TRANSACTIONS}
${APPLICATION_NAME}-amq	AMQ_USER	User name for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	${AMQ_USERNAME}
	AMQ_PASSWORD	Password for standard broker user. It is required for connecting to the broker. If left empty, it will be generated.	${AMQ_PASSWORD}
	AMQ_ROLE	User role for standard broker user.	${AMQ_ROLE}

Deployment	Variable name	Description	Example value
	AMQ_NAME	–	**${APPLICATION_NAME}-broker**
	AMQ_TRANSPORTS	Broker protocols to configure, separated by commas. Allowed values are: **openwire**, **amqp**, **stomp** and **mqtt**. Only **openwire** is supported by EAP.	**${AMQ_PROTOCOL}**
	AMQ_QUEUES	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 value here than 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 env.	**${AMQ_QUEUES}**
	AMQ_GLOBAL_MAX_SIZE	Specifies the maximum amount of memory that message data can consume. If no value is specified, half of the system's memory is allocated.	**${AMQ_GLOBAL_MAX_SIZE}**
	AMQ_REQUIRE_LOGIN	–	false
	AMQ_ANYCAST_PREFIX	–	–

Deployment	Variable name	Description	Example value
	AMQ_MULTICAST_P REFIX	–	–

5.3.2.4.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
${APPLICATION _NAME}- kieserver	kieserver- keystore-volume	**/etc/kieserver- secret-volume**	ssl certs	True
${APPLICATION _NAME}- postgresql	**${APPLICATION _NAME}- postgresql-pvol**	**/var/lib/pgsql/da ta**	postgresql	false

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
${APPLICATION_NAME}-postgresql-claim	ReadWriteOnce

5.3.2.5.2. Secrets

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

kieserver-app-secret

5.4. RHPAM74-KIESERVER-EXTERNALDB.YAML TEMPLATE

Application template for a managed KIE Server with an external database, for Red Hat Process Automation Manager 7.4

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
APPLICATION_ NAME	–	The name for the application.	myapp	True
MAVEN_MIRRO R_URL	**MAVEN_MIRRO R_URL**	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for building and deploying your services.	–	False
MAVEN_MIRRO R_OF	**MAVEN_MIRRO R_OF**	Maven mirror configuration for KIE server.	external:*	False
MAVEN_REPO_I D	**EXTERNAL_MA VEN_REPO_ID**	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
MAVEN_REPO_ URL	**EXTERNAL_MA VEN_REPO_UR L**	Fully qualified URL to a Maven repository or service.	http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/	True

Variable name	Image Environment Variable	Description	Example value	Required
MAVEN_REPO_ USERNAME	**EXTERNAL_MA VEN_REPO_US ERNAME**	Username to access the Maven repository, if required.	–	False
MAVEN_REPO_ PASSWORD	**EXTERNAL_MA VEN_REPO_PA SSWORD**	Password to access the Maven repository, if required.	–	False
BUSINESS_CEN TRAL_SERVICE	**WORKBENCH_ SERVICE_NAME**	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
BUSINESS_CEN TRAL_MAVEN_ USERNAME	**RHPAMCENTR_ MAVEN_REPO_ USERNAME**	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
BUSINESS_CEN TRAL_MAVEN_ PASSWORD	**RHPAMCENTR_ MAVEN_REPO_ PASSWORD**	Password to access the Maven service hosted by Business Central inside EAP.	maven1!	False
KIE_ADMIN_US ER	**KIE_ADMIN_US ER**	KIE administrator username.	adminUser	False
KIE_ADMIN_PW D	**KIE_ADMIN_PW D**	KIE administrator password.	–	False
KIE_SERVER_U SER	**KIE_SERVER_U SER**	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_P WD	KIE_SERVER_P WD	KIE server password. (Sets the org.kie.server.pwd system property)	–	False
IMAGE_STREA M_NAMESPACE	–	Namespace in which the ImageStreams for Red Hat Middleware 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/projec t.	openshift	True
KIE_SERVER_I MAGE_STREAM _NAME	–	The name of the image stream to use for KIE server. Default is "rhpam74-kieserver-openshift".	rhpam74-kieserver-openshift	True
IMAGE_STREA M_TAG	–	A named pointer to an image in an image stream. Default is "1.0".	1.0	True
KIE_SERVER_P ERSISTENCE_S CHEMA	KIE_SERVER_P ERSISTENCE_S CHEMA	Hibernate persistence schema.	bd.schema	False
KIE_SERVER_E XTERNALDB_DI ALECT	KIE_SERVER_P ERSISTENCE_D IALECT	KIE server external database Hibernate dialect.	org.hibernate.diale ct.MySQL57Dialec t	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_E XTERNALDB_S ERVICE_HOST	**RHPAM_SERVI CE_HOST**	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_EXT ERNALDB_URL is set.	10.10.10.1	False
KIE_SERVER_E XTERNALDB_S ERVICE_PORT	**RHPAM_SERVI CE_PORT**	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_EXT ERNALDB_URL is set.	4321	False
KIE_SERVER_E XTERNALDB_N ONXA	**RHPAM_NONX A**	Sets the datasources type. It can be XA or NONXA. For non XA set it to true. Default value is false.	True	False

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_EXTERNALDB_URL	RHPAM_URL	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
KIE_SERVER_EXTERNALDB_DRIVER	RHPAM_DRIVER	The predefined driver name, available values are mysql, postgresql or the preferred name for the external driver.	mariadb	True
KIE_SERVER_EXTERNALDB_JNDI	KIE_SERVER_PERSISTENCE_DS	Database JNDI name used by application to resolve the datasource, e.g. java:/jboss/datasources/ExampleDS.	java:jboss/datasources/jbpmDS	True
KIE_SERVER_EXTERNALDB_DB	RHPAM_DATABASE	KIE server external database name. Leave blank if the KIE_SERVER_EXTERNALDB_URL is set.	rhpam	False
KIE_SERVER_EXTERNALDB_USER	RHPAM_USERNAME	KIE server external database username.	rhpam	True
KIE_SERVER_EXTERNALDB_PWD	RHPAM_PASSWORD	KIE server external database password.	–	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_E XTERNALDB_M IN_POOL_SIZE	**RHPAM_MIN_P OOL_SIZE**	Sets xa-pool/min-pool-size for the configured datasource.	–	False
KIE_SERVER_E XTERNALDB_M AX_POOL_SIZE	**RHPAM_MAX_P OOL_SIZE**	Sets xa-pool/max-pool-size for the configured datasource.	–	False
KIE_SERVER_E XTERNALDB_C ONNECTION_C HECKER	**RHPAM_CONN ECTION_CHEC KER**	An org.jboss.jca.adapt ers.jdbc.ValidConn ectionChecker that provides a SQLException isValidConnection(Connection e) method to validate if a connection is valid.	org.jboss.jca.adapt ers.jdbc.extension s.mysql.MySQLVal idConnectionChec ker	False
KIE_SERVER_E XTERNALDB_E XCEPTION_SO RTER	**RHPAM_EXCEP TION_SORTER**	An org.jboss.jca.adapt ers.jdbc.Exception Sorter that provides a boolean isExceptionFatal(S QLException e) method to validate if an exception should be broadcast to all javax.resource.spi. ConnectionEventL istener as a connectionErrorO ccurred.	org.jboss.jca.adapt ers.jdbc.extension s.mysql.MySQLEx ceptionSorter	False
KIE_SERVER_E XTERNALDB_B ACKGROUND_ VALIDATION	**RHPAM_BACK GROUND_VALI DATION**	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
KIE_SERVER_E XTERNALDB_B ACKGROUND_ VALIDATION_MI LLIS	**RHPAM_VALID ATION_MILLIS**	Defines the interval for the background-validation check for the jdbc connections.	10000	False
KIE_SERVER_E XTERNALDB_D RIVER_TYPE	**RHPAM_DRIVE R_TYPE**	KIE server external database driver type, applicable only for DB2, possible values are 4 (default) or 2.	4	False
EXTENSIONS_I MAGE	–	ImageStreamTag definition for the image containing the drivers and configuration. i.e custom-driver-image:1.0.	custom-driver-extension:1.0	True
EXTENSIONS_I MAGE_NAMESP ACE	–	Namespace within which the ImageStream definition for the image containing the drivers and configuration is located.	openshift	True
EXTENSIONS_I NSTALL_DIR	–	Full path to the directory within the extensions image where the extensions are located (e.g. install.sh, modules/, etc.).	**/extensions**	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_M ODE	**KIE_SERVER_M ODE**	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.mod e system property).	**PRODUCTION**	False
KIE_MBEANS	**KIE_MBEANS**	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbean s system properties).	enabled	False
DROOLS_SERV ER_FILTER_CL ASSES	**DROOLS_SERV ER_FILTER_CL ASSES**	KIE server class filtering (Sets the org.drools.server.fil ter.classes system property).	true	False
PROMETHEUS_ SERVER_EXT_D ISABLED	**PROMETHEUS_ SERVER_EXT_D ISABLED**	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheu s.server.ext.disable d system property)	false	False

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

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_BYPASS_AUTH_USER	**KIE_SERVER_BYPASS_AUTH_USER**	Allows the KIE server to bypass the authenticated user for task related operations e.g. queries. (Sets the org.kie.server.bypass.auth.user system property)	false	False
TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL	**TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL**	Sets refresh-interval for the EJB timer database data-store service.	30000	False
KIE_SERVER_MEMORY_LIMIT	–	KIE server Container memory limit.	1Gi	False
KIE_SERVER_CONTAINER_DEPLOYMENT	**KIE_SERVER_CONTAINER_DEPLOYMENT**	KIE Server Container deployment configuration in format: containerId=groupId:artifactId:version |c2=g2:a2:v2	rhpam-kieserver-library=org.openshift.quickstarts:rhpam-kieserver-library:1.5.0-SNAPSHOT	False
KIE_SERVER_MGMT_DISABLED	**KIE_SERVER_MGMT_DISABLED**	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.	true	False

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

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_J AAS_SECURITY _DOMAIN	**AUTH_LDAP_J AAS_SECURITY _DOMAIN**	The JMX ObjectName of the JaasSecurityDoma in used to decrypt the password.	–	False
AUTH_LDAP_B ASE_CTX_DN	**AUTH_LDAP_B ASE_CTX_DN**	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=exam ple,ou=com	False
AUTH_LDAP_B ASE_FILTER	**AUTH_LDAP_B ASE_FILTER**	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
AUTH_LDAP_S EARCH_SCOPE	**AUTH_LDAP_S EARCH_SCOPE**	The search scope to use.	**SUBTREE_SCO PE**	False
AUTH_LDAP_S EARCH_TIME_L IMIT	**AUTH_LDAP_S EARCH_TIME_L IMIT**	The timeout in milliseconds for user or role searches.	10000	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	**AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE**	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
AUTH_LDAP_PARSE_USERNAME	**AUTH_LDAP_PARSE_USERNAME**	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 usernameBeginString and usernameEndString.	true	False
AUTH_LDAP_USERNAME_BEGIN_STRING	**AUTH_LDAP_USERNAME_BEGIN_STRING**	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_U SERNAME_END _STRING	**AUTH_LDAP_U SERNAME_END _STRING**	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False
AUTH_LDAP_R OLE_ATTRIBUT E_ID	**AUTH_LDAP_R OLE_ATTRIBUT E_ID**	Name of the attribute containing the user roles.	memberOf	False
AUTH_LDAP_R OLES_CTX_DN	**AUTH_LDAP_R OLES_CTX_DN**	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=exa mple,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_FILTER	**AUTH_LDAP_R OLE_FILTER**	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
AUTH_LDAP_R OLE_RECURSI ON	**AUTH_LDAP_R OLE_RECURSI ON**	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
AUTH_LDAP_D EFAULT_ROLE	**AUTH_LDAP_D EFAULT_ROLE**	A role included for all authenticated users.	user	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_NAME_AT TRIBUTE_ID	**AUTH_LDAP_R OLE_NAME_AT TRIBUTE_ID**	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	name	False
AUTH_LDAP_P ARSE_ROLE_N AME_FROM_DN	**AUTH_LDAP_P ARSE_ROLE_N AME_FROM_DN**	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
AUTH_LDAP_R OLE_ATTRIBUT E_IS_DN	**AUTH_LDAP_R OLE_ATTRIBUT E_IS_DN**	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
AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK	**AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK**	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
AUTH_ROLE_M APPER_ROLES _PROPERTIES	**AUTH_ROLE_M APPER_ROLES _PROPERTIES**	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,r ole2,role3	–	False
AUTH_ROLE_M APPER_REPLA CE_ROLE	**AUTH_ROLE_M APPER_REPLA CE_ROLE**	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
${APPLICATION_NAME}-kieserver	8080	http	All the KIE server web server's ports.
	8443	https	
${APPLICATION_NAME}-kieserver-ping	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-${APPLICATION_NAME}-kieserver-http	none	**${KIE_SERVER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-kieserver-https	TLS passthrough	**${KIE_SERVER_HOSTNAME_HTTPS}**

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
rhpam74-kieserver-openshift:1.0	**rhpam-7/rhpam74-kieserver-openshift**	**${APPLICATION_NAME}-kieserver:latest**	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
${APPLICATION_NAME}-kieserver	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
${APPLICATION_NAME}-kieserver	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
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**

5.4.2.4.3.2. Image

Deployment	Image
${APPLICATION_NAME}-kieserver	**${KIE_SERVER_IMAGE_STREAM_NAME}**

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

5.4.2.4.3.6. Image Environment Variables

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

Deployment	Variable name	Description	Example value
	KIE_SERVER_MODE	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).	**${KIE_SERVER_MODE}**
	KIE_MBEANS	KIE server mbeans enabled/disabled (Sets the kie.mbeans and kie.scanner.mbeans system properties).	**${KIE_MBEANS}**
	DROOLS_SERVER_FILTER_CLASSES	KIE server class filtering (Sets the org.drools.server.filter.classes system property).	**${DROOLS_SERVER_FILTER_CLASSES}**
	PROMETHEUS_SERVER_EXT_DISABLED	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	**${PROMETHEUS_SERVER_EXT_DISABLED}**
	KIE_SERVER_BYPASS_AUTH_USER	Allows the KIE server to bypass the authenticated user for task related operations e.g. queries. (Sets the org.kie.server.bypass.auth.user system property)	**${KIE_SERVER_BYPASS_AUTH_USER}**
	KIE_SERVER_ID	–	–
	KIE_SERVER_ROUTE_NAME	–	**${APPLICATION_NAME}-kieserver**

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

Deployment	Variable name	Description	Example value
	RHPAMCENTR_MAVEN_REPO_USERNAME	Username to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_USERNAME}**
	RHPAMCENTR_MAVEN_REPO_PASSWORD	Password to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_PASSWORD}**
	EXTERNAL_MAVEN_REPO_ID	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.	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Fully qualified URL to a Maven repository or service.	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Username to access the Maven repository, if required.	**${MAVEN_REPO_USERNAME}**
	EXTERNAL_MAVEN_REPO_PASSWORD	Password to access the Maven repository, if required.	**${MAVEN_REPO_PASSWORD}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_MGMT_DISABLED	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 LocalContainersStartup Strategy.	**${KIE_SERVER_MGMT_DISABLED}**
	KIE_SERVER_STARTUP_STRATEGY	–	OpenShiftStartupStrategy
	KIE_SERVER_PERSISTENCE_DS	Database JNDI name used by application to resolve the datasource, e.g. java:/jboss/datasources/ExampleDS.	**${KIE_SERVER_EXTERNALDB_JNDI}**
	KIE_SERVER_PERSISTENCE_SCHEMA	Hibernate persistence schema.	**${KIE_SERVER_PERSISTENCE_SCHEMA}**
	KIE_SERVER_PERSISTENCE_DIALECT	KIE server external database Hibernate dialect.	**${KIE_SERVER_EXTERNALDB_DIALECT}**
	DATASOURCES	–	**RHPAM**
	RHPAM_DATABASE	KIE server external database name. Leave blank if the KIE_SERVER_EXTERNALDB_URL is set.	**${KIE_SERVER_EXTERNALDB_DB}**
	RHPAM_SERVICE_HOST	Sets the datasource service host. Use this if you want to use the predefined mysql or postgresql datasource properties. Leave blank if the KIE_SERVER_EXTERNALDB_URL is set.	**${KIE_SERVER_EXTERNALDB_SERVICE_HOST}**

Deployment	Variable name	Description	Example value
	RHPAM_SERVICE_P ORT	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_EXTERNA LDB_URL is set.	**${KIE_SERVER_EXT ERNALDB_SERVICE _PORT}**
	RHPAM_JNDI	Database JNDI name used by application to resolve the datasource, e.g. java:/jboss/datasources /ExampleDS.	**${KIE_SERVER_EXT ERNALDB_JNDI}**
	RHPAM_DRIVER	The predefined driver name, available values are mysql, postgresql or the preferred name for the external driver.	**${KIE_SERVER_EXT ERNALDB_DRIVER}**
	RHPAM_USERNAME	KIE server external database username.	**${KIE_SERVER_EXT ERNALDB_USER}**
	RHPAM_PASSWORD	KIE server external database password.	**${KIE_SERVER_EXT ERNALDB_PWD}**
	RHPAM_NONXA	Sets the datasources type. It can be XA or NONXA. For non XA set it to true. Default value is false.	**${KIE_SERVER_EXT ERNALDB_NONXA}**
	RHPAM_URL	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.	**${KIE_SERVER_EXT ERNALDB_URL}**

Deployment	Variable name	Description	Example value
	RHPAM_XA_CONNE CTION_PROPERTY_ URL	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.	**${KIE_SERVER_EXT ERNALDB_URL}**
	RHPAM_MIN_POOL_ SIZE	Sets xa-pool/min-pool-size for the configured datasource.	**${KIE_SERVER_EXT ERNALDB_MIN_PO OL_SIZE}**
	RHPAM_MAX_POOL _SIZE	Sets xa-pool/max-pool-size for the configured datasource.	**${KIE_SERVER_EXT ERNALDB_MAX_PO OL_SIZE}**
	RHPAM_CONNECTI ON_CHECKER	An org.jboss.jca.adapters.jd bc.ValidConnectionChe cker that provides a SQLException isValidConnection(Conn ection e) method to validate if a connection is valid.	**${KIE_SERVER_EXT ERNALDB_CONNEC TION_CHECKER}**
	RHPAM_EXCEPTION _SORTER	An org.jboss.jca.adapters.jd bc.ExceptionSorter that provides a boolean isExceptionFatal(SQLEx ception e) method to validate if an exception should be broadcast to all javax.resource.spi.Conne ctionEventListener as a connectionErrorOccurre d.	**${KIE_SERVER_EXT ERNALDB_EXCEPTI ON_SORTER}**
	RHPAM_BACKGRO UND_VALIDATION	Sets the sql validation method to background-validation, if set to false the validate-on-match method will be used.	**${KIE_SERVER_EXT ERNALDB_BACKGR OUND_VALIDATION}**

Deployment	Variable name	Description	Example value
	RHPAM_VALIDATION_MILLIS	Defines the interval for the background-validation check for the jdbc connections.	**${KIE_SERVER_EXTERNALDB_BACKGROUND_VALIDATION_MILLIS}**
	RHPAM_DRIVER_TYPE	KIE server external database driver type, applicable only for DB2, possible values are 4 (default) or 2.	**${KIE_SERVER_EXTERNALDB_DRIVER_TYPE}**
	RHPAM_JTA	–	true
	TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL	Sets refresh-interval for the EJB timer database data-store service.	**${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}**
	HTTPS_KEYSTORE_DIR	–	**/etc/kieserver-secret-volume**
	HTTPS_KEYSTORE	The name of the keystore file within the secret.	**${KIE_SERVER_HTTPS_KEYSTORE}**
	HTTPS_NAME	The name associated with the server certificate.	**${KIE_SERVER_HTTPS_NAME}**
	HTTPS_PASSWORD	The password for the keystore and certificate.	**${KIE_SERVER_HTTPS_PASSWORD}**
	JGROUPS_PING_PROTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PING_SERVICE_NAME	–	**${APPLICATION_NAME}-kieserver-ping**
	OPENSHIFT_DNS_PING_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL.	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO Realm name.	**${SSO_REALM}**

Deployment	Variable name	Description	Example value
	SSO_SECRET	KIE Server RH-SSO Client Secret.	**${KIE_SERVER_SSO _SECRET}**
	SSO_CLIENT	KIE Server RH-SSO Client name.	**${KIE_SERVER_SSO _CLIENT}**
	SSO_USERNAME	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	**${SSO_USERNAME}**
	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client.	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_ CERTIFICATE_VALI DATION	RH-SSO Disable SSL Certificate Validation.	**${SSO_DISABLE_SS L_CERTIFICATE_VA LIDATION}**
	SSO_PRINCIPAL_AT TRIBUTE	RH-SSO Principal Attribute to use as username.	**${SSO_PRINCIPAL_ ATTRIBUTE}**
	HOSTNAME_HTTP	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTP}**
	HOSTNAME_HTTPS	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTPS}**
	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication.	**${AUTH_LDAP_URL}**
	AUTH_LDAP_BIND_ DN	Bind DN used for authentication.	**${AUTH_LDAP_BIND _DN}**
	AUTH_LDAP_BIND_ CREDENTIAL	LDAP Credentials used for authentication.	**${AUTH_LDAP_BIND _CREDENTIAL}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_JAAS_ SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	**${AUTH_LDAP_JAA S_SECURITY_DOMA IN}**
	AUTH_LDAP_BASE_ CTX_DN	LDAP Base DN of the top-level context to begin the user search.	**${AUTH_LDAP_BAS E_CTX_DN}**
	AUTH_LDAP_BASE_ FILTER	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}).	**${AUTH_LDAP_BAS E_FILTER}**
	AUTH_LDAP_SEAR CH_SCOPE	The search scope to use.	**${AUTH_LDAP_SEA RCH_SCOPE}**
	AUTH_LDAP_SEAR CH_TIME_LIMIT	The timeout in milliseconds for user or role searches.	**${AUTH_LDAP_SEA RCH_TIME_LIMIT}**
	AUTH_LDAP_DISTIN GUISHED_NAME_AT TRIBUTE	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	**${AUTH_LDAP_DIST INGUISHED_NAME_ ATTRIBUTE}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE_USERNAME	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 usernameBeginString and usernameEndString.	**${AUTH_LDAP_PARSE_USERNAME}**
	AUTH_LDAP_USERNAME_BEGIN_STRING	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USERNAME_BEGIN_STRING}**
	AUTH_LDAP_USERNAME_END_STRING	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USERNAME_END_STRING}**
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	Name of the attribute containing the user roles.	**${AUTH_LDAP_ROLE_ATTRIBUTE_ID}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE S_CTX_DN	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.	**${AUTH_LDAP_ROL ES_CTX_DN}**
	AUTH_LDAP_ROLE_ FILTER	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member= {0}). An alternative that matches on the authenticated userDN is (member={1}).	**${AUTH_LDAP_ROL E_FILTER}**
	AUTH_LDAP_ROLE_ RECURSION	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	**${AUTH_LDAP_ROL E_RECURSION}**
	AUTH_LDAP_DEFA ULT_ROLE	A role included for all authenticated users.	**${AUTH_LDAP_DEF AULT_ROLE}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	**${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}**
	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	**${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}**
	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	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.	**${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK	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.	${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}
	AUTH_ROLE_MAPPER_ROLES_PROPERTIES	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	${AUTH_ROLE_MAPPER_ROLES_PROPERTIES}
	AUTH_ROLE_MAPPER_REPLACE_ROLE	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	${AUTH_ROLE_MAPPER_REPLACE_ROLE}

5.4.2.4.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
${APPLICATION_NAME}-kieserver	kieserver-keystore-volume	/etc/kieserver-secret-volume	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. RHPAM74-KIESERVER-MYSQL.YAML TEMPLATE

Application template for a managed KIE Server with a MySQL database, for Red Hat Process Automation Manager 7.4

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
APPLICATION_ NAME	–	The name for the application.	myapp	True
MAVEN_MIRRO R_URL	**MAVEN_MIRRO R_URL**	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for building and deploying your services.	–	False
MAVEN_MIRRO R_OF	**MAVEN_MIRRO R_OF**	Maven mirror configuration for KIE server.	external:*	False

Variable name	Image Environment Variable	Description	Example value	Required
MAVEN_REPO_ID	**EXTERNAL_MA VEN_REPO_ID**	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
MAVEN_REPO_ URL	**EXTERNAL_MA VEN_REPO_UR L**	Fully qualified URL to a Maven repository or service.	[http://nexus.nexu s-project.svc.cluster. local:8081/nexus/ content/groups/p ublic/](http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/)	True
MAVEN_REPO_ USERNAME	**EXTERNAL_MA VEN_REPO_US ERNAME**	Username to access the Maven repository, if required.	–	False
MAVEN_REPO_ PASSWORD	**EXTERNAL_MA VEN_REPO_PA SSWORD**	Password to access the Maven repository, if required.	–	False
BUSINESS_CEN TRAL_SERVICE	**WORKBENCH_ SERVICE_NAME**	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
BUSINESS_CEN TRAL_MAVEN_ USERNAME	**RHPAMCENTR_ MAVEN_REPO_ USERNAME**	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
BUSINESS_CEN TRAL_MAVEN_ PASSWORD	**RHPAMCENTR_ MAVEN_REPO_ PASSWORD**	Password to access the Maven service hosted by Business Central inside EAP.	maven1!	False
KIE_ADMIN_US ER	**KIE_ADMIN_US ER**	KIE administrator username.	adminUser	False
KIE_ADMIN_PW D	**KIE_ADMIN_PW D**	KIE administrator password.	–	False
KIE_SERVER_U SER	**KIE_SERVER_U SER**	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False
KIE_SERVER_P WD	**KIE_SERVER_P WD**	KIE server password. (Sets the org.kie.server.pwd system property)	–	False

Variable name	Image Environment Variable	Description	Example value	Required
IMAGE_STREAM_NAMESPACE	–	Namespace in which the ImageStreams for Red Hat Middleware 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
KIE_SERVER_IMAGE_STREAM_NAME	–	The name of the image stream to use for KIE server. Default is "rhpam74-kieserver-openshift".	rhpam74-kieserver-openshift	True
IMAGE_STREAM_TAG	–	A named pointer to an image in an image stream. Default is "1.0".	1.0	True
KIE_SERVER_PERSISTENCE_DS	KIE_SERVER_PERSISTENCE_DS	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
MYSQL_IMAGE _STREAM_NAM ESPACE	–	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/projec t. Default is "openshift".	openshift	False
MYSQL_IMAGE _STREAM_TAG	–	The MySQL image version, which is intended to correspond to the MySQL version. Default is "5.7".	5.7	False
KIE_SERVER_M YSQL_USER	**RHPAM_USERN AME**	KIE server MySQL database username.	rhpam	False
KIE_SERVER_M YSQL_PWD	**RHPAM_PASSW ORD**	KIE server MySQL database password.	–	False
KIE_SERVER_M YSQL_DB	**RHPAM_DATAB ASE**	KIE server MySQL database name.	rhpam7	False
DB_VOLUME_C APACITY	–	Size of persistent storage for the database volume.	1Gi	True
KIE_SERVER_M YSQL_DIALECT	**KIE_SERVER_P ERSISTENCE_D IALECT**	KIE server MySQL Hibernate dialect.	org.hibernate.diale ct.MySQL57Dialec t	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_M ODE	**KIE_SERVER_M ODE**	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.mod e system property).	**PRODUCTION**	False
KIE_MBEANS	**KIE_MBEANS**	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbean s system properties)	enabled	False
DROOLS_SERV ER_FILTER_CL ASSES	**DROOLS_SERV ER_FILTER_CL ASSES**	KIE server class filtering. (Sets the org.drools.server.fil ter.classes system property)	true	False
PROMETHEUS_ SERVER_EXT_D ISABLED	**PROMETHEUS_ SERVER_EXT_D ISABLED**	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheu s.server.ext.disable d system property)	false	False

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

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_B YPASS_AUTH_ USER	**KIE_SERVER_B YPASS_AUTH_ USER**	Allows the KIE server to bypass the authenticated user for task related operations e.g. queries. (Sets the org.kie.server.bypa ss.auth.user system property)	false	False
TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL	**TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL**	Sets refresh-interval for the EJB timer database data-store service.	30000	False
KIE_SERVER_M EMORY_LIMIT	–	KIE server Container memory limit.	1Gi	False
KIE_SERVER_C ONTAINER_DE PLOYMENT	**KIE_SERVER_C ONTAINER_DE PLOYMENT**	KIE Server Container deployment configuration in format: containerId=groupI d:artifactId:version |c2=g2:a2:v2	rhpam-kieserver-library=org.opensh ift.quickstarts:rhpa m-kieserver-library:1.5.0-SNAPSHOT	False
KIE_SERVER_M GMT_DISABLE D	**KIE_SERVER_M GMT_DISABLE D**	Disable management api and don't allow KIE containers to be deployed/undeplo yed or started/stopped sets the property org.kie.server.mgm t.api.disabled to true and org.kie.server.start up.strategy to LocalContainersSt artupStrategy.	true	False

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

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_J AAS_SECURITY _DOMAIN	**AUTH_LDAP_J AAS_SECURITY _DOMAIN**	The JMX ObjectName of the JaasSecurityDoma in used to decrypt the password.	–	False
AUTH_LDAP_B ASE_CTX_DN	**AUTH_LDAP_B ASE_CTX_DN**	LDAP Base DN of the top-level context to begin the user search.	ou=users,ou=exam ple,ou=com	False
AUTH_LDAP_B ASE_FILTER	**AUTH_LDAP_B ASE_FILTER**	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
AUTH_LDAP_S EARCH_SCOPE	**AUTH_LDAP_S EARCH_SCOPE**	The search scope to use.	**SUBTREE_SCO PE**	False
AUTH_LDAP_S EARCH_TIME_L IMIT	**AUTH_LDAP_S EARCH_TIME_L IMIT**	The timeout in milliseconds for user or role searches.	10000	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	**AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE**	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
AUTH_LDAP_PARSE_USERNAME	**AUTH_LDAP_PARSE_USERNAME**	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 usernameBeginString and usernameEndString.	true	False
AUTH_LDAP_USERNAME_BEGIN_STRING	**AUTH_LDAP_USERNAME_BEGIN_STRING**	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_U SERNAME_END _STRING	**AUTH_LDAP_U SERNAME_END _STRING**	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False
AUTH_LDAP_R OLE_ATTRIBUT E_ID	**AUTH_LDAP_R OLE_ATTRIBUT E_ID**	Name of the attribute containing the user roles.	memberOf	False
AUTH_LDAP_R OLES_CTX_DN	**AUTH_LDAP_R OLES_CTX_DN**	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=exa mple,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_ROLE_FILTER	**AUTH_LDAP_ROLE_FILTER**	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
AUTH_LDAP_ROLE_RECURSION	**AUTH_LDAP_ROLE_RECURSION**	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
AUTH_LDAP_DEFAULT_ROLE	**AUTH_LDAP_DEFAULT_ROLE**	A role included for all authenticated users.	user	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	**AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID**	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	name	False
AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	**AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN**	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
AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	**AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN**	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
AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK	**AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK**	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
AUTH_ROLE_M APPER_ROLES _PROPERTIES	**AUTH_ROLE_M APPER_ROLES _PROPERTIES**	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,r ole2,role3	–	False
AUTH_ROLE_M APPER_REPLA CE_ROLE	**AUTH_ROLE_M APPER_REPLA CE_ROLE**	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
${APPLICATION_NAME}-kieserver	8080	http	All the KIE server web server's ports.
	8443	https	
${APPLICATION_NAME}-kieserver-ping	8888	ping	The JGroups ping port for clustering.
${APPLICATION_NAME}-mysql	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-${APPLICATION_NAME}-kieserver-http	none	**${KIE_SERVER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-kieserver-https	TLS passthrough	**${KIE_SERVER_HOSTNAME_HTTPS}**

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
${APPLICATION_NAME}-kieserver	ImageChange
${APPLICATION_NAME}-mysql	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
${APPLICATION_NAME}-kieserver	1
${APPLICATION_NAME}-mysql	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
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**

5.5.2.3.3.2. Image

Deployment	Image
${APPLICATION_NAME}-kieserver	**${KIE_SERVER_IMAGE_STREAM_NAME}**
${APPLICATION_NAME}-mysql	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
${APPLICATION_NAME}-kieserver	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
	ping	8888	**TCP**
${APPLICATION_NAME}-mysql	–	3306	**TCP**

5.5.2.3.3.6. Image Environment Variables

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

Deployment	Variable name	Description	Example value
	KIE_SERVER_MODE	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).	**${KIE_SERVER_MODE}**
	KIE_MBEANS	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	**${KIE_MBEANS}**
	DROOLS_SERVER_FILTER_CLASSES	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	**${DROOLS_SERVER_FILTER_CLASSES}**
	PROMETHEUS_SERVER_EXT_DISABLED	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	**${PROMETHEUS_SERVER_EXT_DISABLED}**
	KIE_SERVER_BYPASS_AUTH_USER	Allows the KIE server to bypass the authenticated user for task related operations e.g. queries. (Sets the org.kie.server.bypass.auth.user system property)	**${KIE_SERVER_BYPASS_AUTH_USER}**
	KIE_SERVER_ID	–	–
	KIE_SERVER_ROUTE_NAME	–	**${APPLICATION_NAME}-kieserver**

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

Deployment	Variable name	Description	Example value
	RHPAMCENTR_MAVEN_REPO_USERNAME	Username to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_USERNAME}**
	RHPAMCENTR_MAVEN_REPO_PASSWORD	Password to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_PASSWORD}**
	EXTERNAL_MAVEN_REPO_ID	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.	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Fully qualified URL to a Maven repository or service.	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Username to access the Maven repository, if required.	**${MAVEN_REPO_USERNAME}**
	EXTERNAL_MAVEN_REPO_PASSWORD	Password to access the Maven repository, if required.	**${MAVEN_REPO_PASSWORD}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_MGMT _DISABLED	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.str ategy to LocalContainersStartup Strategy.	**${KIE_SERVER_MG MT_DISABLED}**
	KIE_SERVER_STAR TUP_STRATEGY	–	OpenShiftStartupStrate gy
	KIE_SERVER_PERSI STENCE_DS	KIE server persistence datasource. (Sets the org.kie.server.persistenc e.ds system property)	**${KIE_SERVER_PER SISTENCE_DS}**
	DATASOURCES	–	**RHPAM**
	RHPAM_JNDI	KIE server persistence datasource. (Sets the org.kie.server.persistenc e.ds system property)	**${KIE_SERVER_PER SISTENCE_DS}**
	RHPAM_DATABASE	KIE server MySQL database name.	**${KIE_SERVER_MYS QL_DB}**
	RHPAM_DRIVER	–	mariadb
	KIE_SERVER_PERSI STENCE_DIALECT	KIE server MySQL Hibernate dialect.	**${KIE_SERVER_MYS QL_DIALECT}**
	RHPAM_USERNAME	KIE server MySQL database username.	**${KIE_SERVER_MYS QL_USER}**
	RHPAM_PASSWORD	KIE server MySQL database password.	**${KIE_SERVER_MYS QL_PWD}**
	RHPAM_SERVICE_H OST	–	**${APPLICATION_NA ME}-mysql**
	RHPAM_SERVICE_P ORT	–	3306

Deployment	Variable name	Description	Example value
	RHPAM_JTA	–	true
	TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL	Sets refresh-interval for the EJB timer database data-store service.	**${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}**
	HTTPS_KEYSTORE_DIR	–	**/etc/kieserver-secret-volume**
	HTTPS_KEYSTORE	The name of the keystore file within the secret.	**${KIE_SERVER_HTTPS_KEYSTORE}**
	HTTPS_NAME	The name associated with the server certificate.	**${KIE_SERVER_HTTPS_NAME}**
	HTTPS_PASSWORD	The password for the keystore and certificate.	**${KIE_SERVER_HTTPS_PASSWORD}**
	JGROUPS_PING_PROTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PING_SERVICE_NAME	–	**${APPLICATION_NAME}-kieserver-ping**
	OPENSHIFT_DNS_PING_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL.	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO Realm name.	**${SSO_REALM}**
	SSO_SECRET	KIE Server RH-SSO Client Secret.	**${KIE_SERVER_SSO_SECRET}**
	SSO_CLIENT	KIE Server RH-SSO Client name.	**${KIE_SERVER_SSO_CLIENT}**
	SSO_USERNAME	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	**${SSO_USERNAME}**

Deployment	Variable name	Description	Example value
	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client.	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_ CERTIFICATE_VALI DATION	RH-SSO Disable SSL Certificate Validation.	**${SSO_DISABLE_SS L_CERTIFICATE_VA LIDATION}**
	SSO_PRINCIPAL_AT TRIBUTE	RH-SSO Principal Attribute to use as username.	**${SSO_PRINCIPAL_ ATTRIBUTE}**
	HOSTNAME_HTTP	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTP}**
	HOSTNAME_HTTPS	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTPS}**
	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication.	**${AUTH_LDAP_URL}**
	AUTH_LDAP_BIND_ DN	Bind DN used for authentication.	**${AUTH_LDAP_BIND _DN}**
	AUTH_LDAP_BIND_ CREDENTIAL	LDAP Credentials used for authentication.	**${AUTH_LDAP_BIND _CREDENTIAL}**
	AUTH_LDAP_JAAS_ SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	**${AUTH_LDAP_JAA S_SECURITY_DOMA IN}**
	AUTH_LDAP_BASE_ CTX_DN	LDAP Base DN of the top-level context to begin the user search.	**${AUTH_LDAP_BAS E_CTX_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_BASE_FILTER	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}).	**${AUTH_LDAP_BASE_FILTER}**
	AUTH_LDAP_SEARCH_SCOPE	The search scope to use.	**${AUTH_LDAP_SEARCH_SCOPE}**
	AUTH_LDAP_SEARCH_TIME_LIMIT	The timeout in milliseconds for user or role searches.	**${AUTH_LDAP_SEARCH_TIME_LIMIT}**
	AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE	The name of the attribute in the user entry that contains the DN of the user. This may be necessary if the DN of the user itself contains special characters, backslash for example, that prevent correct user mapping. If the attribute does not exist, the entry's DN is used.	**${AUTH_LDAP_DISTINGUISHED_NAME_ATTRIBUTE}**
	AUTH_LDAP_PARSE_USERNAME	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 usernameBeginString and usernameEndString.	**${AUTH_LDAP_PARSE_USERNAME}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_USER NAME_BEGIN_STRI NG	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_BEGIN_STR ING}**
	AUTH_LDAP_USER NAME_END_STRING	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USE RNAME_END_STRIN G}**
	AUTH_LDAP_ROLE_ ATTRIBUTE_ID	Name of the attribute containing the user roles.	**${AUTH_LDAP_ROL E_ATTRIBUTE_ID}**
	AUTH_LDAP_ROLE S_CTX_DN	The fixed DN of the context to search for user roles. This is not the DN where the actual roles are, but the DN where the objects containing the user roles are. For example, in a Microsoft Active Directory server, this is the DN where the user account is.	**${AUTH_LDAP_ROL ES_CTX_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE_ FILTER	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}).	**${AUTH_LDAP_ROL E_FILTER}**
	AUTH_LDAP_ROLE_ RECURSION	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	**${AUTH_LDAP_ROL E_RECURSION}**
	AUTH_LDAP_DEFA ULT_ROLE	A role included for all authenticated users.	**${AUTH_LDAP_DEF AULT_ROLE}**
	AUTH_LDAP_ROLE_ NAME_ATTRIBUTE_I D	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	**${AUTH_LDAP_ROL E_NAME_ATTRIBUT E_ID}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	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.	**${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}**
	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	Whether or not the roleAttributeID contains the fully-qualified DN of a role object. If false, the role name is taken from the value of the roleNameAttributeId attribute of the context name. Certain directory schemas, such as Microsoft Active Directory, require this attribute to be set to true.	**${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}**
	AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK	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.	**${AUTH_LDAP_REFERRAL_USER_ATTRIBUTE_ID_TO_CHECK}**

Deployment	Variable name	Description	Example value
	AUTH_ROLE_MAPP ER_ROLES_PROPE RTIES	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,r ole3	**${AUTH_ROLE_MAP PER_ROLES_PROPE RTIES}**
	AUTH_ROLE_MAPP ER_REPLACE_ROLE	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	**${AUTH_ROLE_MAP PER_REPLACE_ROL E}**
${APPLICATION_NA ME}-mysql	**MYSQL_USER**	KIE server MySQL database username.	**${KIE_SERVER_MYS QL_USER}**
	MYSQL_PASSWORD	KIE server MySQL database password.	**${KIE_SERVER_MYS QL_PWD}**
	MYSQL_DATABASE	KIE server MySQL database name.	**${KIE_SERVER_MYS QL_DB}**

5.5.2.3.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
${APPLICATION _NAME}- kieserver	kieserver- keystore-volume	**/etc/kieserver- secret-volume**	ssl certs	True
${APPLICATION _NAME}-mysql	**${APPLICATION _NAME}-mysql- pvol**	**/var/lib/mysql/d ata**	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
${APPLICATION_NAME}-mysql-claim	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. RHPAM74-KIESERVER-POSTGRESQL.YAML TEMPLATE

Application template for a managed KIE Server with a PostgreSQL database, for Red Hat Process Automation Manager 7.4

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
APPLICATION_ NAME	–	The name for the application.	myapp	True
MAVEN_MIRRO R_URL	**MAVEN_MIRRO R_URL**	Maven mirror that the KIE server must use. If you configure a mirror, this mirror must contain all artifacts that are required for building and deploying your services.	–	False
MAVEN_MIRRO R_OF	**MAVEN_MIRRO R_OF**	Maven mirror configuration for KIE server.	external:*	False

Variable name	Image Environment Variable	Description	Example value	Required
MAVEN_REPO_ID	**EXTERNAL_MAVEN_REPO_ID**	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
MAVEN_REPO_URL	**EXTERNAL_MAVEN_REPO_URL**	Fully qualified URL to a Maven repository or service.	http://nexus.nexus-project.svc.cluster.local:8081/nexus/content/groups/public/	True
MAVEN_REPO_USERNAME	**EXTERNAL_MAVEN_REPO_USERNAME**	Username to access the Maven repository, if required.	–	False
MAVEN_REPO_PASSWORD	**EXTERNAL_MAVEN_REPO_PASSWORD**	Password to access the Maven repository, if required.	–	False
BUSINESS_CENTRAL_SERVICE	**WORKBENCH_SERVICE_NAME**	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
BUSINESS_CEN TRAL_MAVEN_ USERNAME	**RHPAMCENTR_ MAVEN_REPO_ USERNAME**	Username to access the Maven service hosted by Business Central inside EAP.	mavenUser	False
BUSINESS_CEN TRAL_MAVEN_ PASSWORD	**RHPAMCENTR_ MAVEN_REPO_ PASSWORD**	Password to access the Maven service hosted by Business Central inside EAP.	maven1!	False
KIE_ADMIN_US ER	**KIE_ADMIN_US ER**	KIE administrator username.	adminUser	False
KIE_ADMIN_PW D	**KIE_ADMIN_PW D**	KIE administrator password.	–	False
KIE_SERVER_U SER	**KIE_SERVER_U SER**	KIE server username. (Sets the org.kie.server.user system property)	executionUser	False
KIE_SERVER_P WD	**KIE_SERVER_P WD**	KIE server password. (Sets the org.kie.server.pwd system property)	–	False
IMAGE_STREA M_NAMESPACE	–	Namespace in which the ImageStreams for Red Hat Middleware 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/projec t.	openshift	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_I MAGE_STREAM _NAME	–	The name of the image stream to use for KIE server. Default is "rhpam74-kieserver-openshift".	rhpam74-kieserver-openshift	True
IMAGE_STREA M_TAG	–	A named pointer to an image in an image stream. Default is "1.0".	1.0	True
KIE_SERVER_P ERSISTENCE_D S	**KIE_SERVER_P ERSISTENCE_D S**	KIE server persistence datasource. (Sets the org.kie.server.persi stence.ds system property)	java:/jboss/dataso urces/rhpam	False
KIE_SERVER_P OSTGRESQL_U SER	**RHPAM_USERN AME**	KIE server PostgreSQL database username.	rhpam	False
KIE_SERVER_P OSTGRESQL_P WD	**RHPAM_PASSW ORD**	KIE server PostgreSQL database password.	–	False
KIE_SERVER_P OSTGRESQL_D B	**RHPAM_DATAB ASE**	KIE server PostgreSQL database name.	rhpam7	False

Variable name	Image Environment Variable	Description	Example value	Required
POSTGRESQL_IMAGE_STREAM_NAMESPACE	–	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
POSTGRESQL_IMAGE_STREAM_TAG	–	The PostgreSQL image version, which is intended to correspond to the PostgreSQL version. Default is "10".	10	False
POSTGRESQL_MAX_PREPARED_TRANSACTIONS	**POSTGRESQL_MAX_PREPARED_TRANSACTIONS**	Allows the PostgreSQL to handle XA transactions.	100	True
DB_VOLUME_CAPACITY	–	Size of persistent storage for the database volume.	1Gi	True
KIE_SERVER_POSTGRESQL_DIALECT	**KIE_SERVER_PERSISTENCE_DIALECT**	KIE server PostgreSQL Hibernate dialect.	org.hibernate.dialect.PostgreSQLDialect	True

Variable name	Image Environment Variable	Description	Example value	Required
KIE_SERVER_M ODE	**KIE_SERVER_M ODE**	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.mod e system property).	**PRODUCTION**	False
KIE_MBEANS	**KIE_MBEANS**	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbean s system properties)	enabled	False
DROOLS_SERV ER_FILTER_CL ASSES	**DROOLS_SERV ER_FILTER_CL ASSES**	KIE server class filtering. (Sets the org.drools.server.fil ter.classes system property)	true	False
PROMETHEUS_ SERVER_EXT_D ISABLED	**PROMETHEUS_ SERVER_EXT_D ISABLED**	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheu s.server.ext.disable d system property)	false	False

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

Variable name	Image Environment Variable	Description	Example value	Required
TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL	**TIMER_SERVIC E_DATA_STOR E_REFRESH_IN TERVAL**	Sets refresh-interval for the EJB timer database data-store service.	30000	False
KIE_SERVER_M EMORY_LIMIT	–	KIE server Container memory limit.	1Gi	False
KIE_SERVER_C ONTAINER_DE PLOYMENT	**KIE_SERVER_C ONTAINER_DE PLOYMENT**	KIE Server Container deployment configuration in format: containerId=groupI d:artifactId:version |c2=g2:a2:v2	rhpam-kieserver-library=org.opensh ift.quickstarts:rhpa m-kieserver-library:1.5.0-SNAPSHOT	False
KIE_SERVER_M GMT_DISABLE D	**KIE_SERVER_M GMT_DISABLE D**	Disable management api and don't allow KIE containers to be deployed/undeplo yed or started/stopped sets the property org.kie.server.mgm t.api.disabled to true and org.kie.server.start up.strategy to LocalContainersSt artupStrategy.	true	False
SSO_URL	**SSO_URL**	RH-SSO URL.	https://rh-sso.example.com/ auth	False
SSO_REALM	**SSO_REALM**	RH-SSO Realm name.	–	False
KIE_SERVER_S SO_CLIENT	**SSO_CLIENT**	KIE Server RH-SSO Client name.	–	False
KIE_SERVER_S SO_SECRET	**SSO_SECRET**	KIE Server RH-SSO Client Secret.	252793ed-7118-4ca8-8dab-5622fa97d892	False

Variable name	Image Environment Variable	Description	Example value	Required
SSO_USERNAME	SSO_USERNAME	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	–	False
SSO_PASSWORD	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client.	–	False
SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	SSO_DISABLE_SSL_CERTIFICATE_VALIDATION	RH-SSO Disable SSL Certificate Validation.	false	False
SSO_PRINCIPAL_ATTRIBUTE	SSO_PRINCIPAL_ATTRIBUTE	RH-SSO Principal Attribute to use as username.	preferred_username	False
AUTH_LDAP_URL	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication.	ldap://myldap.example.com	False
AUTH_LDAP_BIND_DN	AUTH_LDAP_BIND_DN	Bind DN used for authentication.	uid=admin,ou=users,ou=exmample,ou=com	False
AUTH_LDAP_BIND_CREDENTIAL	AUTH_LDAP_BIND_CREDENTIAL	LDAP Credentials used for authentication.	Password	False
AUTH_LDAP_JAAS_SECURITY_DOMAIN	AUTH_LDAP_JAAS_SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	–	False
AUTH_LDAP_BASE_CTX_DN	AUTH_LDAP_BASE_CTX_DN	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
AUTH_LDAP_B ASE_FILTER	**AUTH_LDAP_B ASE_FILTER**	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
AUTH_LDAP_S EARCH_SCOPE	**AUTH_LDAP_S EARCH_SCOPE**	The search scope to use.	**SUBTREE_SCO PE**	False
AUTH_LDAP_S EARCH_TIME_L IMIT	**AUTH_LDAP_S EARCH_TIME_L IMIT**	The timeout in milliseconds for user or role searches.	10000	False
AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE	**AUTH_LDAP_DI STINGUISHED_ NAME_ATTRIB UTE**	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
AUTH_LDAP_P ARSE_USERNA ME	**AUTH_LDAP_P ARSE_USERNA ME**	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 usernameBeginStri ng and usernameEndStrin g.	true	False
AUTH_LDAP_U SERNAME_BEG IN_STRING	**AUTH_LDAP_U SERNAME_BEG IN_STRING**	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False
AUTH_LDAP_U SERNAME_END _STRING	**AUTH_LDAP_U SERNAME_END _STRING**	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndStrin g and only taken into account if parseUsername is set to true.	–	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_ATTRIBUT E_ID	**AUTH_LDAP_R OLE_ATTRIBUT E_ID**	Name of the attribute containing the user roles.	memberOf	False
AUTH_LDAP_R OLES_CTX_DN	**AUTH_LDAP_R OLES_CTX_DN**	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=exa mple,ou=com	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_FILTER	**AUTH_LDAP_R OLE_FILTER**	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
AUTH_LDAP_R OLE_RECURSI ON	**AUTH_LDAP_R OLE_RECURSI ON**	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	1	False
AUTH_LDAP_D EFAULT_ROLE	**AUTH_LDAP_D EFAULT_ROLE**	A role included for all authenticated users	user	False

Variable name	Image Environment Variable	Description	Example value	Required
AUTH_LDAP_R OLE_NAME_AT TRIBUTE_ID	**AUTH_LDAP_R OLE_NAME_AT TRIBUTE_ID**	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	name	False
AUTH_LDAP_P ARSE_ROLE_N AME_FROM_DN	**AUTH_LDAP_P ARSE_ROLE_N AME_FROM_DN**	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
AUTH_LDAP_R OLE_ATTRIBUT E_IS_DN	**AUTH_LDAP_R OLE_ATTRIBUT E_IS_DN**	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
AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK	**AUTH_LDAP_R EFERRAL_USE R_ATTRIBUTE_I D_TO_CHECK**	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
AUTH_ROLE_M APPER_ROLES _PROPERTIES	**AUTH_ROLE_M APPER_ROLES _PROPERTIES**	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,r ole2,role3	–	False
AUTH_ROLE_M APPER_REPLA CE_ROLE	**AUTH_ROLE_M APPER_REPLA CE_ROLE**	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
${APPLICATION_NAME}-kieserver	8080	http	All the KIE server web server's ports.
	8443	https	
${APPLICATION_NAME}-kieserver-ping	8888	ping	The JGroups ping port for clustering.
${APPLICATION_NAME}-postgresql	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-${APPLICATION_NAME}-kieserver-http	none	**${KIE_SERVER_HOSTNAME_HTTP}**
${APPLICATION_NAME}-kieserver-https	TLS passthrough	**${KIE_SERVER_HOSTNAME_HTTPS}**

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
${APPLICATION_NAME}-kieserver	ImageChange
${APPLICATION_NAME}-postgresql	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
${APPLICATION_NAME}-kieserver	1
${APPLICATION_NAME}-postgresql	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
${APPLICATION_NAME}-kieserver	**${APPLICATION_NAME}-kieserver**

5.6.2.3.3.2. Image

Deployment	Image
${APPLICATION_NAME}-kieserver	**${KIE_SERVER_IMAGE_STREAM_NAME}**
${APPLICATION_NAME}-postgresql	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
${APPLICATION_NAME}-kieserver	jolokia	8778	**TCP**
	http	8080	**TCP**
	https	8443	**TCP**
	ping	8888	**TCP**
${APPLICATION_NAME}-postgresql	–	5432	**TCP**

5.6.2.3.3.6. Image Environment Variables

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

Deployment	Variable name	Description	Example value
	KIE_SERVER_MODE	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).	**${KIE_SERVER_MODE}**
	KIE_MBEANS	KIE server mbeans enabled/disabled. (Sets the kie.mbeans and kie.scanner.mbeans system properties)	**${KIE_MBEANS}**
	DROOLS_SERVER_FILTER_CLASSES	KIE server class filtering. (Sets the org.drools.server.filter.classes system property)	**${DROOLS_SERVER_FILTER_CLASSES}**
	PROMETHEUS_SERVER_EXT_DISABLED	If set to false, the prometheus server extension will be enabled. (Sets the org.kie.prometheus.server.ext.disabled system property)	**${PROMETHEUS_SERVER_EXT_DISABLED}**
	KIE_SERVER_BYPASS_AUTH_USER	Allows the KIE server to bypass the authenticated user for task related operations e.g. queries. (Sets the org.kie.server.bypass.auth.user system property)	**${KIE_SERVER_BYPASS_AUTH_USER}**
	KIE_SERVER_ID	–	–
	KIE_SERVER_ROUTE_NAME	–	**${APPLICATION_NAME}-kieserver**

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

Deployment	Variable name	Description	Example value
	RHPAMCENTR_MAVEN_REPO_USERNAME	Username to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_USERNAME}**
	RHPAMCENTR_MAVEN_REPO_PASSWORD	Password to access the Maven service hosted by Business Central inside EAP.	**${BUSINESS_CENTRAL_MAVEN_PASSWORD}**
	EXTERNAL_MAVEN_REPO_ID	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.	**${MAVEN_REPO_ID}**
	EXTERNAL_MAVEN_REPO_URL	Fully qualified URL to a Maven repository or service.	**${MAVEN_REPO_URL}**
	EXTERNAL_MAVEN_REPO_USERNAME	Username to access the Maven repository, if required.	**${MAVEN_REPO_USERNAME}**
	EXTERNAL_MAVEN_REPO_PASSWORD	Password to access the Maven repository, if required.	**${MAVEN_REPO_PASSWORD}**

Deployment	Variable name	Description	Example value
	KIE_SERVER_MGMT _DISABLED	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.str ategy to LocalContainersStartup Strategy.	**${KIE_SERVER_MG MT_DISABLED}**
	KIE_SERVER_STAR TUP_STRATEGY	–	OpenShiftStartupStrate gy
	KIE_SERVER_PERSI STENCE_DS	KIE server persistence datasource. (Sets the org.kie.server.persistenc e.ds system property)	**${KIE_SERVER_PER SISTENCE_DS}**
	DATASOURCES	–	**RHPAM**
	RHPAM_DATABASE	KIE server PostgreSQL database name.	**${KIE_SERVER_POS TGRESQL_DB}**
	RHPAM_DRIVER	–	postgresql
	RHPAM_USERNAME	KIE server PostgreSQL database username.	**${KIE_SERVER_POS TGRESQL_USER}**
	RHPAM_PASSWORD	KIE server PostgreSQL database password.	**${KIE_SERVER_POS TGRESQL_PWD}**
	RHPAM_SERVICE_H OST	–	**${APPLICATION_NA ME}-postgresql**
	RHPAM_SERVICE_P ORT	–	5432
	KIE_SERVER_PERSI STENCE_DIALECT	KIE server PostgreSQL Hibernate dialect.	**${KIE_SERVER_POS TGRESQL_DIALECT }**
	RHPAM_JTA	–	true

Deployment	Variable name	Description	Example value
	RHPAM_JNDI	KIE server persistence datasource. (Sets the org.kie.server.persistence.ds system property)	**${KIE_SERVER_PERSISTENCE_DS}**
	TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL	Sets refresh-interval for the EJB timer database data-store service.	**${TIMER_SERVICE_DATA_STORE_REFRESH_INTERVAL}**
	HTTPS_KEYSTORE_DIR	–	**/etc/kieserver-secret-volume**
	HTTPS_KEYSTORE	The name of the keystore file within the secret.	**${KIE_SERVER_HTTPS_KEYSTORE}**
	HTTPS_NAME	The name associated with the server certificate.	**${KIE_SERVER_HTTPS_NAME}**
	HTTPS_PASSWORD	The password for the keystore and certificate.	**${KIE_SERVER_HTTPS_PASSWORD}**
	JGROUPS_PING_PROTOCOL	–	openshift.DNS_PING
	OPENSHIFT_DNS_PING_SERVICE_NAME	–	**${APPLICATION_NAME}-kieserver-ping**
	OPENSHIFT_DNS_PING_SERVICE_PORT	–	8888
	SSO_URL	RH-SSO URL.	**${SSO_URL}**
	SSO_OPENIDCONNECT_DEPLOYMENTS	–	ROOT.war
	SSO_REALM	RH-SSO Realm name.	**${SSO_REALM}**
	SSO_SECRET	KIE Server RH-SSO Client Secret.	**${KIE_SERVER_SSO_SECRET}**
	SSO_CLIENT	KIE Server RH-SSO Client name.	**${KIE_SERVER_SSO_CLIENT}**

Deployment	Variable name	Description	Example value
	SSO_USERNAME	RH-SSO Realm Admin Username used to create the Client if it doesn't exist.	**${SSO_USERNAME}**
	SSO_PASSWORD	RH-SSO Realm Admin Password used to create the Client.	**${SSO_PASSWORD}**
	SSO_DISABLE_SSL_ CERTIFICATE_VALI DATION	RH-SSO Disable SSL Certificate Validation.	**${SSO_DISABLE_SS L_CERTIFICATE_VA LIDATION}**
	SSO_PRINCIPAL_AT TRIBUTE	RH-SSO Principal Attribute to use as username.	**${SSO_PRINCIPAL_ ATTRIBUTE}**
	HOSTNAME_HTTP	Custom hostname for http service route. Leave blank for default hostname, e.g.: insecure-<application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTP}**
	HOSTNAME_HTTPS	Custom hostname for https service route. Leave blank for default hostname, e.g.: <application-name>-kieserver-<project>.<default-domain-suffix>	**${KIE_SERVER_HOS TNAME_HTTPS}**
	AUTH_LDAP_URL	LDAP Endpoint to connect for authentication.	**${AUTH_LDAP_URL}**
	AUTH_LDAP_BIND_ DN	Bind DN used for authentication.	**${AUTH_LDAP_BIND _DN}**
	AUTH_LDAP_BIND_ CREDENTIAL	LDAP Credentials used for authentication.	**${AUTH_LDAP_BIND _CREDENTIAL}**
	AUTH_LDAP_JAAS_ SECURITY_DOMAIN	The JMX ObjectName of the JaasSecurityDomain used to decrypt the password.	**${AUTH_LDAP_JAA S_SECURITY_DOMA IN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_BASE_ CTX_DN	LDAP Base DN of the top-level context to begin the user search.	**${AUTH_LDAP_BAS E_CTX_DN}**
	AUTH_LDAP_BASE_ FILTER	LDAP search filter used to locate the context of the user to authenticate. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. A common example for the search filter is (uid= {0}).	**${AUTH_LDAP_BAS E_FILTER}**
	AUTH_LDAP_SEAR CH_SCOPE	The search scope to use.	**${AUTH_LDAP_SEA RCH_SCOPE}**
	AUTH_LDAP_SEAR CH_TIME_LIMIT	The timeout in milliseconds for user or role searches.	**${AUTH_LDAP_SEA RCH_TIME_LIMIT}**
	AUTH_LDAP_DISTIN GUISHED_NAME_AT TRIBUTE	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.	**${AUTH_LDAP_DIST INGUISHED_NAME_ ATTRIBUTE}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_PARSE_USERNAME	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 usernameBeginString and usernameEndString.	**${AUTH_LDAP_PARSE_USERNAME}**
	AUTH_LDAP_USERNAME_BEGIN_STRING	Defines the String which is to be removed from the start of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USERNAME_BEGIN_STRING}**
	AUTH_LDAP_USERNAME_END_STRING	Defines the String which is to be removed from the end of the DN to reveal the username. This option is used together with usernameEndString and only taken into account if parseUsername is set to true.	**${AUTH_LDAP_USERNAME_END_STRING}**
	AUTH_LDAP_ROLE_ATTRIBUTE_ID	Name of the attribute containing the user roles.	**${AUTH_LDAP_ROLE_ATTRIBUTE_ID}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE S_CTX_DN	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.	**${AUTH_LDAP_ROL ES_CTX_DN}**
	AUTH_LDAP_ROLE_ FILTER	A search filter used to locate the roles associated with the authenticated user. The input username or userDN obtained from the login module callback is substituted into the filter anywhere a {0} expression is used. The authenticated userDN is substituted into the filter anywhere a {1} is used. An example search filter that matches on the input username is (member= {0}). An alternative that matches on the authenticated userDN is (member={1}).	**${AUTH_LDAP_ROL E_FILTER}**
	AUTH_LDAP_ROLE_ RECURSION	The number of levels of recursion the role search will go below a matching context. Disable recursion by setting this to 0.	**${AUTH_LDAP_ROL E_RECURSION}**
	AUTH_LDAP_DEFA ULT_ROLE	A role included for all authenticated users	**${AUTH_LDAP_DEF AULT_ROLE}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID	Name of the attribute within the roleCtxDN context which contains the role name. If the roleAttributeIsDN property is set to true, this property is used to find the role object's name attribute.	**${AUTH_LDAP_ROLE_NAME_ATTRIBUTE_ID}**
	AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN	A flag indicating if the DN returned by a query contains the roleNameAttributeID. If set to true, the DN is checked for the roleNameAttributeID. If set to false, the DN is not checked for the roleNameAttributeID. This flag can improve the performance of LDAP queries.	**${AUTH_LDAP_PARSE_ROLE_NAME_FROM_DN}**
	AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN	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.	**${AUTH_LDAP_ROLE_ATTRIBUTE_IS_DN}**

Deployment	Variable name	Description	Example value
	AUTH_LDAP_REFER RAL_USER_ATTRIB UTE_ID_TO_CHECK	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.	**${AUTH_LDAP_REF ERRAL_USER_ATTR IBUTE_ID_TO_CHEC K}**
	AUTH_ROLE_MAPP ER_ROLES_PROPE RTIES	When present, the RoleMapping Login Module will be configured to use the provided file. This parameter defines the fully-qualified file path and name of a properties file or resource which maps roles to replacement roles. The format is original_role=role1,role2,r ole3	**${AUTH_ROLE_MAP PER_ROLES_PROPE RTIES}**
	AUTH_ROLE_MAPP ER_REPLACE_ROLE	Whether to add to the current roles, or replace the current roles with the mapped ones. Replaces if set to true.	**${AUTH_ROLE_MAP PER_REPLACE_ROL E}**
${APPLICATION_NA ME}-postgresql	**POSTGRESQL_USE R**	KIE server PostgreSQL database username.	**${KIE_SERVER_POS TGRESQL_USER}**
	POSTGRESQL_PAS SWORD	KIE server PostgreSQL database password.	**${KIE_SERVER_POS TGRESQL_PWD}**
	POSTGRESQL_DAT ABASE	KIE server PostgreSQL database name.	**${KIE_SERVER_POS TGRESQL_DB}**

Deployment	Variable name	Description	Example value
	POSTGRESQL_MAX _PREPARED_TRANS ACTIONS	Allows the PostgreSQL to handle XA transactions.	**${POSTGRESQL_MA X_PREPARED_TRAN SACTIONS}**

5.6.2.3.3.7. Volumes

Deployment	Name	mountPath	Purpose	readOnly
${APPLICATION _NAME}- kieserver	kieserver- keystore-volume	**/etc/kieserver- secret-volume**	ssl certs	True
${APPLICATION _NAME}- postgresql	**${APPLICATION _NAME}- postgresql-pvol**	**/var/lib/pgsql/da ta**	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
${APPLICATION_NAME}-postgresql-claim	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. OPENSHIFT 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 Monday, March 01, 2021.