Red Hat Decision Manager 7.1

Deploying a Red Hat Decision Manager authoring or managed server environment on Red Hat OpenShift Container Platform

Last Updated: 2018-10-12

Red Hat Decision Manager 7.1 Deploying a Red Hat Decision Manager authoring or managed 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 Decision Manager 7.1 authoring or managed server environment on Red Hat OpenShift Container Platform.

Table of Contents

PREFACE

As a system engineer, you can deploy a Red Hat Decision Manager authoring or managed environment on Red Hat OpenShift Container Platform to provide a platform for developing or running services and other business assets.

Prerequisites

- At least four gigabytes of memory must be available in the OpenShift cluster/namespace.
- The OpenShift project for the deployment must be created.
- You must be 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 must be enabled. Alternatively, if dynamic PV provisioning is not enabled, a sufficient persistent volume must be available. By default, Decision Central requires one 1Gi PV. You can change the PV size for Decision Central persistent storage in the template parameters.
- If you intend to use the Authoring High Availability template, which scales the Decision Central pod:
  - The image streams for Red Hat AMQ version 7.1 or later must be available in your OpenShift environment.
  - Your OpenShift environment must support 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 DECISION MANAGER ON RED HAT OPENSHIFT CONTAINER PLATFORM

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

In this solution, components of Red Hat Decision Manager are deployed as separate OpenShift pods. You can scale each of the pods up and down individually, providing as few or as many containers as necessary 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 Decision Manager are available on OpenShift:

- Decision Server, also known as *Execution Server* or *KIE Server*, is the infrastructure element that runs decision services and other deployable assets (collectively referred to as *services*) . All logic of the services runs on execution servers.
  You can freely scale up a Decision Server pod, providing as many copies as necessary, running on the same host or different hosts. As you scale a pod up or down, all its copies run the same services. OpenShift provides load balancing and a request can be handled by any of the pods.

  You can deploy a separate Decision 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 Decision Server pods as necessary.

- Decision Central is a web-based interactive environment for authoring services. It also provides a management console. You can use Decision Central to develop services and deploy them to Decision Servers.
  Decision Central is a centralized application. However, you can configure it for high availability, where multiple pods run and share the same data.

  Decision 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, Decision 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 Decision Central functionality is a technology preview.

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

The following environment types are typical:

- *Authoring or managed environment*: An environment architecture that can be used for creating and modifying services using Decision Central and also for running services on Decision Servers. It consists of pods that provide Decision Central for the authoring work and one or more Decision Servers for execution of the services. Each Decision Server is a pod that you can replicate by scaling it up or down as necessary. You can deploy and undeploy services on each Decision Server using Decision Central. For instructions about deploying this environment, see *Deploying a Red Hat Decision Manager authoring or 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 Decision 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 Decision 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. For instructions about deploying this environment, see *Deploying a Red Hat Decision Manager immutable server environment on Red Hat OpenShift Container Platform*.

You can also deploy a *trial* or evaluation environment. This environment includes Decision Central and a Decision 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 Decision Manager trial environment on Red Hat OpenShift Container Platform*.

To deploy a Red Hat Decision Manager environment on OpenShift, you can use the templates that are provided with Red Hat Decision Manager.

CHAPTER 2. PREPARING TO DEPLOY RED HAT DECISION MANAGER IN YOUR OPENSHIFT ENVIRONMENT

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

2.1. ENSURING THE AVAILABILITY OF IMAGE STREAMS

You must ensure that the image streams that are required for the deployment are available in your OpenShift environment. Some versions of the OpenShift environment include the necessary image streams. You must check if they are available. If they are not available, you must install the **`rhdm71-image-streams.yaml`** file.

Procedure

1. Run the following commands:

```
$ oc get imagestreamtag -n openshift | grep rhdm71-decisioncentral-openshift
$ oc get imagestreamtag -n openshift | grep rhdm71-kieserver-openshift
```

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

2. If the output of one or both of the commands is empty, download the **`rhdm-7.1.0-openshift-templates.zip`** product deliverable file from the Software Downloads page. Extract the **`rhdm71-image-streams.yaml`** file from it. Complete one of the following actions:

   - Run the following command:

```
$ oc create -f rhdm71-image-streams.yaml
```

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

2.2. CREATING THE SECRETS FOR DECISION SERVER

OpenShift uses objects called **`Secrets`** to hold sensitive information, such as passwords or keystores. See the Secrets chapter in the OpenShift documentation for more information.

You must create an SSL certificate for Decision 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 Decision Server. In a production environment, generate a valid signed certificate that matches the expected URL of the Decision Server. Save the keystore in a file named **`keystore.jks`**. Record the name of the certificate and the password of the keystore file.
   See Generate a SSL Encryption Key and Certificate for more information on how to create a keystore with self-signed or purchased SSL certificates.

2. 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 DECISION CENTRAL

If you are planning to deploy Decision Central in your OpenShift environment, you must create an SSL certificate for Decision Central and provide it to your OpenShift environment as a secret. Do not use the same certificate and keystore for Decision Central and for Decision Server.

Procedure

1. Generate an SSL keystore with a private and public key for SSL encryption for Decision Central. In a production environment, generate a valid signed certificate that matches the expected URL of the Decision Central. Save the keystore in a file named **keystore.jks**. Record the name of the certificate and the password of the keystore file.
   See Generate a SSL Encryption Key and Certificate for more information on how to create a keystore with self-signed or purchased SSL certificates.

2. Use the **oc** command to generate a secret named **decisioncentral-app-secret** from the new keystore file:

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

2.4. CHANGING GLUSTERFS CONFIGURATION

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

Procedure

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

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

Where **class-name** is the name of the default storage class. For 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**. For example:

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

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

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

Where **class-name** is the name of the default storage class. For example:

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

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

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

CHAPTER 3. AUTHORING OR MANAGED SERVER ENVIRONMENT

You can deploy an environment for creating and modifying services using Decision Central and for running them in Decision Servers managed by Decision Central. This environment consists of Decision Central and one or more Decision Servers.

You can use Decision Central both to develop services and to deploy them to one or several Decision Servers. For example, you can deploy test versions of services to one Decision Server and production versions to another Decision Server.

To avoid accidentally deploying wrong versions to a production Decision Server, you can create separate environments to author services (*authoring environment*) and to manage deployment of production services (*managed server environment*). You can use a shared external Maven repository between these environments, so that services developed in the authoring environment are available in the managed server environment. However, the procedures to deploy these environments are the same.

Depending on your needs, you can deploy either a single or high-availability Decision Central. A single Decision Central pod is not replicated; only a single copy of Decision Central is used. In an HA Decision Central deployment, you can scale Decision Central.

An HA Decision Central provides maximum reliability and responsiveness for authoring services, but has higher memory and storage requirements and also requires support for persistent volumes with ReadWriteMany mode.

IMPORTANT

In the current version, the high-availability functionality is a technology preview.

You can scale Decision Server pods as necessary in any version of the authoring or managed server environment.

To deploy an authoring or managed server environment, first deploy the single or high-availability Decision Central and a single Decision Server using the authoring template.

To add additional Decision Servers, you can deploy the Decision Server template in the same project.

3.1. DEPLOYING SINGLE DECISION CENTRAL AND ONE DECISION SERVER IN AN AUTHORING OR MANAGED SERVER ENVIRONMENT

To deploy single Decision Central and one Decision Server in an authoring or managed server environment, use the **`rhdm71-authoring.yaml`** template file. You can extract this file from the **`rhdm-7.1.0-openshift-templates.zip`** product deliverable file. You can download the file from the Software Downloads page.

Procedure

1. Use one of the following methods to deploy the template:
    - In the OpenShift Web UI, select **Add to Project** → **Import YAML / JSON** and then select or paste the **`rhdm71-authoring.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>/rhdm71-authoring.yaml -p
DECISION_CENTRAL_HTTPS_SECRET=decisioncentral-app-secret -p
KIE_SERVER_HTTPS_SECRET=kieserver-app-secret
```

In this command line:

- 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. You can view the template file to see descriptions for all parameters.

2. Set the following parameters as necessary:

- **Decision Central Server Keystore Secret Name** (**`DECISION_CENTRAL_HTTPS_SECRET`**): The name of the secret for Decision Central, as created in Section 2.3, “Creating the secrets for Decision Central”.
- **KIE Server Keystore Secret Name** (**`KIE_SERVER_HTTPS_SECRET`**): The name of the secret for Decision Server, as created in Section 2.2, “Creating the secrets for Decision Server”.
- **Application Name** (**`APPLICATION_NAME`**): The name of the OpenShift application. It is used in the default URLs for Decision Central and Decision 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) on the Decision Central that the Decision Server is to join.
- **Decision Central Server Certificate Name** (**`DECISION_CENTRAL_HTTPS_NAME`**): The name of the certificate in the keystore that you created in Section 2.3, “Creating the secrets for Decision Central”.
- **Decision Central Server Keystore Password** (**`DECISION_CENTRAL_HTTPS_PASSWORD`**): The password for the keystore that you created in Section 2.3, “Creating the secrets for Decision Central”.
- **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 Decision 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 Decision Server”.
- **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”), the namespace is **`openshift`**. If you have installed the image streams file, the namespace is the name of the OpenShift project.
  You can also set the following user names and passwords:
- **KIE Admin User** (**`KIE_ADMIN_USER`**) and **KIE Admin Password** (**`KIE_ADMIN_PWD`**): The user name and password for the administrative user in Decision Central.
- **KIE Server User** (**`KIE_SERVER_USER`**) and **KIE Server Password** (**`KIE_SERVER_PWD`**): The user name and password that a client application must use to connect to the Decision Server.

3. If you want to deploy additional Decision Servers and connect them to this Decision Central, set the following parameters:

   - **KIE Server Controller User** (**`KIE_SERVER_CONTROLLER_USER`**) and **KIE Server Controller Password** (**`KIE_SERVER_CONTROLLER_PWD`**): The user name and password that a Decision Server must use to connect to the Decision Central.

4. If you want to place the built KJAR files into an external Maven repository, set the following parameters:

   - **Maven repository URL** (**`MAVEN_REPO_URL`**): The URL for the Maven repository.
   - **Maven repository username** (**`MAVEN_REPO_USERNAME`**): The user name for the Maven repository.
   - **Maven repository password** (**`MAVEN_REPO_PASSWORD`**): The password for the Maven repository.
   - **Maven repository ID** (**`MAVEN_REPO_ID`**): The Maven ID, which must match the **`id`** setting for the Maven repository.
     Alternatively, if you want to use the Maven repository that is built into Decision Central and to connect additional Decision Servers to the Decision Central, set the following parameters:
   - **Username for the Maven service hosted by Decision Central** (**`DECISION_CENTRAL_MAVEN_USERNAME`**): The user name for the built-in Maven repository.
   - **Password for the Maven service hosted by Decision Central** (**`DECISION_CENTRAL_MAVEN_PASSWORD`**): The password for the built-in Maven repository.

5. If you want to use RH-SSO or LDAP authentication, complete the following additional configuration:

   a. In the RH-SSO or 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,kiemgmt,Administrators`**
      - **`KIE_SERVER_CONTROLLER_USER`**: default user name **`controllerUser`**, roles: **`kie-server,rest-all,guest`**
      - **`DECISION_CENTRAL_MAVEN_USERNAME`** (not needed if you configure the use of an external Maven repository): default user name **`mavenUser`**. No roles are required.
      - **`KIE_SERVER_USER`**: default user name **`executionUser`**, roles **`kie-server,rest-all,guest`**

   b. If you want to configure Red Hat Single Sign On (RH-SSO) authentication, an RH-SSO realm that applies to Red Hat Decision Manager must exist. Decision Server. If the client does not yet exist, the template can create it during deployment. Clients within RH-SSO must also exist for Decision Central and for Decision Server. If the clients do not yet exist, the template can create them during deployment.
      For the user roles that you can configure in RH-SSO, see Roles and users.

      Use one of the following procedures:

i. If the clients for Red Hat Decision Manager within RH-SSO already exist, set the following parameters in the template:

- **RH-SSO URL** (**`SSO_URL`**): The URL for RH-SSO.
- **RH-SSO Realm name** (**`SSO_REALM`**): The RH-SSO realm for Red Hat Decision Manager.
- **Decision Central RH-SSO Client name** (**`DECISION_CENTRAL_SSO_CLIENT`**): The RH-SSO client name for Decision Central.
- **Decision Central RH-SSO Client Secret** (**`DECISION_CENTRAL_SSO_SECRET`**): The secret string that is set in RH-SSO for the client for Decision Central.
- **KIE Server RH-SSO Client name** (**`KIE_SERVER_SSO_CLIENT`**): The RH-SSO client name for Decision Server.
- **KIE Server RH-SSO Client Secret** (**`KIE_SERVER_SSO_SECRET`**): The secret string that is set in RH-SSO for the client for Decision Server.
- **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.

ii. To create the clients for Red Hat Decision Manager within RH-SSO, set the following parameters in the template:

- **RH-SSO URL** (**`SSO_URL`**): The URL for RH-SSO.
- **RH-SSO Realm name** (**`SSO_REALM`**): The RH-SSO realm for Red Hat Decision Manager.
- **Decision Central RH-SSO Client name** (**`DECISION_CENTRAL_SSO_CLIENT`**): The name of the client to create in RH-SSO for Decision Central.
- **Decision Central RH-SSO Client Secret** (**`DECISION_CENTRAL_SSO_SECRET`**): The secret string to set in RH-SSO for the client for Decision Central.
- **Decision Central Custom http Route Hostname** (**`DECISION_CENTRAL_HOSTNAME_HTTP`**): The fully qualified host name to use for the HTTP endpoint for Decision Central. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **Decision Central Custom https Route Hostname** (**`DECISION_CENTRAL_HOSTNAME_HTTPS`**): The fully qualified host name to use for the HTTPS endpoint for Decision Central. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **KIE Server RH-SSO Client name** (**`KIE_SERVER_SSO_CLIENT`**): The name of the client to create in RH-SSO for Decision Server.
- **KIE Server RH-SSO Client Secret** (**`KIE_SERVER_SSO_SECRET`**): The secret string to set in RH-SSO for the client for Decision Server.
- **KIE Server Custom http Route Hostname** (**`KIE_SERVER_HOSTNAME_HTTP`**): The fully qualified host name to use for the HTTP endpoint for Decision Server. If you need to create a client in RH-SSO, you can not leave this parameter blank.

- **KIE Server Custom https Route Hostname** (`KIE_SERVER_HOSTNAME_HTTPS`): The fully qualified host name to use for the HTTPS endpoint for Decision Server. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **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 Decision 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.

c. To configure LDAP, set the `AUTH_LDAP*` parameters of the template. These parameters correspond to the settings of the LdatExtended Login module of Red Hat JBoss EAP. For instructions about using these settings, see LdapExtended Login Module.
Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

6. Complete the creation of the environment, depending on the method that you are using:
   - In the OpenShift Web UI, click **Create**.
   - Complete and run the command line.

3.2. DEPLOYING HIGH-AVAILABILITY DECISION CENTRAL AND ONE DECISION SERVER IN AN AUTHORING OR MANAGED SERVER ENVIRONMENT

To deploy high-availability Decision Central and one Decision Server in an authoring or managed server environment, use the `rhdm71-authoring-ha.yaml` template file. You can download the file from the Software Downloads page.

IMPORTANT

In the current version, the high-availability functionality is a technology preview.

Procedure

1. Use one of the following methods to deploy the template:
   - In the OpenShift Web UI, select **Add to Project** → **Import YAML / JSON** and then select or paste the `rhdm71-authoring-ha.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>/rhdm71-authoring-ha.yaml -p
     DECISION_CENTRAL_HTTPS_SECRET=decisioncentral-app-secret -p
     KIE_SERVER_HTTPS_SECRET=kieserver-app-secret
     ```

     In this command line:
     - 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. You can view the template file to see descriptions for all parameters.

2. Set the following parameters as necessary:

- **Decision Central Server Keystore Secret Name** (**`DECISION_CENTRAL_HTTPS_SECRET`**): The name of the secret for Decision Central, as created in Section 2.3, “Creating the secrets for Decision Central”.
- **KIE Server Keystore Secret Name** (**`KIE_SERVER_HTTPS_SECRET`**): The name of the secret for Decision Server, as created in Section 2.2, “Creating the secrets for Decision Server”.
- **Application Name** (**`APPLICATION_NAME`**): The name of the OpenShift application. It is used in the default URLs for Decision Central and Decision 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) on the Decision Central that the Decision Server is to join.
- **Decision Central Server Certificate Name** (**`DECISION_CENTRAL_HTTPS_NAME`**): The name of the certificate in the keystore that you created in Section 2.3, “Creating the secrets for Decision Central”.
- **Decision Central Server Keystore Password** (**`DECISION_CENTRAL_HTTPS_PASSWORD`**): The password for the keystore that you created in Section 2.3, “Creating the secrets for Decision Central”.
- **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 Decision 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 Decision Server”.
- **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”), the namespace is **`openshift`**. If you have installed the image streams file, the namespace is the name of the OpenShift project.
  You can also set the following user names and passwords:
- **KIE Admin User** (**`KIE_ADMIN_USER`**) and **KIE Admin Password** (**`KIE_ADMIN_PWD`**): The user name and password for the administrative user in Decision Central.
- **KIE Server User** (**`KIE_SERVER_USER`**) and **KIE Server Password** (**`KIE_SERVER_PWD`**): The user name and password that a client application must use to connect to the Decision Server.

3. If you want to deploy additional Decision Servers and connect them to this Decision Central, set the following parameters:

- **KIE Server Controller User** (**`KIE_SERVER_CONTROLLER_USER`**) and **KIE Server Controller Password** (**`KIE_SERVER_CONTROLLER_PWD`**): The user name and password that a Decision Server must use to connect to the Decision Central.

4. If you want to place the built KJAR files into an external Maven repository, set the following parameters:
   - **Maven repository URL** (`MAVEN_REPO_URL`): The URL for the Maven repository.
   - **Maven repository username** (`MAVEN_REPO_USERNAME`): The user name for the Maven repository.
   - **Maven repository password** (`MAVEN_REPO_PASSWORD`): The password for the Maven repository.
   - **Maven repository ID** (`MAVEN_REPO_ID`): The Maven ID, which must match the `id` setting for the Maven repository.
     Alternatively, if you want to use the Maven repository that is built into Decision Central and to connect additional Decision Servers to the Decision Central, set the following parameters:
   - **Username for the Maven service hosted by Decision Central** (`DECISION_CENTRAL_MAVEN_USERNAME`): The user name for the built-in Maven repository.
   - **Password for the Maven service hosted by Decision Central** (`DECISION_CENTRAL_MAVEN_PASSWORD`): The password for the built-in Maven repository.
5. If you want to use RH-SSO or LDAP authentication, complete the following additional configuration:
   a. In the RH-SSO or 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,kiemgmt,Administrators`
      - `KIE_SERVER_CONTROLLER_USER`: default user name `controllerUser`, roles: `kie-server,rest-all,guest`
      - `DECISION_CENTRAL_MAVEN_USERNAME` (not needed if you configure the use of an external Maven repository): default user name `mavenUser`. No roles are required.
      - `KIE_SERVER_USER`: default user name `executionUser`, roles `kie-server,rest-all,guest`

   b. If you want to configure Red Hat Single Sign On (RH-SSO) authentication, an RH-SSO realm that applies to Red Hat Decision Manager must exist. Decision Server. If the client does not yet exist, the template can create it during deployment. Clients within RH-SSO must also exist for Decision Central and for Decision Server. If the clients do not yet exist, the template can create them during deployment.
      For the user roles that you can configure in RH-SSO, see Roles and users.

      Use one of the following procedures:

      i. If the clients for Red Hat Decision Manager within RH-SSO already exist, set the following parameters in the template:
         - **RH-SSO URL** (`SSO_URL`): The URL for RH-SSO.

- **RH-SSO Realm name** (**`SSO_REALM`**): The RH-SSO realm for Red Hat Decision Manager.
- **Decision Central RH-SSO Client name** (**`DECISION_CENTRAL_SSO_CLIENT`**): The RH-SSO client name for Decision Central.
- **Decision Central RH-SSO Client Secret** (**`DECISION_CENTRAL_SSO_SECRET`**): The secret string that is set in RH-SSO for the client for Decision Central.
- **KIE Server RH-SSO Client name** (**`KIE_SERVER_SSO_CLIENT`**): The RH-SSO client name for Decision Server.
- **KIE Server RH-SSO Client Secret** (**`KIE_SERVER_SSO_SECRET`**): The secret string that is set in RH-SSO for the client for Decision Server.
- **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.

ii. To create the clients for Red Hat Decision Manager within RH-SSO, set the following parameters in the template:

- **RH-SSO URL** (**`SSO_URL`**): The URL for RH-SSO.
- **RH-SSO Realm name** (**`SSO_REALM`**): The RH-SSO realm for Red Hat Decision Manager.
- **Decision Central RH-SSO Client name** (**`DECISION_CENTRAL_SSO_CLIENT`**): The name of the client to create in RH-SSO for Decision Central.
- **Decision Central RH-SSO Client Secret** (**`DECISION_CENTRAL_SSO_SECRET`**): The secret string to set in RH-SSO for the client for Decision Central.
- **Decision Central Custom http Route Hostname** (**`DECISION_CENTRAL_HOSTNAME_HTTP`**): The fully qualified host name to use for the HTTP endpoint for Decision Central. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **Decision Central Custom https Route Hostname** (**`DECISION_CENTRAL_HOSTNAME_HTTPS`**): The fully qualified host name to use for the HTTPS endpoint for Decision Central. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **KIE Server RH-SSO Client name** (**`KIE_SERVER_SSO_CLIENT`**): The name of the client to create in RH-SSO for Decision Server.
- **KIE Server RH-SSO Client Secret** (**`KIE_SERVER_SSO_SECRET`**): The secret string to set in RH-SSO for the client for Decision Server.
- **KIE Server Custom http Route Hostname** (**`KIE_SERVER_HOSTNAME_HTTP`**): The fully qualified host name to use for the HTTP endpoint for Decision Server. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **KIE Server Custom https Route Hostname** (**`KIE_SERVER_HOSTNAME_HTTPS`**): The fully qualified host name to use for the HTTPS endpoint for Decision Server. If you need to create a client in RH-SSO, you can not leave this parameter blank.

- **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 Decision 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.

c. To configure LDAP, set the **`AUTH_LDAP*`** parameters of the template. These parameters correspond to the settings of the LdatExtended Login module of Red Hat JBoss EAP. For instructions about using these settings, see LdapExtended Login Module.
Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

6. If an AMQ 7.1 image is not available in the **`openshift`** namespace with default settings, set the following parameters:
   - **AMQ ImageStream Namespace** (**`AMQ_IMAGE_STREAM_NAMESPACE`**): Namespace in which the ImageStream for the AMQ image is installed. The default setting is **`openshift`**.
   - **AMQ ImageStream Name** (**`AMQ_IMAGE_STREAM_NAME`**): The name of the image stream for the AMQ broker. The default setting is **`amq-broker71-openshift`**.
   - **AMQ ImageStream Tag** (**`AMQ_IMAGE_STREAM_TAG`**): The AMQ image stream tag. The default setting is **`1.0`**.
7. Complete the creation of the environment, depending on the method that you are using:
   - In the OpenShift Web UI, click **Create**.
   - Complete and run the command line.

3.3. DEPLOYING AN ADDITIONAL DECISION SERVER

As a part of a managed server infrastructure, you can deploy an additional Decision Server on the OpenShift infrastructure. You can then use Decision Central to deploy, undeploy, and manage services on this Decision Server.

To deploy an additional Decision Server, use the **`rhdm71-kieserver.yaml`** template file. You can download the file from the Software Downloads page.

Procedure

1. Use one of the following methods to deploy the template:
   - In the OpenShift Web UI, select **Add to Project** → **Import YAML / JSON** and then select or paste the **`rhdm71-kieserver.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>/rhdm71-kieserver.yaml -p
     KIE_SERVER_HTTPS_SECRET=kieserver-app-secret
     ```

     In this command line:

- 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. You can view the template file to see descriptions for all parameters.

2. Set the following parameters:
   - **KIE server controller service** (**KIE_SERVER_CONTROLLER_SERVICE**): The OpenShift service name for the Decision Central that you installed for this environment.
   - **KIE server controller user** (**KIE_SERVER_CONTROLLER_USER**): The controller user name for logging onto the Decision Central that you configured.
   - **KIE server controller password** (**KIE_SERVER_CONTROLLER_PWD**): The controller password for logging onto the Decision Central that you configured.
   - **KIE Server Keystore Secret Name** (**KIE_SERVER_HTTPS_SECRET**): The name of the secret for Decision Server, as created in Section 2.2, “Creating the secrets for Decision Server”.
   - **Application Name** (**APPLICATION_NAME**): The name of the OpenShift application. It is used in the default URL for Decision 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) on the Decision Central that the Decision Server is to join.
   - **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 Decision 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 Decision Server”.
3. Set the parameters for access to the Maven repository, depending on whether you configured the Decision Central to use the built-in or external repository:
   a. For a built-in repository:
      - **Name of the Maven service hosted by Decision Central** (**DECISION_CENTRAL_MAVEN_SERVICE**): The service name for the built-in Maven repository of the Decision Central.
      - **Username for the Maven service hosted by Decision Central** (**DECISION_CENTRAL_MAVEN_USERNAME**): The user name for the built-in Maven repository of the Decision Central. Enter the user name that you configured for the Decision Central as **DECISION_CENTRAL_MAVEN_USERNAME**.
      - **Password to access the Maven service hosted by Decision Central** (**DECISION_CENTRAL_MAVEN_PASSWORD**): The password for the built-in Maven repository of the Decision Central. Enter the password that you configured for the Decision Central as **DECISION_CENTRAL_MAVEN_PASSWORD**.

   b. For an external repository:
      - **Maven repository URL** (**MAVEN_REPO_URL**): The URL for the Maven repository with services.

- **Maven repository username** (`MAVEN_REPO_USERNAME`): The user name for the Maven repository.
- **Maven repository password** (`MAVEN_REPO_PASSWORD`): The password for the Maven repository.

NOTE

You can set up access to both the built-in Maven repository of the Decision Central an external Maven repository if your services have dependencies in both repositories.

4. If you want to use RH-SSO or LDAP authentication, complete the following additional configuration:
   a. In the RH-SSO or 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,kiemgmt,Administrators`
      - `KIE_SERVER_USER`: default user name `executionUser`, roles `kie-server,rest-all,guest`
   b. If you want to configure Red Hat Single Sign On (RH-SSO) authentication, an RH-SSO realm that applies to Red Hat Decision Manager must exist. A client within RH-SSO must also exist for
      For the user roles that you can configure in RH-SSO, see Roles and users.

      Use one of the following procedures:

      i. If the client for Red Hat Decision Manager within RH-SSO already exists, set the following parameters in the template:
         - **RH-SSO URL** (`SSO_URL`): The URL for RH-SSO.
         - **RH-SSO Realm name** (`SSO_REALM`): The RH-SSO realm for Red Hat Decision Manager.
         - **KIE Server RH-SSO Client name** (`KIE_SERVER_SSO_CLIENT`): The RH-SSO client name for Decision Server.
         - **KIE Server RH-SSO Client Secret** (`KIE_SERVER_SSO_SECRET`): The secret string that is set in RH-SSO for the client for Decision Server.
         - **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.

      ii. To create the client for Red Hat Decision Manager within RH-SSO, set the following parameters in the template:
         - **RH-SSO URL** (`SSO_URL`): The URL for RH-SSO.

- **RH-SSO Realm name** (**`SSO_REALM`**): The RH-SSO realm for Red Hat Decision Manager.
- **KIE Server RH-SSO Client name** (**`KIE_SERVER_SSO_CLIENT`**): The name of the client to create in RH-SSO for Decision Server.
- **KIE Server RH-SSO Client Secret** (**`KIE_SERVER_SSO_SECRET`**): The secret string to set in RH-SSO for the client for Decision Server.
- **KIE Server Custom http Route Hostname** (**`KIE_SERVER_HOSTNAME_HTTP`**): The fully qualified host name to use for the HTTP endpoint for Decision Server. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **KIE Server Custom https Route Hostname** (**`KIE_SERVER_HOSTNAME_HTTPS`**): The fully qualified host name to use for the HTTPS endpoint for Decision Server. If you need to create a client in RH-SSO, you can not leave this parameter blank.
- **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 Decision 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.

c. To configure LDAP, set the **`AUTH_LDAP*`** parameters of the template. These parameters correspond to the settings of the LdatExtended Login module of Red Hat JBoss EAP. For instructions about using these settings, see LdapExtended Login Module.
Do not configure LDAP authentication and RH-SSO authentication in the same deployment.

5. Complete the creation of the environment, depending on the method that you are using:
   - In the OpenShift Web UI, click **Create**.
   - Complete and run the command line.

APPENDIX A. VERSIONING INFORMATION

Documentation last updated on Friday, October 12, 2018.