Red Hat Decision Manager 7.7

Deploying a Red Hat Decision Manager environment on Red Hat OpenShift Container Platform using Operators
Red Hat Decision Manager 7.7 Deploying a Red Hat Decision Manager environment on Red Hat OpenShift Container Platform using Operators

Red Hat Customer Content Services
brms-docs@redhat.com
Abstract

This document describes how to deploy a Red Hat Decision Manager 7.7 environment on Red Hat OpenShift Container Platform using Operators.
# Table of Contents

PREFACE .................................................................................................................. 3

CHAPTER 1. OVERVIEW OF RED HAT DECISION MANAGER ON RED HAT OPENSIFT CONTAINER PLATFORM .................................................................................. 4

CHAPTER 2. PREPARING TO DEPLOY RED HAT DECISION MANAGER IN YOUR OPENSIFT ENVIRONMENT .................................................................................. 5

2.1. ENSURING YOUR ENVIRONMENT IS AUTHENTICATED TO THE RED HAT REGISTRY 5
2.2. CREATING THE SECRETS FOR KIE SERVER 5
2.3. CREATING THE SECRETS FOR BUSINESS CENTRAL 6
2.4. CREATING THE SECRETS FOR THE AMQ BROKER CONNECTION 7
2.5. PROVISIONING PERSISTENT VOLUMES WITH READWRITE MANY ACCESS MODE USING NFS 7
2.6. PREPARING FOR DEPLOYMENT IN A RESTRICTED NETWORK 7
2.7. PREPARING A MAVEN MIRROR REPOSITORY FOR OFFLINE USE 8

CHAPTER 3. DEPLOYMENT AND MANAGEMENT OF A RED HAT DECISION MANAGER ENVIRONMENT USING OPENSIFT OPERATORS .............................................. 10

3.1. SUBSCRIBING TO THE BUSINESS AUTOMATION OPERATOR 10
3.2. DEPLOYING A RED HAT DECISION MANAGER ENVIRONMENT USING THE OPERATOR 10

3.2.1. Starting the deployment of a Red Hat Decision Manager environment using the Business Automation operator 10
3.2.2. Setting the basic configuration of the environment 11
3.2.3. Setting the security configuration of the environment 12
3.2.4. Setting the Business Central configuration of the environment 14
3.2.5. Setting custom KIE Server configuration of the environment 16

3.3. MODIFYING AN ENVIRONMENT THAT IS DEPLOYED USING OPERATORS 20
3.4. JVM CONFIGURATION PARAMETERS 21

APPENDIX A. VERSIONING INFORMATION .................................................................... 24
Red Hat Decision Manager 7.7 Deploying a Red Hat Decision Manager environment on Red Hat OpenShift Container Platform using Operators
PREFACE

As a system engineer, you can deploy a Red Hat Decision Manager environment on Red Hat OpenShift Container Platform to provide an infrastructure to develop or execute processes and other business assets. You can use OpenShift Operators to deploy the environment defined in a structured YAML file and to maintain and modify this environment as necessary.

Prerequisites

- A Red Hat OpenShift Container Platform environment is available. The Operator is supported on Red Hat OpenShift Container Platform version 4.1, 4.2, and 4.3.
- At least four gigabytes of memory are available in the OpenShift environment.
- The OpenShift project for the deployment is created.
- You are logged in to the project using the OpenShift 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 deployed components require the following PV sizes:
  - By default, Business Central requires one 1Gi PV. You can change the PV size for Business Central persistent storage.
- If you intend to scale any of the Business Central pods, your OpenShift environment supports persistent volumes with **ReadWriteMany** mode. If your environment does not support this mode, you can use NFS to provision the volumes. For information about access mode support in OpenShift public and dedicated clouds, 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 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 Decision Manager are available on OpenShift:

- **KIE Server**, also known as *Execution 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. In some templates, you can scale up a KIE 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 run the same services. OpenShift provides load balancing and a request can be handled by any of the pods.

  You can deploy a separate KIE 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 KIE Server pods as required.

- **Business Central** is a web-based interactive environment used for authoring services. It also provides a management console. You can use Business Central to develop services and deploy them to KIE Servers.

  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.

You can arrange these and other components into various environment configurations within OpenShift.
CHAPTER 2. PREPARING TO DEPLOY RED HAT DECISION MANAGER IN YOUR OPENSHIFT ENVIRONMENT

Before deploying Red Hat Decision 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 decision services or for other decision services.

2.1. ENSURING YOUR ENVIRONMENT IS AUTHENTICATED TO THE RED HAT REGISTRY

To deploy Red Hat Decision Manager components of Red Hat OpenShift Container Platform, you must ensure that OpenShift can download the correct images from the Red Hat registry.

OpenShift must be configured to authenticate with the Red Hat registry using your service account user name and password. This configuration is specific for a namespace, and if operators work, the configuration is already completed for the openshift namespace.

However, if the image streams for Red Hat Decision Manager are not found in the openshift namespace or if the operator is configured to update Red Hat Decision Manager to a new version automatically, the operator needs to download images into the namespace of your project. You must complete the authentication configuration for this namespace.

Procedure

1. Ensure you are logged in to OpenShift with the oc command and that your project is active.

2. Complete the steps documented in Registry Service Accounts for Shared Environments. You must log in to Red Hat Customer Portal to access the document and to complete the steps to create a registry service account.

3. Select the OpenShift Secret tab and click the link under Download secret to download the YAML secret file.

4. View the downloaded file and note the name that is listed in the name: entry.

5. Run 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.

2.2. CREATING THE SECRETS FOR KIE SERVER

OpenShift uses objects called secrets to hold sensitive information such as passwords or keystores. For more information about OpenShift secrets, see What is a secret in the OpenShift documentation.

In order to provide HTTPS access, KIE Server uses an SSL certificate. The deployment can create a sample secret automatically. However, in production environments you must create an SSL certificate for KIE 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 KIE 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 KIE 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 Decision Manager configuration is jboss.

4. Record the password of the keystore file. The default value for this name in Red Hat Decision 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

In order to provide HTTPS access, Business Central uses an SSL certificate. The deployment can create a sample secret automatically. However, in production environments you must create an SSL certificate for Business Central and provide it to your OpenShift environment as a secret.

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

Procedure

1. Generate an SSL keystore with a private and public key for SSL encryption for KIE 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 Decision Manager configuration is jboss.

4. Record the password of the keystore file. The default value for this name in Red Hat Decision Manager configuration is mykeystorepass.

5. Use the oc command to generate a secret named decisioncentral-app-secret from the new keystore file:
### 2.4. CREATING THE SECRETS FOR THE AMQ BROKER CONNECTION

If you want to connect any KIE Server to an AMQ broker and to use SSL for the AMQ broker connection, you must create an SSL certificate for the connection 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 KIE 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 the AMQ broker connection.

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 Decision Manager configuration is `jboss`.

4. Record the password of the keystore file. The default value for this name in Red Hat Decision Manager configuration is `mykeystorepass`.

5. Use the `oc` command to generate a secret named `broker-app-secret` from the new keystore file:

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

### 2.5. PROVISIONING PERSISTENT VOLUMES WITH **ReadWriteMany** ACCESS MODE USING NFS

If you want to deploy high-availability Business Central, your environment must provision persistent volumes with **ReadWriteMany** access mode.

If your configuration requires provisioning persistent volumes with **ReadWriteMany** access mode but your environment does not support such provisioning, use NFS to provision the volumes. Otherwise, skip this procedure.

**Procedure**

Deploy an NFS server and provision the persistent volumes using NFS. For information about provisioning persistent volumes using NFS, see the “Persistent storage using NFS” section of the [OpenShift Container Platform 4.3 Storage](#) guide.

### 2.6. PREPARING FOR DEPLOYMENT IN A RESTRICTED NETWORK
You can deploy Red Hat Decision Manager in a restricted network that is not connected to the public Internet. For instructions about operator deployment in a restricted network, see Using Operator Lifecycle Manager on restricted networks in Red Hat OpenShift Container Platform documentation.

**IMPORTANT**

In Red Hat Decision Manager 7.7, deployment on restricted networks is for Technology Preview only. For more information on Red Hat Technology Preview features, see Technology Preview Features Scope.

In order to use a deployment that does not have outgoing access to the public Internet, you must also prepare a Maven repository with a mirror of all the necessary artifacts. For instructions about creating this repository, see Section 2.7, “Preparing a Maven mirror repository for offline use”.

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

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

**NOTE**

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

#### Prerequisites

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

#### Procedure

1. Configure a Maven release repository to which you have write access. The repository must allow read access without authentication and your OpenShift environment must have network 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 in the Red Hat OpenShift Container Platform 3.11 documentation. The documented procedure is applicable to Red Hat OpenShift Container Platform version 4. Use this repository as a separate mirror repository.
   
   Alternatively, if you use a custom external repository (for example, Nexus) for your services, you can use the same repository as a mirror repository.

2. On the computer that has an outgoing connection to the public Internet, complete the following steps:
   
   
   b. Extract the contents of the rhdm-7.0-offliner.zip file into any directory.
   
   c. Change to the directory and enter the following command:

```
./offline-repo-builder.sh offliner.txt
```
This command creates a **repository** subdirectory and downloads the necessary artifacts into this subdirectory.

If a message reports that some downloads have failed, run the same command again. If downloads fail again, contact Red Hat support.

d. Upload all artifacts from the **repository** subdirectory to the Maven mirror repository that you prepared. You can use the Maven Repository Provisioner utility, available from the [Maven repository tools](https://maven.apache.org/download.html) Git repository, 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, available from the [Maven repository tools](https://maven.apache.org/download.html) Git repository, to upload the artifacts.
CHAPTER 3. DEPLOYMENT AND MANAGEMENT OF A RED HAT DECISION MANAGER ENVIRONMENT USING OPENShift OPERATORS

To deploy a Red Hat Decision Manager environment, the OpenShift Operator uses a YAML source that describes the environment. Red Hat Decision Manager provides an installer that you can use to form the YAML source and deploy the environment.

When the Business Automation operator deploys the environment, it creates a YAML description of the environment, and then ensures that the environment is consistent with the description at all times. You can edit the description to modify the environment.

3.1. SUBSCRIBING TO THE BUSINESS AUTOMATION OPERATOR

To be able to deploy Red Hat Decision Manager using operators, you must subscribe to the Business Automation operator in OpenShift.

Procedure

1. Enter your project in the OpenShift Web cluster console.
2. In the OpenShift Web console navigation panel, select Catalog → OperatorHub or Operators → OperatorHub.
3. Search for Business Automation, select it and click Install.
4. On the Create Operator Subscription page, select your target namespace and approval strategy and then click Subscribe to create a subscription.

3.2. DEPLOYING A RED HAT DECISION MANAGER ENVIRONMENT USING THE OPERATOR

After you subscribe to the Business Automation operator, you can use the installer wizard to configure and deploy a Red Hat Decision Manager environment.

IMPORTANT

In Red Hat Decision Manager 7.7, the operator installer wizard is for Technology Preview only. For more information on Red Hat Technology Preview features, see Technology Preview Features Support Scope.

3.2.1. Starting the deployment of a Red Hat Decision Manager environment using the Business Automation operator

To start deploying a Red Hat Decision Manager environment using the Business Automation operator, access the installer wizard. The installer wizard is deployed when you subscribe to the Operator.

Prerequisites

- You subscribed to the Business Automation operator. For instructions about subscribing to the Operator, see Section 3.1, “Subscribing to the Business Automation operator”.

Procedure

1. In the Red Hat OpenShift Container Platform web cluster console menu, select Catalog → Installed operators or Operators → Installed operators.

2. Click the name of the operator that contains businessautomation. Information about this operator is displayed.

3. Click the Installer link, located on the left side of the window in Red Hat OpenShift Container Platform version 4.1 or on the right side of the window in Red Hat OpenShift Container Platform version 4.2 or later.

4. If prompted, log in with your OpenShift credentials.

Result

The Installation tab of the wizard is displayed.

3.2.2. Setting the basic configuration of the environment

After you start to deploy a Red Hat Decision Manager environment using the Business Automation operator, you must select the type of the environment and set other basic configuration.

Prerequisites

- You started to deploy a Red Hat Decision Manager environment using the Business Automation operator and accessed the installer wizard according to the instructions in Section 3.2.1, “Starting the deployment of a Red Hat Decision Manager environment using the Business Automation operator”.

Procedure

1. In the Application Name field, enter a name for the OpenShift application. This name is used in the default URLs for all components.

2. In the Environment list, select the type of environment. This type determines the default configuration; you can modify this configuration as necessary. The following types are available for Red Hat Decision Manager:

   - **rhdm-trial**: A trial environment that you can set up quickly and use to evaluate or demonstrate developing and running assets. Includes Business Central and a KIE Server. This environment does not use any persistent storage, and any work you do in the environment is not saved.

   - **rhdm-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 KIE Server for test execution of the services. You can also use this environment to run services for staging and production purposes. You can add KIE Servers to the environment and they are managed by the same Business Central.

   - **rhdm-authoring-ha**: An environment for creating and modifying services using Business Central. It consists of pods that provide Business Central for the authoring work and a KIE Server for test execution of the services. This version of the authoring environment supports scaling the Business Central pod to ensure high availability.
In Red Hat Decision Manager 7.7, high-availability Business Central functionality is for Technology Preview only. For more information about Red Hat Technology Preview features, see Technology Preview Features Support Scope.

- **rhdm-production-immutable**: An alternate environment for running existing services for staging and production purposes. You can configure one or more KIE Server replicated pods that build a service from source. In this environment, when you deploy a KIE 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 KIE 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.

3. If you want to enable automatic upgrades to new versions, select the **Enable Upgrades** box. If this box is selected, when a new patch version of Red Hat Decision Manager 7.7 becomes available, the Operator automatically upgrades your deployment to this version. All services are preserved and normally remain available throughout the upgrade process. If you also want to enable the same automatic upgrade process when a new minor version of Red Hat Decision Manager 7.x becomes available, select the **Include minor version upgrades** box.

4. If you want to use a custom image registry, under **Custom registry**, enter the URL of the registry in the **Image registry** field. If this registry does not have a properly signed and recognized SSL certificate, select the **Insecure** box.

5. Under **Admin user**, enter the user name and password for the administrative user for Red Hat Decision Manager in the **Username** and **Password** fields.

- **IMPORTANT**

If you use RH-SSO or LDAP authentication, the same user must be configured in your authentication system with the **kie-server,rest-all,admin** roles for Red Hat Decision Manager.

6. If you want to use a custom version tag for images, complete the following steps:
   a. Click **Next** to access the **Security** tab.
   b. Scroll to the bottom of the window.
   c. Enter the image tag in the **Image tag** field.

**Next steps**

If you want to deploy the environment with the default configuration, click **Finish** and then click **Deploy** to deploy the environment. Otherwise, continue to set other configuration parameters.

### 3.2.3. Setting the security configuration of the environment

After you set the basic configuration of a Red Hat Decision Manager environment using the Business Automation operator, you can optionally configure authentication (security) settings for the environment.
Prerequisites

- You completed basic configuration of a Red Hat Decision Manager environment using the Business Automation operator in the installer wizard according to the instructions in Section 3.2.2, “Setting the basic configuration of the environment”.

- If you want to use RH-SSO or LDAP for authentication, you created users with the correct roles in your authentication system. You must create at least one administrative user (for example, adminUser) with the kie-server,rest-all,admin roles. This user must have the user name and password that you configured on the Installation tab.

- If you want to use RH-SSO authentication, you created the clients in your RH-SSO system for all components of your environment, specifying the correct URLs. This action ensures maximum control. Alternatively, the deployment can create the clients.

Procedure

1. If the Installation tab is open, click Next to view the Security tab.

2. In the Authentication mode list, select one of the following modes:
   - Internal: You configure the initial administration user when deploying the environment. The user can use Business Central to set up other users as necessary.
   - LDAP: Red Hat Decision Manager uses LDAP for authentication

3. Complete the security configuration based on the Authentication mode that you selected.
   If you selected RH-SSO, configure RH-SSO authentication:
   a. In the RH-SSO URL field, enter the RH-SSO URL.
   b. In the Realm field, enter the RH-SSO realm name.
   c. If you did not create RH-SSO clients for components of your environment enter the credentials of an administrative user for your RH-SSO system in the SSO admin user and SSO admin password fields.
   d. If your RH-SSO system does not have a proper signed SSL certificate, select the Disable SSL cert validation box.
   e. If you want to change the RH-SSO principal attribute used for the user name, in the Principal attribute field enter the name of the new attribute.

   If you selected LDAP, configure LDAP authentication:
   a. In the LDAP URL field, enter the LDAP URL.
   b. Configure LDAP parameters that correspond to the settings of the LdapExtended Login module of Red Hat JBoss EAP. For instructions about using these settings, see LdapExtended Login Module.

4. If you selected RH-SSO or LDAP, if your RH-SSO or LDAP system does not define all the roles required for your deployment, you can map authentication system roles to Red Hat Decision Manager roles.
To enable role mapping, you must provide a role mapping configuration file in an OpenShift configuration map or secret object in the project namespace. The file must contain entries in the following format:

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

For example:

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

To enable the use of this file, make the following changes:

a. Under RoleMapper, in the Roles properties file field, enter the fully qualified path name of the role mapping configuration file, for example, `/opt/eap/standalone/configuration/rolemapping/rolemapping.properties`.

b. If you want to replace roles defined in the authentication system with roles that you define in the mapping file, select the Replace roles box. Otherwise, both the roles defined in RHSSO or LDAP and the roles defined in the configuration file are available.

c. In the fields under RoleMapper Configuration object, select the Kind of the object that provides the file (ConfigMap or Secret) and enter the Name of the object. This object is automatically mounted on Business Central and KIE Server pods in the path that you specified for the role mapping configuration file.

5. Configure other passwords, if necessary:

   - **AMQ password** and **AMQ cluster password** are passwords for interaction with ActiveMQ using the JMS API.
   
   - **Keystore password** is the password for the keystore files used in secrets for HTTPS communication. Set this password if you created secrets according to instructions in Section 2.2, “Creating the secrets for KIE Server” or Section 2.3, “Creating the secrets for Business Central”.
   
   - **Database password** is the password for database server pods that are a part of the environments.

Next steps

If you want to deploy the environment with the default configuration of all components, click Finish and then click Deploy to deploy the environment. Otherwise, continue to set configuration parameters for Business Central and KIE Servers.

### 3.2.4. Setting the Business Central configuration of the environment

After you set the basic and security configuration of a Red Hat Decision Manager environment using the Business Automation operator, you can optionally configure settings for the Business Central or Business Central Monitoring component of the environment.

Do not change these settings for an immutable server environment, as this environment does not include Business Central or Business Central Monitoring.

**Prerequisites**
You completed basic configuration of a Red Hat Decision Manager environment using the Business Automation operator in the installer wizard according to the instructions in Section 3.2.2, “Setting the basic configuration of the environment”.

If you want to use RH-SSO or LDAP for authentication, you completed security configuration according to the instructions in Section 3.2.3, “Setting the security configuration of the environment”.

Procedure

1. If the Installation or Security tab is open, click Next until you view the Console tab.

2. If you created the secret for Business Central according to the instructions in Section 2.3, “Creating the secrets for Business Central”, enter the name of the secret in the Secret field.

3. In an authoring environment, you can use Git hooks to facilitate interaction between the internal Git repository of Business Central and an external Git repository. If you want to use Git hooks, you must prepare a Git hooks directory in an OpenShift configuration map, secret, or persistent volume claim object in the project namespace. To use this directory, make the following changes:
   a. Under GitHooks, in the Mount path field, enter a fully qualified path for the directory, for example, /opt/kie/data/git/hooks.
   b. In the fields under GitHooks Configuration object, select the Kind of the object that provides the file (ConfigMap, Secret, or PersistentVolumeClaim) and enter the Name of the object. This object is automatically mounted on the Business Central pods in the path that you specified for the Git hooks directory.

4. Optionally, enter the number of replicas for Business Central or Business Central monitoring in the Replicas field. Do not change this number in a rhdm-authoring environment.

5. Optionally, enter requested and maximum CPU and memory limits in the fields under Resource quotas.

6. If you want to customize the configuration of the Java virtual machine on the Business Central pods, select the Enable JVM configuration box and then enter information in any of the fields under Enable JVM configuration. All fields are optional. For the JVM parameters that you can configure, see Section 3.4, “JVM configuration parameters”.

7. If you selected RH-SSO authentication, configure RH-SSO for Business Central:
   a. Enter the client name in the Client name field and the client secret in the Client secret field. If a client with this name does not exist, the deployment attempts to create a new client with this name and secret.

   b. If the deployment is to create a new client, enter the HTTP and HTTPS URLs that will be used for accessing the KIE Server into the SSO HTTP URL and SSO HTTPS URL fields. This information is recorded in the client.

8. Optionally, depending on your needs, set environment variables. To set an environment variable, click Add new Environment variable, then enter the name and value for the variable in the Name and Value fields.
   - If you want to use an external Maven repository, set the following variables:
     - MAVEN_REPO_URL: The URL for the Maven repository
MAVEN_REPO_ID: An identifier for the Maven repository, for example, repo-custom
MAVEN_REPO_USERNAME: The user name for the Maven repository
MAVEN_REPO_PASSWORD: The password for the Maven repository

IMPORTANT
In an authoring environment, if you want Business Central to push a project into an external Maven repository, you must configure this repository during deployment and also configure exporting to the repository in every project. For information about exporting Business Central projects to an external Maven repository, see Packaging and deploying a Red Hat Decision Manager project.

If your OpenShift environment does not have a connection to the public Internet, configure access to a Maven mirror that you set up according to Section 2.7, “Preparing a Maven mirror repository for offline use”. Set the following variables:

MAVEN_MIRROR_URL: The URL for the Maven mirror repository that you set up in Section 2.7, “Preparing a Maven mirror repository for offline use”. This URL must be accessible from a pod in your OpenShift environment.

MAVEN_MIRROR_OF: 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 your authoring environment uses a built-in Business Central Maven repository, change MAVEN_MIRROR_OF to exclude the artifacts in this repository from the mirror: external:*,!repo-rhdmcentr.

In some authoring environments, you might need to ensure that several users can deploy services on the same KIE Server at the same time. By default, after deploying a service onto a KIE Server using Business Central, the user needs to wait for some seconds before more services can be deployed. To remove this limitation, you can configure the environment to use the controller strategy. Do not make this change unless a specific need for it exists; if you decide to enable controller strategy, make this change on Business Central and on all KIE Servers in the same environment.

To enable controller strategy on Business Central, set the KIE_SERVER_CONTROLLER_OPENSHIFT_ENABLED environment variable to false.

Next steps
If you want to deploy the environment with the default configuration of KIE Servers, click Finish and then click Deploy to deploy the environment. Otherwise, continue to set configuration parameters for KIE Servers.

3.2.5. Setting custom KIE Server configuration of the environment
Every environment type in the Business Automation operator includes one or several KIE Servers by default.

Optionally, you can set custom configuration for KIE Servers. In this case, default KIE Servers are not created and only the KIE Servers that you configure are deployed.

Prerequisites

- You completed basic configuration of a Red Hat Decision Manager environment using the Business Automation operator in the installer wizard according to the instructions in Section 3.2.2, “Setting the basic configuration of the environment”.

- If you want to use RH-SSO or LDAP for authentication, you completed security configuration according to the instructions in Section 3.2.3, “Setting the security configuration of the environment”.

Procedure

1. If the Installation, Security, or Console tab is open, click Next until you view the KIE Servers tab.

2. Click Add new KIE Server to add a new KIE Server configuration.

3. In the Id field, enter an identifier for the KIE Server. If the KIE Server connects to a Business Central or Business Central Monitoring instance, this identifier determines which server group the server joins.

4. In the Name field, enter a name for the KIE Server.

5. In the Deployments field, enter the number of similar KIE Servers that are to be deployed. The installer can deploy several KIE Servers with the same configuration. The identifiers and names of the KIE Servers are modified automatically and remain unique.

6. If you created the secret for KIE Server according to the instructions in Section 2.2, “Creating the secrets for KIE Server”, enter the name of the secret in the Keystore secret field.

7. Optionally, enter the number of replicas for the KIE Server in the Replicas field.

8. If you want to use a custom image for the KIE Server, complete the following additional steps:
   a. Click Set KIE Server image
   b. If you want to use a Docker image name and not an OpenShift image stream tag, change the Kind value to DockerImage.
   c. Enter the name of the image stream in the Name field.
   d. If the image stream is not in the openshift namespace, enter the namespace in the Namespace field.

9. If you want to configure an immutable KIE Server, complete the following additional steps:
   a. Click Set Immutable server configuration
   b. In the KIE Server container deployment field, enter the identifying information of the decision services (KJAR files) that the deployment must pull from the Maven repository. The format is <containerId>=<groupId>:<artifactId>:<version> or, if you want to specify
an alias name for the container, `<containerId>(<aliasId>)=<groupId>:<artifactId>:<version>`.
You can provide two or more KJAR files using the `|` separator, as illustrated in the following example:
`containerId=groupId:artifactId:version|c2(alias2)=g2:a2:v2`

c. If your OpenShift environment does not have a connection to the public Internet, enter the
URL of the Maven mirror that you set up according to Section 2.7, "Preparing a Maven
mirror repository for offline use" in the Maven mirror URL field.

d. In the Artifact directory field, enter 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.

e. If you want to use a custom base KIE Server image for the S2I build, click Set Base build
image and then enter the name of the image stream in the Name field. If the image stream
is not in the openshift namespace, enter the namespace in the Namespace field. If you
want to use a Docker image name and not an OpenShift image stream tag, change the Kind
value to DockerImage.

f. If you want to create the immutable server from source in a Git repository using the Source
to Image (S2I) process, click the Set Git source button and enter information in the
following fields:
   - **S2I Git URI**: The URI for the Git repository that contains the source for your services.
   - **Reference**: The branch in the Git repository.
   - **Context directory**: (Optional) The path to the source within the project downloaded
     from the Git repository. By default, the root directory of the downloaded project is the
     source directory.

g. If you are using S2I and want to set a Git Webhook so that changes in the Git repository
cause an automatic rebuild of the KIE Server, click Add new Webhook. Then select the type
of the Webhook in the Type field and enter the secret string for the Webhook in the Secret
field.

10. Optionally, enter requested and maximum CPU and memory limits in the fields under Resource
quotas. If you are configuring several KIE Servers, the limits apply to each server separately.

11. If you selected RH-SSO authentication, configure RH-SSO for the KIE Server:
   a. Enter the client name in the Client name field and the client secret in the Client secret
field. If a client with this name does not exist, the deployment attempts to create a new
client with this name and secret.
   b. If the deployment is to create a new client, enter the HTTP and HTTPS URLs that will be
used for accessing the KIE Server into the SSO HTTP URL and SSO HTTPS URL fields.
This information is recorded in the client.

12. If you want to interact with the KIE Server through JMS API using an external AMQ message
broker, enable the Enable JMS Integration setting. Additional fields for configuring JMS
Integration are displayed and you must enter the values as necessary:
   - **User name, Password**: The user name and password of a standard broker user, if user
authentication in the broker is required in your environment.
   - **Executor**: Select this setting to disable the JMS executor. The executor is enabled by
default.
Executor transacted: Select this setting to enable JMS transactions on the executor queue.

Enable signal: Select this setting to enable signal configuration through JMS.

Enable audit: Select this setting to enable audit logging through JMS.

Audit transacted: Select this setting to enable JMS transactions on the audit queue.

Queue executor, Queue request, Queue response, Queue signal, Queue audit: Custom JNDI names of the queues to use. If you set any of these values, you must also set the AMQ queues parameter.

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 are using any custom queue names, you must enter the names of all the queues uses by the server in this field.

Enable SSL integration: Select this setting if you want to use an SSL connection to the AMQ broker. In this case you must also provide the name of the secret that you created in Section 2.4, “Creating the secrets for the AMQ broker connection” and the names and passwords of the key store and trust store that you used for the secret.

If you want to customize the configuration of the Java virtual machine on the KIE Server pods, select the Enable JVM configuration box and then enter information in any of the fields under Enable JVM configuration. All fields are optional. For the JVM parameters that you can configure, see Section 3.4, “JVM configuration parameters”.

Optionally, depending on your needs, set environment variables. To set an environment variable, click Add new Environment variable, then enter the name and value for the variable in the Name and Value fields.

If you want to configure your KIE Server deployment to use Prometheus to collect and store metrics, set the PROMETHEUS_SERVER_EXT_DISABLED environment variable to false. For instructions about configuring Prometheus metrics collection, see Managing and monitoring KIE Server.

If you want to use an external Maven repository, set the following variables:

- MAVEN_REPO_URL: The URL for the Maven repository
- MAVEN_REPO_ID: An identifier for the Maven repository, for example, repo-custom
- MAVEN_REPO_USERNAME: The user name for the Maven repository
- MAVEN_REPO_PASSWORD: The password for the Maven repository

If your OpenShift environment does not have a connection to the public Internet, configure access to a Maven mirror that you set up according to Section 2.7, “Preparing a Maven mirror repository for offline use”. Set the following variables:

- MAVEN_MIRROR_URL: The URL for the Maven mirror repository that you set up in Section 2.7, “Preparing a Maven mirror repository for offline use”. This URL must be accessible from a pod in your OpenShift environment. If you configured this KIE Server as S2I, you already entered this URL.
- MAVEN_MIRROR_OF: The value that determines which artifacts are to be retrieved from the mirror. If you configured this KIE Server as S2I, do not set this value. For
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 your authoring environment uses a built-in Business Central Maven repository, change MAVEN_MIRROR_OF to exclude the artifacts in this repository from the mirror: external:*,!repo-rhdmcentr.

- In some authoring environments, you might need to ensure that several users can deploy services on the same KIE Server at the same time. By default, after deploying a service onto a KIE Server using Business Central, the user needs to wait for some seconds before more services can be deployed. To remove this limitation, you can configure the environment to use the controller strategy. Do not make this change unless a specific need for it exists; if you decide to enable controller strategy, make this change on Business Central and on all KIE Servers in the same environment.
  To enable controller strategy on a KIE Server, set the KIE_SERVER_STARTUP_STRATEGY environment variable to ControllerBasedStartupStrategy.

Next steps
To configure additional KIE Servers, click Add new KIE Server again and repeat the procedure for the new server configuration.

Click Finish and then click Deploy to deploy the environment.

3.3. MODIFYING AN ENVIRONMENT THAT IS DEPLOYED USING OPERATORS

If an environment is deployed using operators, you cannot modify it using typical OpenShift methods. For example, if you delete a deployment configuration or a service, it is re-created automatically with the same parameters.

To modify the environment, you must modify the YAML description of the environment. You can change common settings such as passwords, add new KIE Servers, and scale KIE Servers.

Procedure

1. Enter your project in the OpenShift web cluster console.

2. In the OpenShift Web console navigation panel, select Catalog → Installed operators or Operators → Installed operators.

3. Find the Business Automation operator line in the table and click KieApp in the line. Information about the environments that you deployed using this operator is displayed.

4. Click the name of a deployed environment.

5. Select the YAML tab. A YAML source is displayed.

6. If you want to change common settings, such as passwords, edit the values under commonConfig:
7. If you want to add new KIE Servers, add their descriptions at the end of the block under **servers:** as shown in the following examples:

- To add two servers named **server-a** and **server-a-2**, add the following lines:
  
  ```yaml
  - deployments: 2
    name: server-a
  ```

- To add an immutable KIE Server that includes services built from source in an S2I process, add the following lines:

  ```yaml
  - build:
    kieServerContainerDeployment: <deployment>
    gitSource:
      url: <url>
      reference: <branch>
      contextDir: <directory>
  ```

Replace the following values:

- `<deployment>`: The identifying information of the decision service (KJAR file) that is built from your source. The format is `<containerId>=<groupId>:<artifactId>:<version>`. You can provide two or more KJAR files using the | separator, for example `containerId=groupId:artifactId:version|c2=g2:a2:v2`. The Maven build process must produce all these files from the source in the Git repository.

- `<url>`: The URL for the Git repository that contains the source for your decision service.

- `<branch>`: The branch in the Git repository.

- `<directory>`: The path to the source within the project downloaded from the Git repository.

8. If you want to scale a KIE Server, find the description of the server in the block under **servers:** and add a **replicas:** setting under that description. For example, **replicas: 3** scales the server to three pods.

9. Click **Save** and then wait for a **has been updated** pop-up message.

10. Click **Reload** to view the new YAML description of the environment.

### 3.4. JVM CONFIGURATION PARAMETERS

When deploying Red Hat Decision Manager using the operator, you can optionally set a number of JVM configuration parameters for Business Central and KIE Servers. These parameters set environment variables for the corresponding containers.

The following table lists all JVM configuration parameters that you can set when deploying Red Hat Decision Manager using the operator.

The default settings are optimal for most use cases. Make any changes only when they are required.

**Table 3.1. JVM configuration parameters**
<table>
<thead>
<tr>
<th>Configuration field</th>
<th>Environment variable</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Opts append</td>
<td>JAVA_OPTS_APPEND</td>
<td>User specified Java options to be appended to generated options in JAVA_OPTS.</td>
<td>-Dsome.property=foo</td>
</tr>
<tr>
<td>Java max memory ratio</td>
<td>JAVA_MAX_MEM_RATIO</td>
<td>The maximum percentage of container memory that can be used for the Java Virtual Machine. The remaining memory is used for the operating system. The default value is 50, for a limit of 50%. Sets the -Xmx JVM option. If you enter a value of 0, the -Xmx option is not set.</td>
<td>40</td>
</tr>
<tr>
<td>Java initial memory ratio</td>
<td>JAVA_INITIAL_MEM_RATIO</td>
<td>The percentage of container memory that is initially used for the Java Virtual Machine. The default value is 25, so 25% of the pod memory is initially allocated for the JVM if this value does not exceed the Java Max Initial Memory value. Sets the -Xms JVM option. If you enter a value of 0, the -Xms option is not set.</td>
<td>25</td>
</tr>
<tr>
<td>Java max initial memory</td>
<td>JAVA_MAX_INITIAL_MEM</td>
<td>The maximum amount of memory, in megabytes, that can be initially used for the Java Virtual Machine. If the initial allocated memory, as set in the Java initial memory ratio parameter, would otherwise be greater than this value, the amount of memory set in this value is allocated using the -Xms JVM option. The default value is 4096.</td>
<td>4096</td>
</tr>
<tr>
<td>Java diagnostics</td>
<td>JAVA_DIAGNOSTICS</td>
<td>Enable this setting to enable output of additional JVM diagnostic information to the standard output. Disabled by default.</td>
<td>true</td>
</tr>
<tr>
<td>Java debug</td>
<td>JAVA_DEBUG</td>
<td>Enable this setting to switch on remote debugging. Disabled by default. Adds the -agentlib:jdwp=transport=dt_socket,server=y,suspend=n,address= parameter, where ${debug_port} defaults to 5005.</td>
<td>true</td>
</tr>
<tr>
<td>Java debug port</td>
<td>JAVA_DEBUG_PORT</td>
<td>The port that is used for remote debugging. The default value is 5005.</td>
<td>8787</td>
</tr>
<tr>
<td>GC min heap free ratio</td>
<td>GC_MIN_HEAP_FREE_RATIO</td>
<td>Minimum percentage of heap free after garbage collection (GC) to avoid expansion. Sets the -XX:MinHeapFreeRatio JVM option.</td>
<td>20</td>
</tr>
<tr>
<td>Configuration field</td>
<td>Environment variable</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>GC max heap free ratio</td>
<td>GC_MAX_HEAP_FREE_RATIO</td>
<td>Maximum percentage of heap free after GC to avoid shrinking. Sets the -XX:MaxHeapFreeRatio JVM option.</td>
<td>40</td>
</tr>
<tr>
<td>GC time ratio</td>
<td>GC_TIME_RATIO</td>
<td>Specifies the ratio of the time spent outside the garbage collection (for example, the time spent for application execution) to the time spent in the garbage collection. Sets the -XX:GCTimeRatio JVM option.</td>
<td>4</td>
</tr>
<tr>
<td>GC adaptive size policy weight</td>
<td>GC_ADAPTIVE_SIZE_POLICY_WEIGHT</td>
<td>The weighting given to the current GC time versus previous GC times. Sets the -XX:AdaptiveSizePolicyWeight JVM option.</td>
<td>90</td>
</tr>
<tr>
<td>GC max metaspace size</td>
<td>GC_MAX_METASPACE_SIZE</td>
<td>The maximum metaspace size. Sets the -XX:MaxMetaspaceSize JVM option.</td>
<td>100</td>
</tr>
</tbody>
</table>
APPENDIX A. VERSIONING INFORMATION

Documentation last updated on Wednesday, March 18, 2020.