Red Hat Application Migration Toolkit 4.3

Web Console Guide

Use the Red Hat Application Migration Toolkit's web console to group your applications into projects for analysis.

Last Updated: 2020-03-19

Red Hat Application Migration Toolkit 4.3 Web Console Guide

Use the Red Hat Application Migration Toolkit's web console to group your applications into projects for analysis.

Legal Notice

Copyright © 2020 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Abstract

This guide describes how to use the Red Hat Application Migration Toolkit web console to simplify migration of Java applications.

Table of Contents

CHAPTER 1. INTRODUCTION 3
1.1. ABOUT THE WEB CONSOLE GUIDE 3
1.2. ABOUT RED HAT APPLICATION MIGRATION TOOLKIT 3
What is Red Hat Application Migration Toolkit? 3
How Does Red Hat Application Migration Toolkit Simplify Migration? 3
How Do I Learn More? 3
1.3. ABOUT THE WEB CONSOLE 3

CHAPTER 2. INSTALLING THE WEB CONSOLE 4
2.1. ZIP INSTALLATION 4
2.1.1. Prerequisites 4
2.1.2. Install the Web Console 4
2.1.3. Start the Web Console 4
2.1.4. Access the Web Console 4
2.2. OPENSHIFT INSTALLATION 5
2.2.1. Prerequisites 5
2.2.2. Understanding the Web Console OpenShift Image 5
OpenShift Template Environment Variables 7
2.2.3. Deploy the RHAMT Application 7
2.2.4. Access the Web Console 9
2.2.5. Troubleshoot the Web Console OpenShift Install 10
2.2.5.1. Ensure Latest Image Version 10
2.2.5.2. Examine and Collect the Web Console Logs 11
2.2.5.2.1. Using the OpenShift Console 11
2.2.5.2.2. Using the OpenShift Client 11
2.2.5.3. Common Issues with Web Console OpenShift 11
2.2.5.3.1. Executor Pod Throws NoRouteToHostException 12
2.2.5.3.2. Pod Reports Insufficient Resources 12
2.2.5.3.3. Pod Takes Longer than 600 seconds to become available 12
2.2.5.4. Report Issues with Web Console OpenShift 13

CHAPTER 3. USING THE WEB CONSOLE TO ANALYZE APPLICATIONS 15
3.1. ADD A PROJECT 15
3.2. ADD APPLICATIONS TO A PROJECT 16
3.3. SPECIFY THE ANALYSIS CONFIGURATION 17
3.4. EXECUTE THE ANALYSIS 20
3.5. VIEW THE RESULTS OF AN ANALYSIS 20
3.5.1. Examine Analysis Details 21
3.5.2. Review the Reports 22

CHAPTER 4. USING CUSTOM RULES AND LABELS 23
4.1. ADDING CUSTOM RULES 23
4.2. ADDING CUSTOM LABELS 23

CHAPTER 5. CONFIGURING AUTHENTICATION FOR THE WEB CONSOLE 25
5.1. ENABLE AUTHENTICATION FOR WEB CONSOLE 25
5.2. CHANGE THE ADMINISTRATIVE USER'S CREDENTIALS 25
5.3. REMOVE THE DEFAULT WEB CONSOLE USER 26
5.4. ADD A NEW WEB CONSOLE USER 27

CHAPTER 1. INTRODUCTION

1.1. ABOUT THE WEB CONSOLE GUIDE

This guide is for engineers, consultants, and others who want to use Red Hat Application Migration Toolkit (RHAMT) to migrate Java applications or other components. It describes how to install and use the web console to manage migration projects and analyze applications.

1.2. ABOUT RED HAT APPLICATION MIGRATION TOOLKIT

What is Red Hat Application Migration Toolkit?

Red Hat Application Migration Toolkit (RHAMT) is an extensible and customizable rule-based tool that helps simplify migration of Java applications.

RHAMT examines application artifacts, including project source directories and application archives, then produces an HTML report that highlights areas needing changes. RHAMT can be used to migrate Java applications from previous versions of *Red Hat JBoss Enterprise Application Platform* or from other containers, such as *Oracle® WebLogic Server* or *IBM® WebSphere® Application Server*.

How Does Red Hat Application Migration Toolkit Simplify Migration?

Red Hat Application Migration Toolkit looks for common resources and highlights technologies and known trouble spots when migrating applications. The goal is to provide a high-level view into the technologies used by the application and provide a detailed report organizations can use to estimate, document, and migrate enterprise applications to Java EE and Red Hat JBoss Enterprise Application Platform.

How Do I Learn More?

See the *Getting Started Guide* to learn more about the features, supported configurations, system requirements, and available tools in the Red Hat Application Migration Toolkit.

1.3. ABOUT THE WEB CONSOLE

The web console for Red Hat Application Migration Toolkit is a web-based system that allows a team of users to assess and prioritize migration and modernization efforts for a large number of applications. It allows you to group applications into projects for analysis and provides numerous reports that highlight the results.

CHAPTER 2. INSTALLING THE WEB CONSOLE

The web console can be installed either using the ZIP distribution or on OpenShift.

2.1. ZIP INSTALLATION

When installed using the ZIP distribution, the RHAMT web console is deployed on Red Hat JBoss Enterprise Application Platform, uses Red Hat Single Sign-On for authentication, and is backed by an H2 database for storage.

2.1.1. Prerequisites

Verify that you meet the following prerequisites.

- OpenJDK 1.8, OpenJDK 11, Oracle JDK 1.8, Oracle JDK 11
- A minimum of 8 GB RAM; 16 GB recommended

NOTE

If you are running macOS, it is recommended to set the maximum number of user processes, **maxproc**, to at least **2048**, and the maximum number of open files, **maxfiles**, to **100000**.

2.1.2. Install the Web Console

1. Download the web console from the RHAMT Download page.
2. Extract the ZIP file to a directory of your choice.
   The path to the directory created by unzipping this file is referred to as ***RHAMT_HOME*** throughout this guide.

2.1.3. Start the Web Console

Run the script to start the web console.

```
$ RHAMT_HOME/run_rhamt.sh
```

NOTE

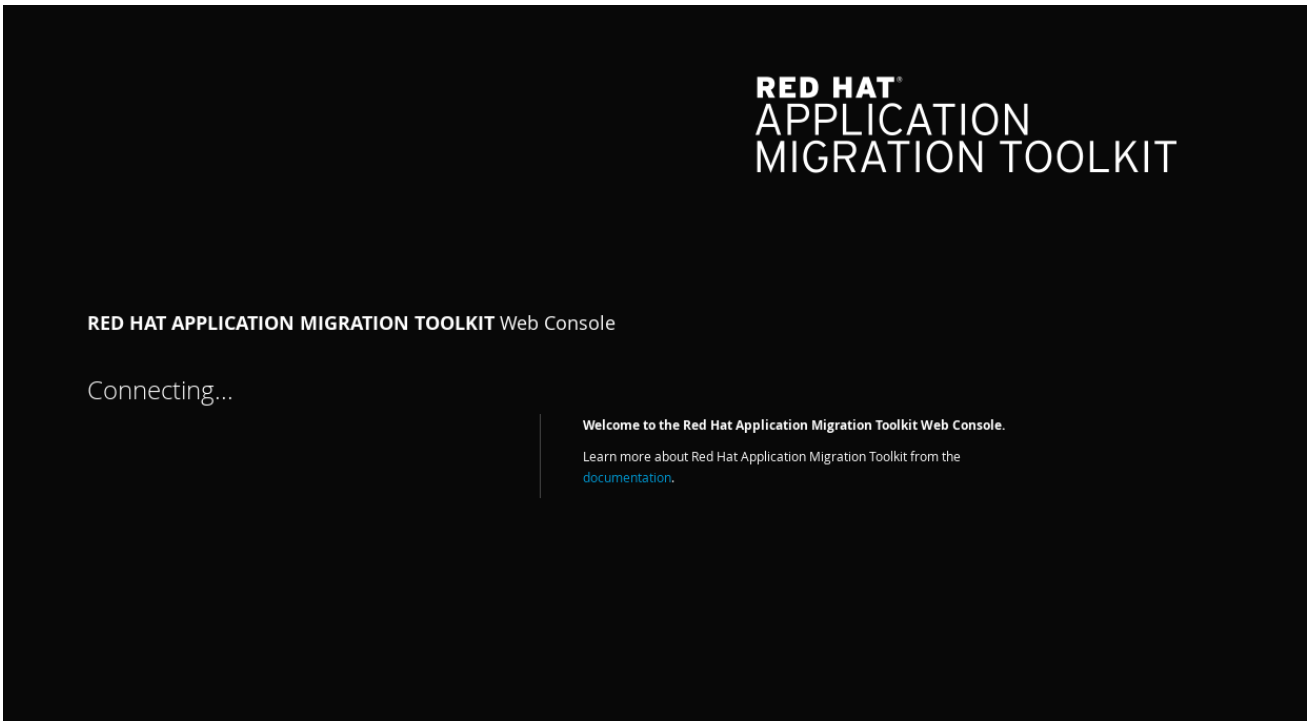
In a Windows environment, use the **run_rhamt.bat** script.

You can now access the web console from a browser.

2.1.4. Access the Web Console

Once started, the web console is accessible from a browser by default on the local host at http://localhost:8080/rhamt-web.

Figure 2.1. Welcome Page



The web console uses a default user to automatically authenticate. The default user's credentials are **rhamt** and **password**. See Configuring Authentication for the Web Console to require individual users to authenticate in order to access the web console.

2.2. OPENSHIFT INSTALLATION

When installed on OpenShift, the RHAMT web console is deployed on Red Hat JBoss Enterprise Application Platform, uses Red Hat Single Sign-On for authentication, and is backed by a PostgreSQL database for storage.

2.2.1. Prerequisites

Verify that you meet the following prerequisites.

- You must have access to an instance of OpenShift Container Platform with version 3.5 or later, up to, and including 3.11.
- Your OpenShift instance must have the middleware image streams installed.
- You must have the OpenShift Container Platform CLI installed on your local machine.
- You must be running Linux or macOS on your local machine. Windows is not currently supported.

See the OpenShift Container Platform documentation for assistance.

2.2.2. Understanding the Web Console OpenShift Image

Red Hat offers containerized images for RHAMT that are designed for use with OpenShift. Using these images developers can quickly and easily manage migration projects and analyze applications.

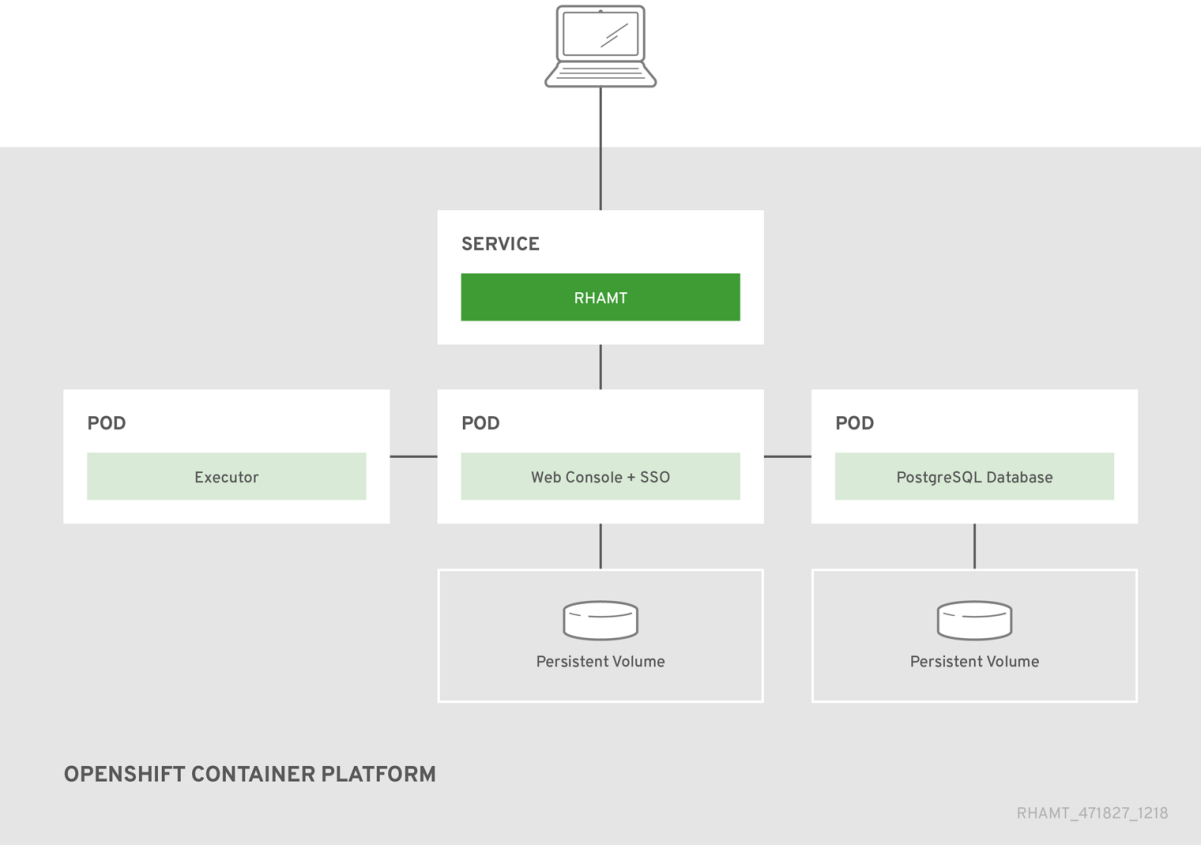
The OpenShift images include three separate pods:

- The executor, responsible for running the analysis and generating the reports
- The web console interface and SSO, which provide access to the web console itself
- The PostgreSQL database, which stores the project's configuraton and analysis tracking information

A separate persistent volume is used for the web console interface and the PostgreSQL pods; however, the executor's storage is dependent on the template used.

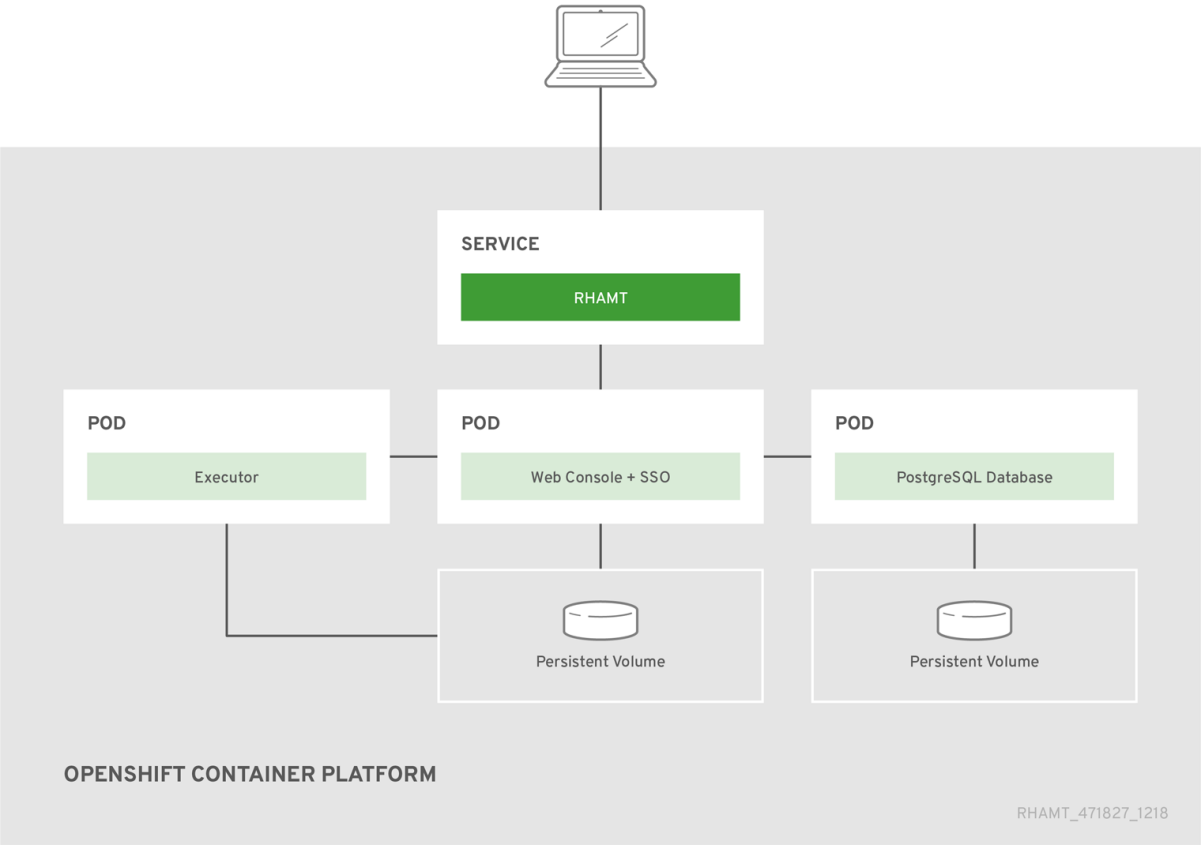
- The **web-template-empty-dir-executor.json** is the recommended template. It configures the executor pod to use temporary storage on a single machine, and has no defined persistent volume. The analysis data is sent between the executor and web console pods using a RESTful web service.

  Figure 2.2. web-template-empty-dir-executor.json



- The **web-template-empty-dir-executor-shared-storage.json** is an alternative template available for use. This template configures the executor pod and the web console pod to use a shared persistent volume. All instances of these pods read and write to the same persistent volume, mounted as **ReadWriteMany** in OpenShift.

Figure 2.3. **web-template-empty-dir-executor-shared-storage.json**



OpenShift Template Environment Variables
The OpenShift image environment variables are configured as a baseline for application analysis, and work well in a variety of environments. No additional configuration is required to perform an analysis.

The most common environment variables modified are the CPU and memory resources allocated to each image. These contain a pattern of ***NODE_NAME*** followed by **REQUESTED_*RESOURCE***. For instance, **EXECUTOR_REQUESTED_CPU** indicates the number of CPU cores to request for the executor pod, while **EXECUTOR_REQUESTED_MEMORY** indicates the amount of memory to request for the executor pod.

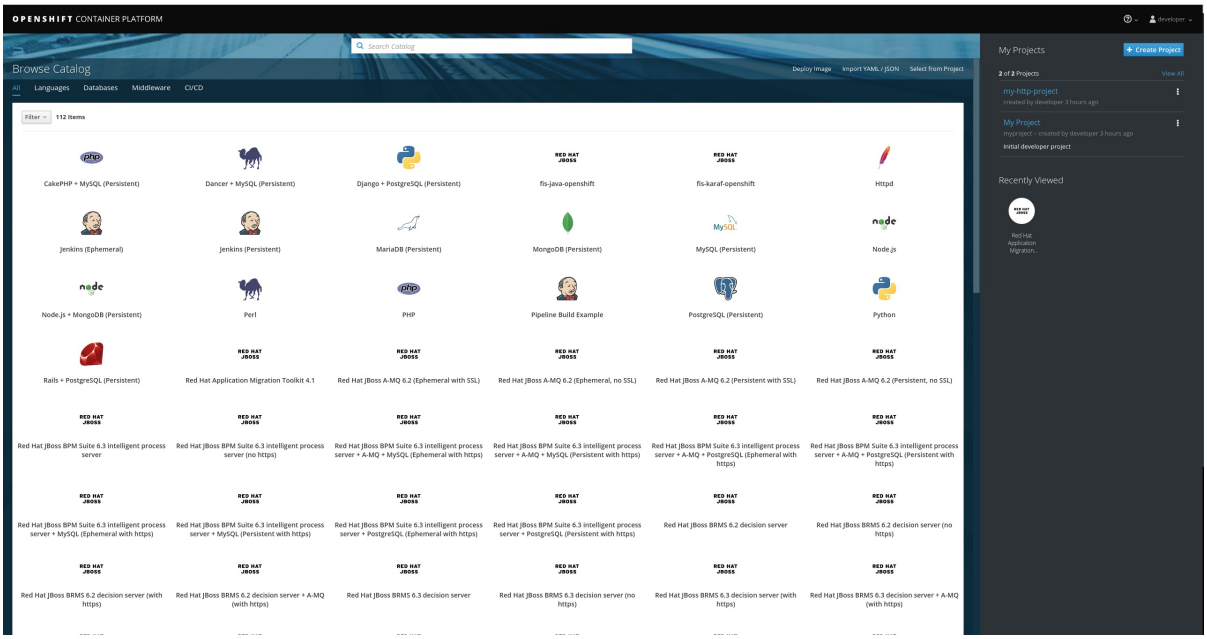
All of the environment variables are found within each template, along with a description of each.

2.2.3. Deploy the RHAMT Application

1. Download the web console from the RHAMT Download page.

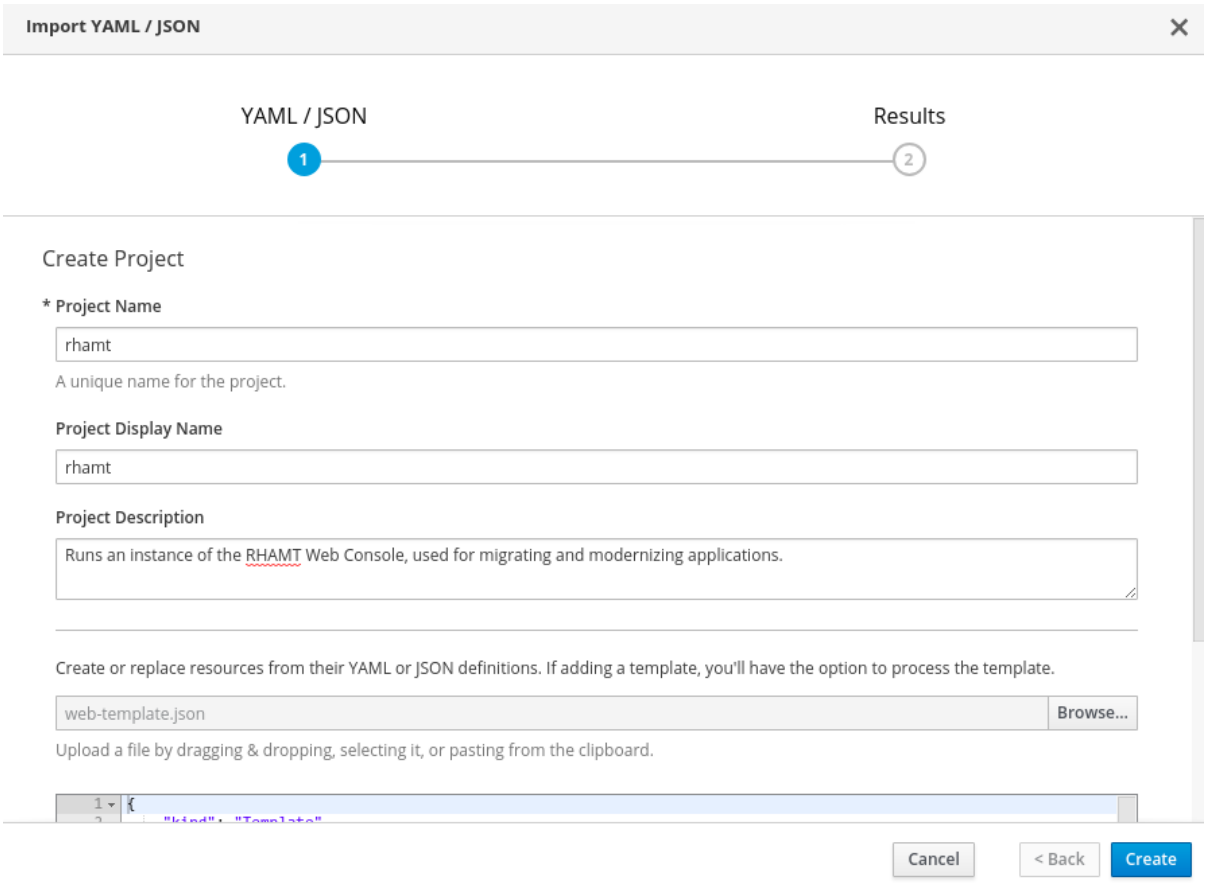
2. Extract the ZIP file to a directory of your choice.
   The path to the directory created by unzipping this file is referred to as ***RHAMT_HOME*** throughout this guide.

3. Access the OpenShift web console. It should appear similar to the following image.



4. Click the **Import YAML / JSON** button in the top-right corner of the web console.

5. Provide the following information in the window that appears, as seen below.



   a. Define a **Project Name**, such as **rhamt**.

   b. Optionally, define a **Project Display Name** to help describe the project.

   c. Optionally, define a **Project Description** to help provide context on how the project will be used.

d. Click the **Browse** button and import the desired web console template. These are included in ***RHAMT_HOME*/openshift/templates**. Once imported, the JSON is visible in the bottom text area.

6. Click the **Create** button to proceed to the next screen.

7. If you would like to save the template as a resource for future projects, check the **Save template** box.

8. Click the **Continue** button to proceed to the next screen.

9. Review the default values provided, adjusting as necessary. For instance, the **web-template-empty-dir-executor.json** file defines 2 CPUs, 4GB of memory, and a 20GB persistent volume.

10. Click the **Create** button to import the template into your project.

Once completed, you can access the web console from a browser.

2.2.4. Access the Web Console

Once the web console has been deployed on OpenShift, you can access it from a browser. The **deploy.sh** script outputs the link, shown in the example below as ***WEB_CONSOLE_URL***, to use to open the web console.

Example: deploy.sh Output

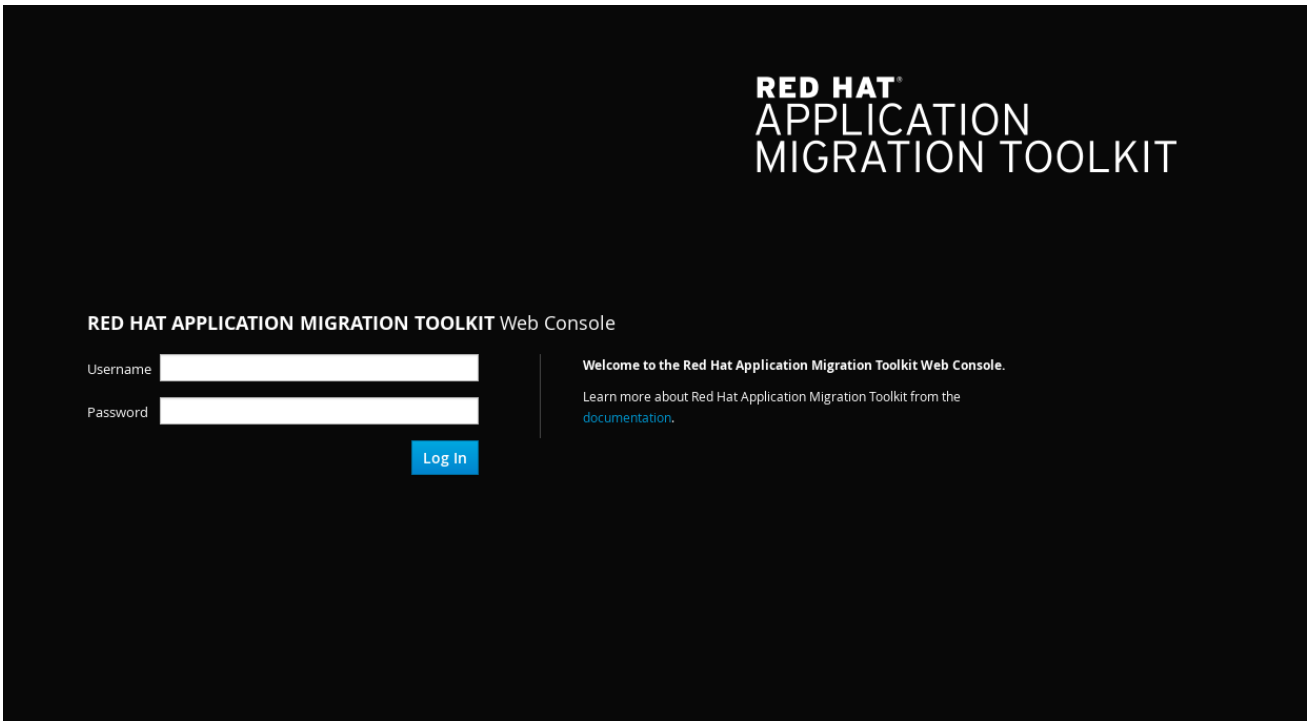
```
...
-> Deploy RHAMT Web Console ...
Upload, build and deployment successful!

Open WEB_CONSOLE_URL to start using the RHAMT Web Console on OpenShift
(user='rhamt',password='password')
```

You can also access the web console from the OpenShift console at ***OPENSHIFT_URL*/console/project/rhamt/overview** by clicking the link in the **RHAMT WEB CONSOLE HTTP** application. If you renamed the OpenShift project when deploying, be sure to replace **rhamt** in this URL with the name of your project.

NOTE

If the web console does not load immediately, check the status of the project in the OpenShift console to see if it is still processing or if there were errors.

Figure 2.4. Welcome Page



Authentication is required in order to access the web console. The default user's credentials are **rhamt** and **password**. See Configuring Authentication for the Web Console for more information on configuring authentication for the web console.

2.2.5. Troubleshoot the Web Console OpenShift Install

The following steps discuss common techniques for troubleshooting the web console in an OpenShift environment. These instructions are focused on issues specific to the web console, for OpenShift specific issues refer to the following troubleshooting sections.

- Troubleshooting OpenShift SDN
- Build Troubleshooting

2.2.5.1. Ensure Latest Image Version

The first step in troubleshooting in an OpenShift environment is to ensure that the latest image is in use.

NOTE

If you have deployed the web console by pasting in a JSON template, then no image stream is created and the following steps are not applicable.

From your OpenShift environment perform the following steps.

1. Access the OpenShift console by navigating to ***OPENSHIFT_URL*/console/project/rhamt/overview**. If you renamed the OpenShift project when deploying, be sure to replace **rhamt** in this URL with the name of your project.
2. Hover over **Builds** along the left side of the console.
3. Click **Images** from the options that appear.

4. Ensure that the column under **Tags** indicates that each image is on the **latest** stream.

5. If the latest image is not in use, follow the steps at OpenShift Installation to redeploy the latest image of the web console.

2.2.5.2. Examine and Collect the Web Console Logs

Each pod is configured to provide detailed logging that assists with narrowing down the precise cause of an issue. The following steps discuss viewing and obtaining these logs.

2.2.5.2.1. Using the OpenShift Console

The following steps walk through the process to examine the logs for each pod.

1. Access the OpenShift console by navigating to ***OPENSHIFT_URL*/console/project/rhamt/overview**. If you renamed the OpenShift project when deploying, be sure to replace **rhamt** in this URL with the name of your project.

2. Hover over **Applications** along the left side of the console.

3. Click **Pods** from the options that appear.

4. Click the name of the pod that you wish to examine. To examine the current web console pod, select the **rhamt-web-console-*POD_NAME*** that is in a **Running** state.

5. Click **Logs** from the options along the top.

6. To download the log file navigate to the top of the page and click **Download**.

2.2.5.2.2. Using the OpenShift Client

1. Determine the pod name by executing **oc get pods** and search for the **web-console** entry with a **Running** status.

```
$ oc get pod
sNAME                      READY     STATUS      RESTARTS   AGE
eap-builder-1-build        0/1       Completed   0          1d
rhamt-postgresql-1-hfbdn   1/1       Running     0          1d
rhamt-sso-1-build          0/1       Completed   0          1d
rhamt-web-console-1-build  0/1       Completed   0          1d
rhamt-web-console-1-vt7s5  1/1       Running     1          1d
sso-1-wjl2n                1/1       Running     1          1d
```

   In the above example this is **rhamt-web-console-1-vt7s5**.

2. Use **oc logs** to examine the current pod's log.

```
oc logs POD_NAME
```

3. The output may be redirected to obtain a copy of the current log.

```
oc logs POD_NAME > ./rhamt-openshift-POD_NAME.log
```

2.2.5.3. Common Issues with Web Console OpenShift

2.2.5.3.1. Executor Pod Throws NoRouteToHostException

When accessing the executor pod's logs the following error is seen.

```
13:44:03,501 SEVERE [org.jboss.windup.web.messaging.executor.ExecutorBootstrap] (main) Could not start messaging listener due to: Failed to connect to any server. Servers tried: [http-remoting://192.0.2.4:8080 (java.net.NoRouteToHostException: No route to host)]: javax.naming.CommunicationException: Failed to connect to any server. Servers tried: [http-remoting://192.0.2.4:8080 (java.net.NoRouteToHostException: No route to host)]
[...]
```

What it means:

A **NoRouteToHostException** indicates that this pod isn't able to connect to the web console pod.

How to resolve it:

In a new deployment this is expected, as the executor starts before the web console. Otherwise, examine the web console pod and resolve any errors seen here. Once the web console is running successfully this error should be resolved.

2.2.5.3.2. Pod Reports Insufficient Resources

After attempting to deploy Web Console on OpenShift, the pod is unable to start, and the following error is seen in the **Events** tab.

```
0/9 nodes are available: 4 Insufficient cpu, 4 MatchNodeSelector, 9 Insufficient memory.
```

What it means:

The resource quota for the OpenShift project has been met, and the pod is unable to obtain the requested resources.

How to resolve it:

Perform either of the following:

- Increase the quota for the OpenShift project. For additional information on OpenShift quotas, see Quotas and Limit Ranges and Setting Limit Ranges.
- Reduce the requested resources for the web console OpenShift project. It is recommended to have at least 2 CPUs and 4 GB of memory for the project.

Once the request is within the available quota, attempt the deployment once again.

2.2.5.3.3. Pod Takes Longer than 600 seconds to become available

After attempting a deployment, the **-deploy** pods timeout and report the following error.

```
error: update acceptor rejected rhamt-web-console-executor-1: pods for rc 'rhamt/POD_NAME' took longer than 600 seconds to become available
```

These errors appear after the pods timeout and are placed into an error state.

What it means:

The deployment pods are unable to successfully launch the pods.

This error can be caused by a number of sources, with the following being the most common:

- The OpenShift instance is currently out of resources to deploy the pod in a timely manner.
- The images were unable to be successfully pulled from the registry.

How to resolve it:

Attempt the deployment again, and view the logs and events of the non deployment pods while they are being created. These messages will provide context to the underlying errors resulting in the deployment pod timeouts.

- To address the first issue reported, where the OpenShift instance is out of resources, follow the instructions in Analyzing Cluster Capacity from the *Cluster Administration* guide in the OpenShift documentation to determine the cluster capacity. Once the capacity has increased, or there are fewer jobs executing, attempt the deployment once again.
- To address the second issue reported, where the images are unable to be pulled from the registry, access the registry to ensure the images are present. This link also includes instructions on examining the logs for the Docker registry, and can be used to troubleshoot the issue further.

2.2.5.4. Report Issues with Web Console OpenShift

{ ProductName} uses JIRA as its issue tracking system. If you encounter any issues while using the web console, please file a JIRA Issue by following the below instructions.

NOTE

If you do not have one already, you must sign up for a JIRA account in order to create a JIRA issue.

1. Open a browser and navigate to the JIRA Create Issue page.
   If you have not yet logged in, click the **Log In** link at the top right side of the page and enter your credentials.
2. Choose the following options and click the **Next** button.
   - **Project**: Choose *Red Hat Application Migration Toolkit (WINDUP)* .
   - **Issue Type**: *Bug*
3. On the next screen complete the following fields.
   - **Summary**: Enter a brief description of the problem or issue.
   - **Environment**: Indicate that this is an OpenShift installation of the web console, and include any environment variables in use with the image.
   - **Description**: Provide a detailed description of the issue. Be sure to include any errors encountered and exception traces.
   - **Attachment**: Include the logs obtained in Examine and Collect the Web Console Logs. At a minimum this should include the logs from each pod.

If the application or archive causing the issue does not contain sensitive information and you are comfortable sharing it with the RHAMT development team, attach it to the issue using the **browse** button.

4. Click the **Create** button to create the JIRA issue.

CHAPTER 3. USING THE WEB CONSOLE TO ANALYZE APPLICATIONS

In order to use the web console to analyze applications, you must create a project. Each project is a way to group applications for analysis and specifies the settings to use during the analysis of its applications. The analysis process generates reports that provide information about the changes necessary for a migration or modernization effort.

Follow these steps to use the web console to analyze your applications and review the results.

1. Add a project.
2. Add applications to the project.
3. Specify the analysis configuration.
4. Execute the analysis.
5. View the results of the analysis.

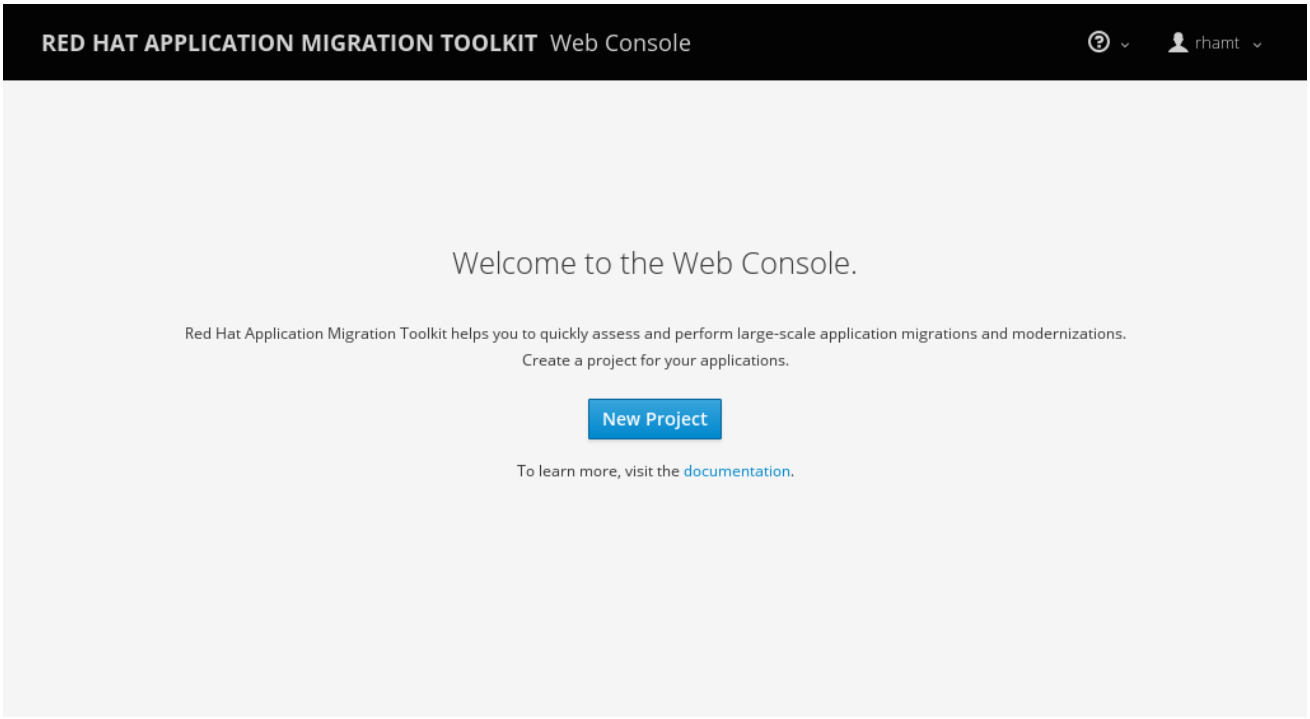
NOTE

Click the **Projects** link at the top of the web console to return to the project list at any time. Visit the help menu for an **About** page and a link to the RHAMT documentation.

3.1. ADD A PROJECT

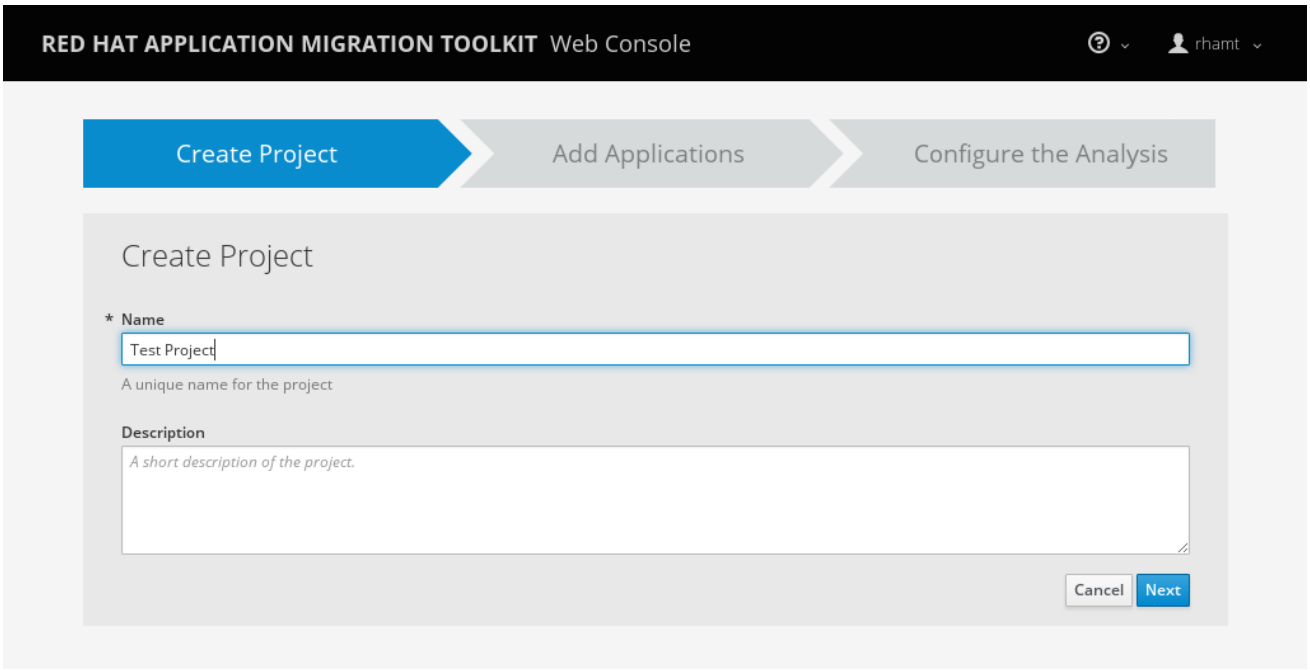
When you first access the web console, you will be prompted to set up a new project.

Figure 3.1. Home



Click the **New Project** button to launch the wizard to set up a new migration project.

Figure 3.2. Add Project

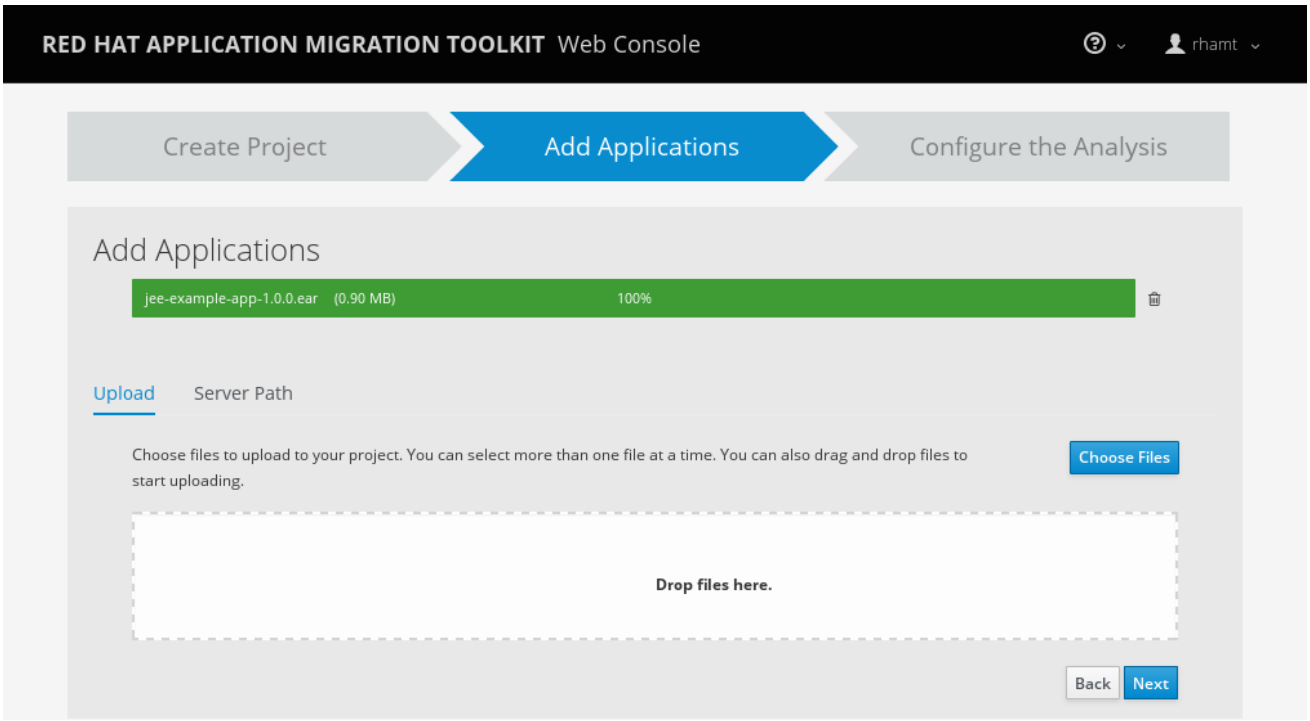


Specify a name and an optional description for this project and press **Next** to continue.

3.2. ADD APPLICATIONS TO A PROJECT

Specify the applications to add to this project. You can either upload applications or register a server path that contains applications.

Figure 3.3. Add Applications



Upload Applications

You can use the **Choose Files** button to select applications, or you can drag and drop applications into the area provided. This uploads the selected applications to the RHAMT server.

Register a Server Path

Select the **Server Path** tab and enter a path on the server that contains applications to be included in this project. This does not copy the files to the RHAMT server, but instead evaluates the applications in the specified location.
This is useful for the following cases:

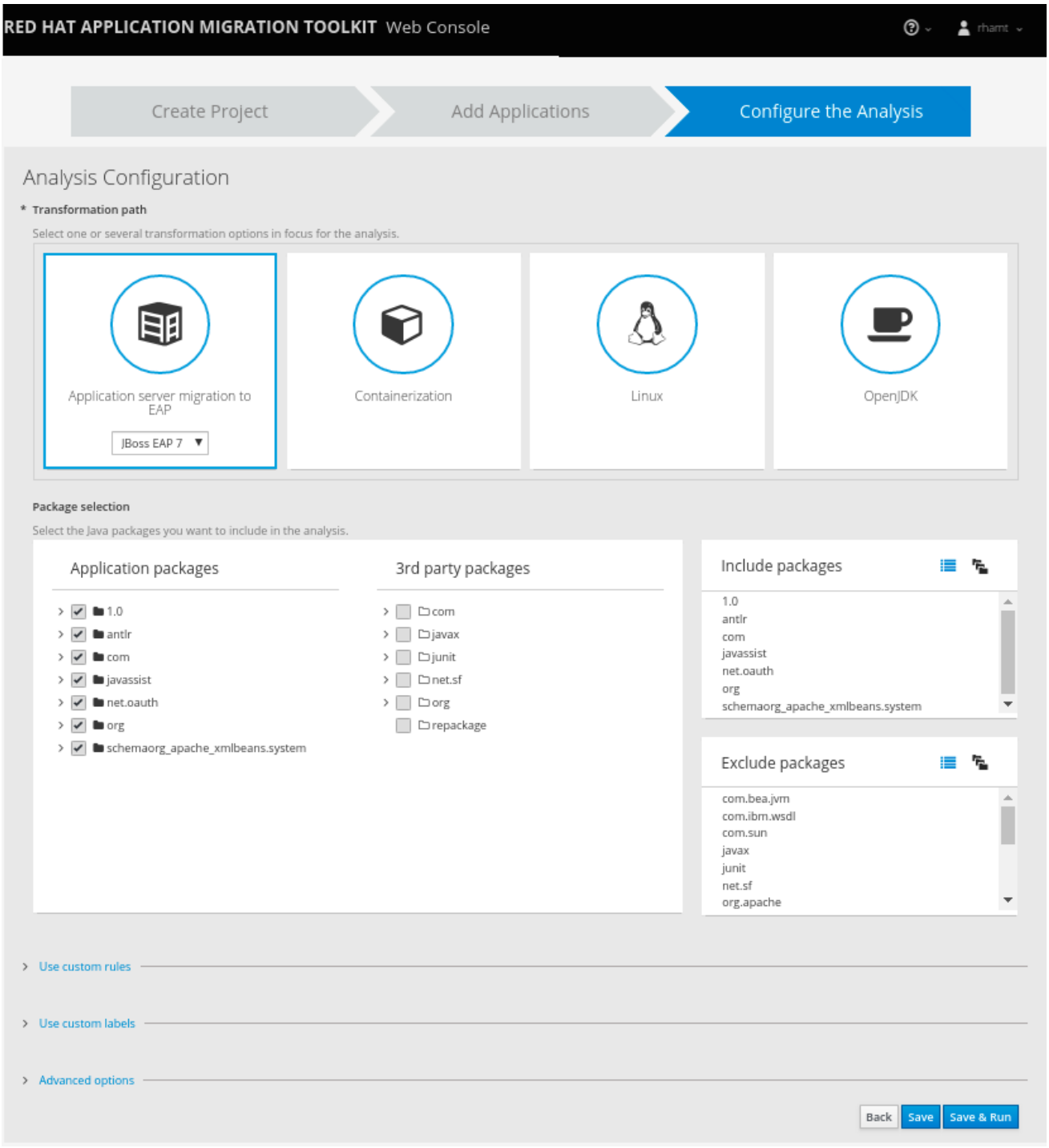
- You want to register an existing directory on the server that contains applications, for example, from a nightly automatic build process. This way, the RHAMT server will analyze the latest versions of applications.
- You want to register an application as an exploded Java archive. In this case, be sure to check the **Directory is an exploded Java application archive** checkbox.

Once you have specified one or more applications for this project, press **Next** to continue.

3.3. SPECIFY THE ANALYSIS CONFIGURATION

Configure the settings for the analysis, such as the transformation path, packages, and other advanced options.

Figure 3.4. Configure Analysis



Transformation Path

Select the transformation path for your applications. The targets displayed under the Transformation Path heading are the most commonly used options:

- JBoss EAP 7 (**eap:7**)
- JBoss EAP 6 (**eap:6**)
- Containerization (**cloud-readiness**)
- Linux (**linux**)
- Open JDK (**openjdk**)

Other available targets can be selected using the *Advanced Options* dialogue.

Include Packages

Select which packages to analyze. If none are selected, all packages will be decompiled and analyzed.

Exclude Packages

Select which packages to exclude from analysis.

Custom Rules

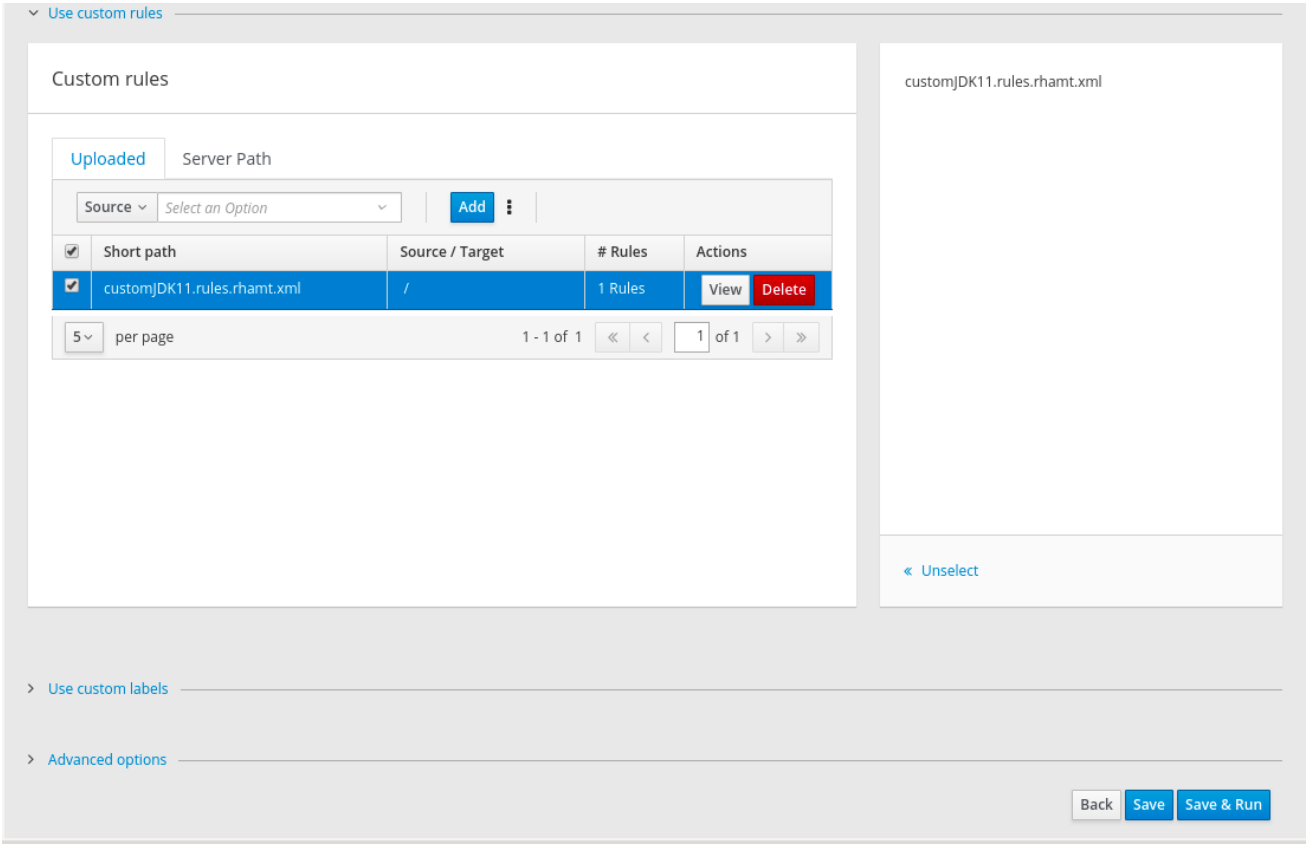
Select which custom rulesets to use during analysis.

Custom rules can be maintained for the current RHAMT project (project scope) or for all RHAMT projects (global scope).

Project custom rules are maintained using the controls below.

The **Add** button allows the user to select the rules files (**.windup.xml** or **.rhamt.xml**). Selected (checked) rules are shown in the right-hand panel and will be executed during the analysis.

Figure 3.5. Custom Rules



See Using Global Custom Rules and Labels for maintaining global custom rules.

Custom Labels

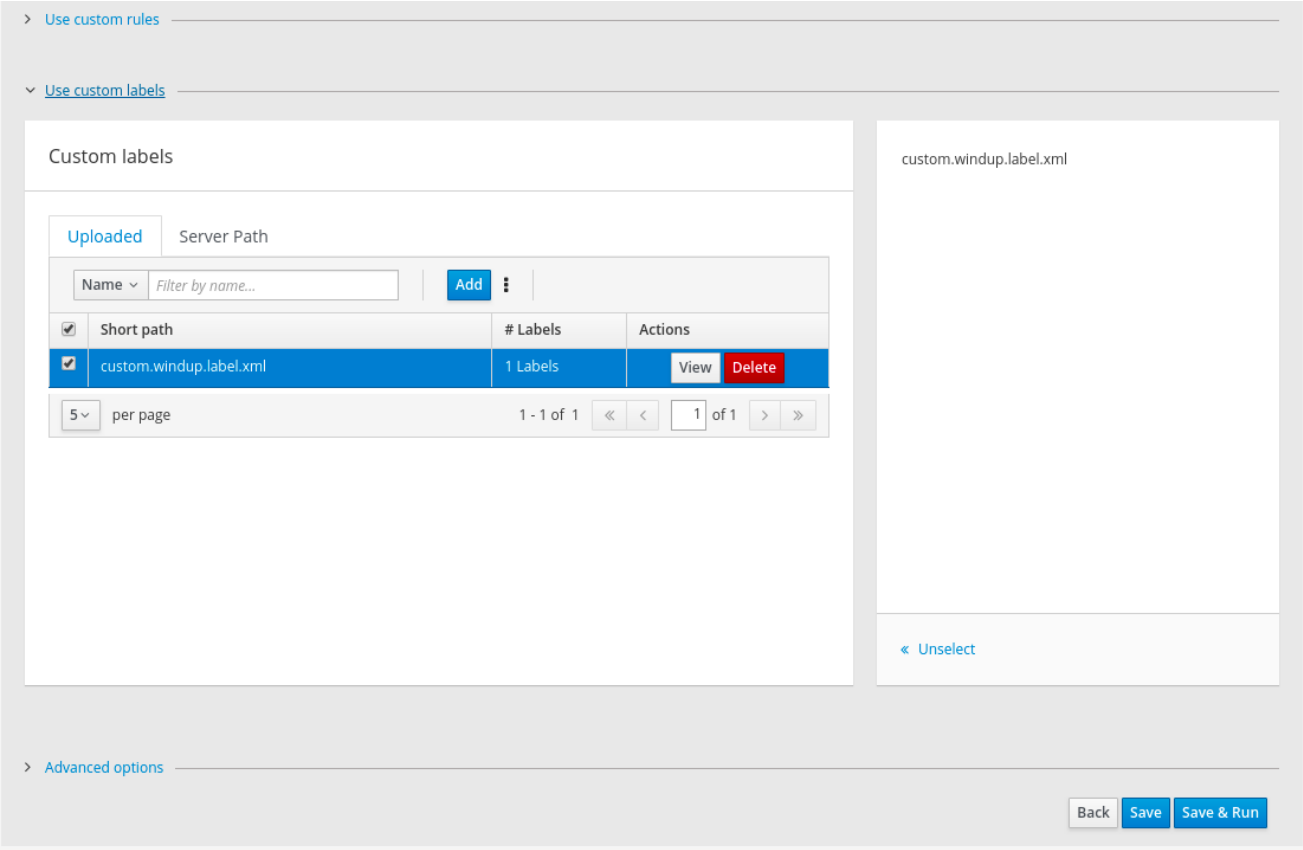
Select which custom labels to use during analysis.

Custom labels can be maintained for the current RHAMT project (project scope) or for all RHAMT projects (global scope).

Project custom rules are maintained using the controls below.

The **Add** button allows the user to select the rules files (**.windup.label.xml** or **.rhamt.label.xml**). Selected (checked) rules are shown in the right-hand panel and will be executed during the analysis.

Figure 3.6. Custom Labels



See Using Global Custom Rules and Labels for maintaining global custom labels.

Advanced Options

Set additional RHAMT options. See the RHAMT Command-line Arguments section of the RHAMT *CLI Guide* for a description of each RHAMT argument.

Press **Save** to save the analysis configuration, or press **Save & Run** to save and execute the analysis using these settings.

3.4. EXECUTE THE ANALYSIS

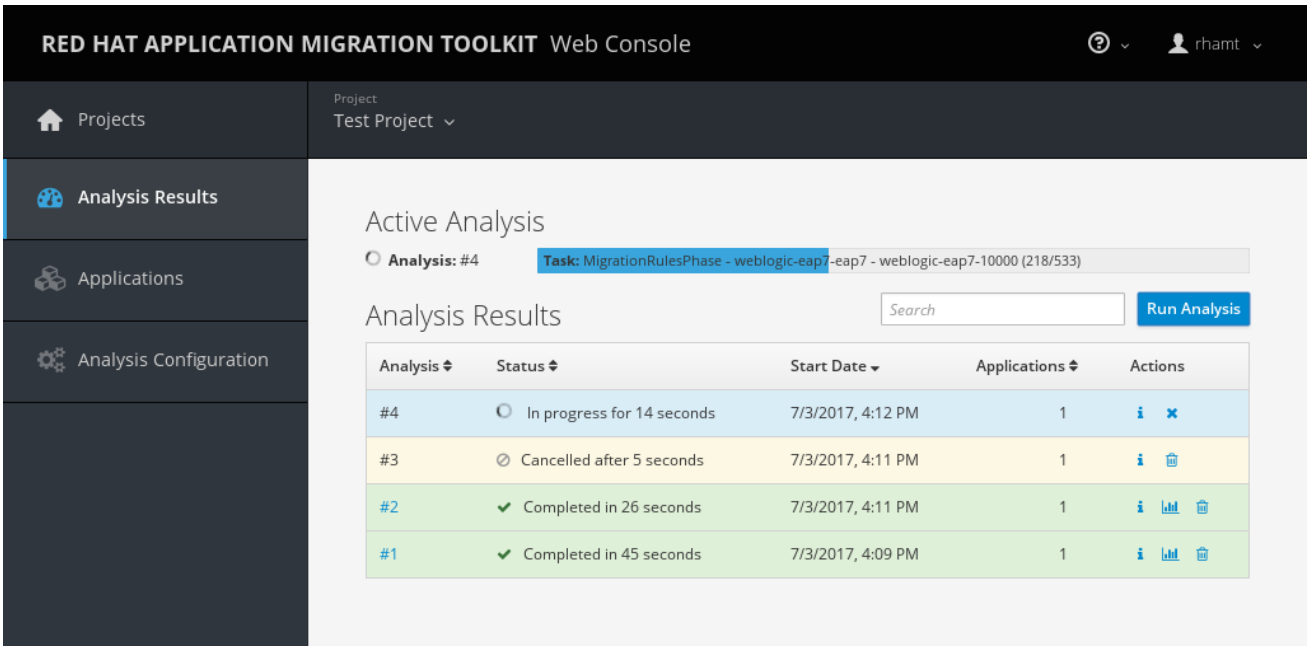
From the analysis configuration page, click the **Save & Run** button to execute the analysis.

On the **Analysis** page, the progress of the analysis that is currently executing is shown. Completed, queued, and in-progress executions are listed in the table. Click the **Run Analysis** to execute the analysis again with the latest configuration.

3.5. VIEW THE RESULTS OF AN ANALYSIS

Once you have executed RHAMT analysis on a project, the analysis is listed in a table that provides the analysis ID, status, and date started. Each row includes actions available for that analysis, including viewing the analysis details and generated reports, as well as canceling or deleting the analysis.

Figure 3.7. Analysis List

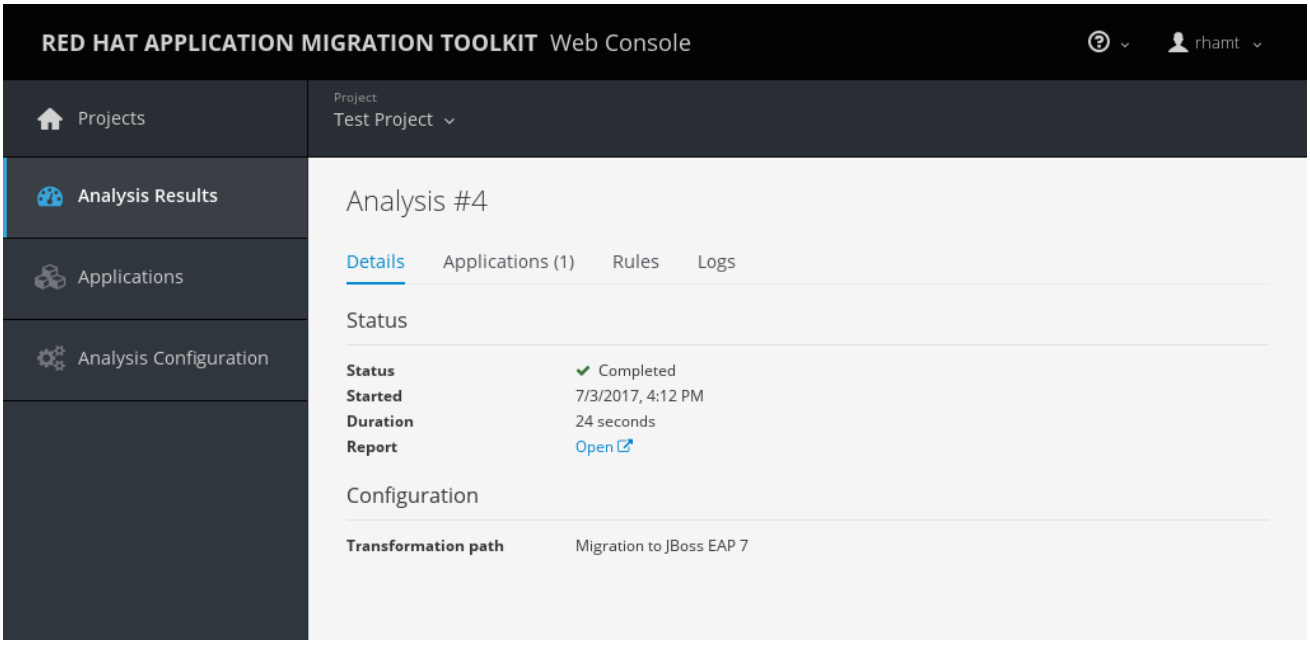


Click the link in the **Analysis** column to view the reports or click the information icon in the **Actions** column to view the analysis details.

3.5.1. Examine Analysis Details

The details of an analysis can be viewed by clicking the information icon in the **Actions** column of the Analysis Results table.

Figure 3.8. Analysis Details



This page provides the following tabs with information about this analysis.

Details

This tab shows the status, start date, and duration of the analysis as well as the configuration settings that were used for this analysis.

Applications

This tab lists the applications that were included in this analysis.

Rules

This tab lists the rules that were evaluated during this analysis.

NOTE

You can view all system and custom rules by selecting **Rules Configuration** from the user drop down.

Logs

This tabs shows the output from this RHAMT analysis engine execution.

3.5.2. Review the Reports

From the analysis table, click the report link in the **Actions** column to view the reports for this analysis. This opens a new window with the generated RHAMT reports.

See the Review the Reports section of the RHAMT *CLI Guide* for information on the RHAMT reports and how to use them to assess your migration or modernization effort.

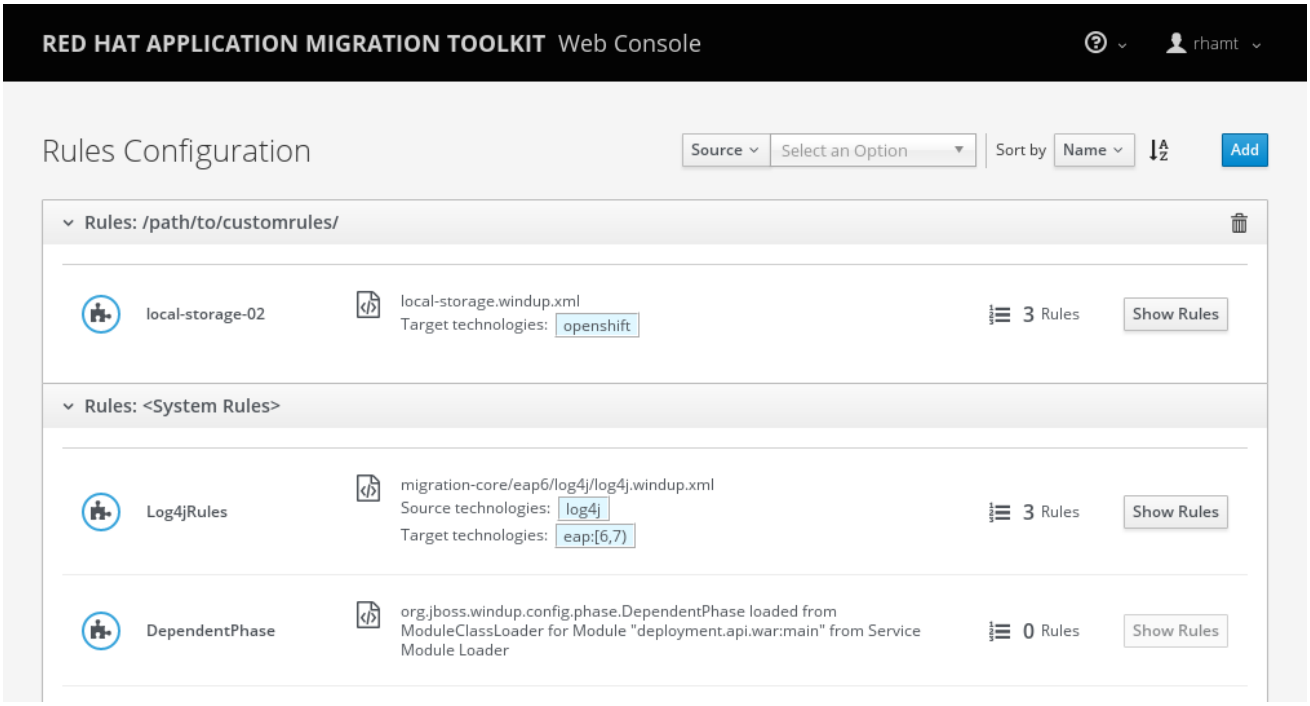
CHAPTER 4. USING CUSTOM RULES AND LABELS

4.1. ADDING CUSTOM RULES

You can add your own custom rules to use during analysis of your applications. For information on writing custom RHAMT rules, see the RHAMT *Rules Development Guide*.

Select **Rules Configuration** from the user drop down to view all existing system and custom rules.

Figure 4.1. Add Custom Rules



To add your own custom rules, click the **Add** button. You can either upload rules or register a server path that contains the rules.

Upload Rules

You can use the **Choose Files** button to select ruleset files, or you can drag and drop the files into the area provided. This uploads the selected ruleset files to the RHAMT server. Click **Add** to upload the rules.

Register a Server Path

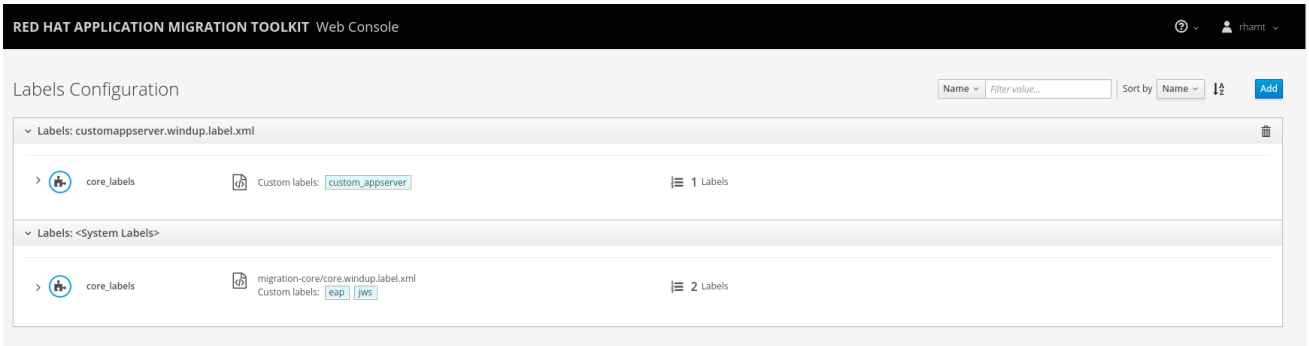
Select the **Server Path** tab and enter a path on the server that contains rules to be available to projects. This does not copy the files to the RHAMT server, but instead uses the rules found in the specified location during analysis. This way, if the rules are updated in this location, the RHAMT server will always use the latest versions of rules during analysis. Click **Add** to register the rules.

Custom rulesets may be selected individually during a project analysis. To enable these select the ruleset in the **Use local custom rules** section of the analysis configuration.

4.2. ADDING CUSTOM LABELS

Select **Labels Configuration** from the user drop down to view all existing system and custom labels.

Figure 4.2. Add Custom Labels



To add your own custom labels, click the **Add** button. You can either upload labels or register a server path that contains the labels files.

Upload Labels

You can use the **Choose Files** button to select label files, or you can drag and drop the files into the area provided. This uploads the selected label files to the RHAMT server. Click **Add** to upload the labels.

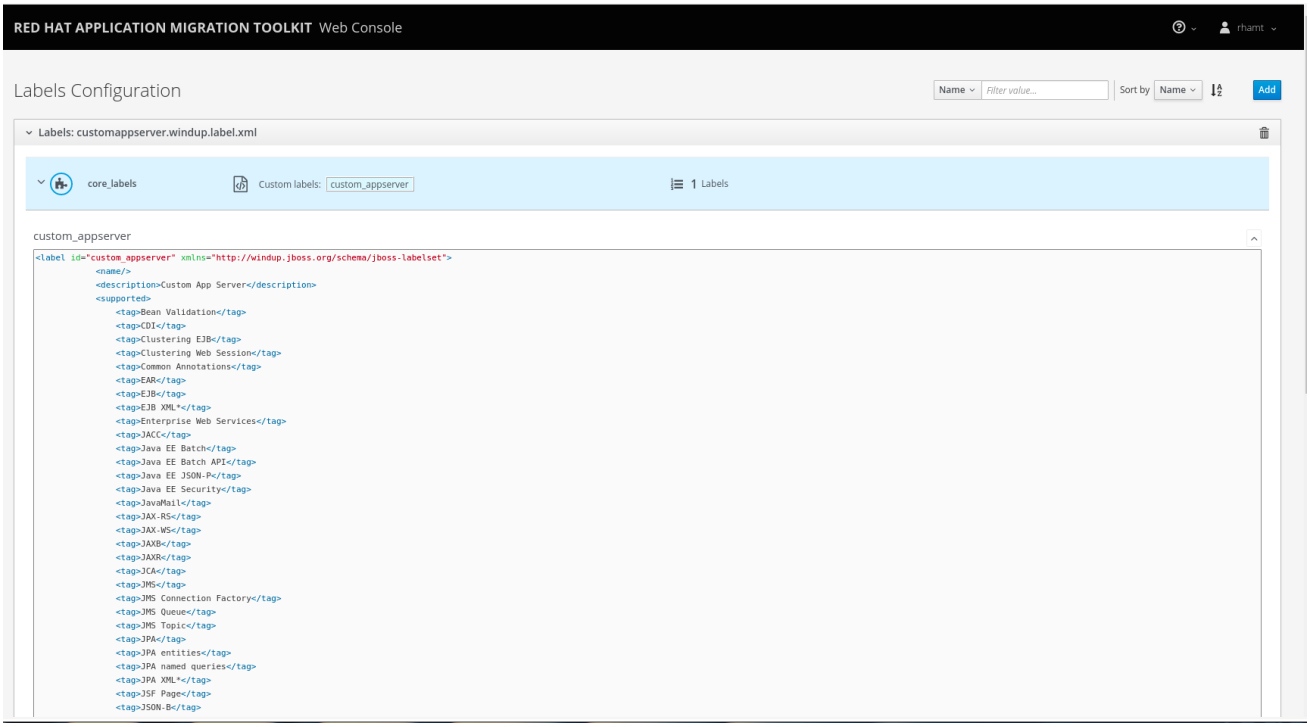
Register a Server Path

Select the **Server Path** tab and enter a path on the server that contains labels to be available to projects. This does not copy the files to the RHAMT server, but instead uses the labels found in the specified location during analysis.

This way, if the labels are updated in this location, the RHAMT server will always use the latest versions of labels during analysis. Click **Add** to register the labels.

Clicking on the *Labels* icon displays the contents of the labels file.

Figure 4.3. View Labels File Contents



CHAPTER 5. CONFIGURING AUTHENTICATION FOR THE WEB CONSOLE

You can configure the web console to require authentication, which is handled by Red Hat Single Sign-On. When enabled, users will be required to authenticate before being granted access to the web console.

It is recommended to complete the following steps to configure authentication for the web console.

1. Enable authentication for the web console.

NOTE

If you have installed web console on OpenShift, authentication is already enabled and cannot be disabled.

2. Change the administrative user's credentials.
3. Remove the default web console user.
4. Add web console users.

5.1. ENABLE AUTHENTICATION FOR WEB CONSOLE

NOTE

If you have installed web console on OpenShift, authentication is already enabled and cannot be disabled.

Run the following script to require users to log in before accessing the web console. This script configures the Red Hat Single Sign-On login page to require users to authenticate before granting access to the web console.

```
$ RHAMT_HOME/switch_to_authentication_required.sh
```

NOTE

In a Windows environment, use the **switch_to_authentication_required.bat** script.

Now, whenever you start the web console, users will be required to authenticate to access it.

5.2. CHANGE THE ADMINISTRATIVE USER'S CREDENTIALS

When you enable authentication for the web console, a default administrative user is provided with the username **admin** and password **password**. You should change this password so that only those that are authorized can make further changes to web console users.

Follow these steps to change the default administrative user's password.

1. Make sure that the web console is running.

2. Open the Red Hat Single Sign-On administration console.
   - For a ZIP installation:
     a. Navigate to **http://localhost:8080/auth/** in a browser.
     b. Select **Administration Console** to access the Red Hat Single Sign-On administration console.
   - For an OpenShift installation:
     a. Navigate to ***OPENSHIFT_URL*/console/project/rhamt/overview** in a browser.

NOTE

If you renamed the OpenShift project when deploying, replace **rhamt** with the name of your project.

     b. Click the link in the **SSO HTTPS** application and add "/auth" to the end of the URL.
     c. Select **Administration Console** to access the Red Hat Single Sign-On administration console.
3. Log in with the default credentials of **admin** and **password**.
4. In the upper left corner, select the **Master** realm from the drop down.
5. In the left-side navigation menu, select **Users** and then click **View all users**.
6. From the **admin** user's row, click **Edit**.
7. Select the **Credentials** tab.
8. Enter the new password in the **New Password** and **Password Confirmation** fields.
9. Change the **Temporary** field to **OFF** to not require the user to change the password upon next login.
10. Click **Reset Password** and then click **Change password** in the popup.

You can also remove this default administrative user completely and create your own administrative users. However, be sure to add the new users before removing the default user.

5.3. REMOVE THE DEFAULT WEB CONSOLE USER

A default web console user is provided with the web console with the username **rhamt** and password **password**. When you enable authentication for the web console, you should remove this user so that the web console can only be accessed by authorized users.

Follow these steps to remove the default web console user.

1. Make sure that the web console is running.
2. Open the Red Hat Single Sign-On administration console.
   - For a ZIP installation:

a. Navigate to **http://localhost:8080/auth/** in a browser.

b. Select **Administration Console** to access the Red Hat Single Sign-On administration console.

- For an OpenShift installation:

a. Navigate to ***OPENSHIFT_URL*/console/project/rhamt/overview** in a browser.

NOTE

If you renamed the OpenShift project when deploying, replace **rhamt** with the name of your project.

b. Click the link in the **SSO HTTPS** application and add "/auth" to the end of the URL.

c. Select **Administration Console** to access the Red Hat Single Sign-On administration console.

3. Log in with an administrative user's credentials. The default credentials are **admin** and **password**.
4. In the upper left corner, select the **Rhamt** realm from the drop down.
5. From the left-side navigation menu, select **Users** and then click **View all users**.
6. From the **rhamt** user's row, click **Delete** and confirm.

5.4. ADD A NEW WEB CONSOLE USER

When authentication is enabled for the web console, administrators will need to add users so that they can access the web console.

Follow these steps to add a new web console user.

1. Make sure that the web console is running.
2. Open the Red Hat Single Sign-On administration console.
   - For a ZIP installation:

a. Navigate to **http://localhost:8080/auth/** in a browser.

b. Select **Administration Console** to access the Red Hat Single Sign-On administration console.

   - For an OpenShift installation:

a. Navigate to ***OPENSHIFT_URL*/console/project/rhamt/overview** in a browser.

NOTE

If you renamed the OpenShift project when deploying, replace **rhamt** with the name of your project.

b. Click the link in the **SSO HTTPS** application and add "/auth" to the end of the URL.

c. Select **Administration Console** to access the Red Hat Single Sign-On administration console.

3. Log in with an administrative user's credentials. The default credentials are **admin** and **password**.
4. In the upper left corner, select the **Rhamt** realm from the drop down.
5. From the left-side navigation menu, select **Users** and then click **Add user**.
6. Enter the **Username**, **First Name**, **Last Name**, and any other required fields and click **Save**.
7. Once the user has been added, select the **Credentials** tab.
8. Enter a temporary password in the **New Password** and **Password Confirmation** fields, and leave the **Temporary** field set to **ON**.
9. Click **Reset Password** and then click **Change password** in the confirmation popup.

The user is enabled by default and will be required to set a new password when they log in to the web console with this temporary password.

Revised on 2020-03-19 14:03:20 UTC