Simplify Migration of Java Applications
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
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
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. Deploy the RHAMT Application 5  
  2.2.3. Access the Web Console 6

## CHAPTER 3. USING THE WEB CONSOLE TO ANALYZE APPLICATIONS
3.1. ADD A PROJECT 8  
3.2. ADD APPLICATIONS TO A PROJECT 9  
3.3. SPECIFY THE ANALYSIS CONFIGURATION 10  
3.4. EXECUTE THE ANALYSIS 11  
3.5. VIEW THE RESULTS OF AN ANALYSIS 11  
  3.5.1. Examine Analysis Details 12  
  3.5.2. Review the Reports 13

## CHAPTER 4. USING CUSTOM RULES 14

## CHAPTER 5. CONFIGURING AUTHENTICATION FOR THE WEB CONSOLE
5.1. ENABLE AUTHENTICATION FOR WEB CONSOLE 15  
5.2. CHANGE THE ADMINISTRATIVE USER’S CREDENTIALS 15  
5.3. REMOVE THE DEFAULT WEB CONSOLE USER 16  
5.4. ADD A NEW WEB CONSOLE USER 17
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.

- Java Platform, JRE version 8+
- 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`. 
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. OPENSSHIFT 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 version 3.5 or higher.
- 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. 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. Use the `oc login` command to connect to your OpenShift instance.

4. Review and adjust default values for the installation.

   The `RHAMT_HOME/openshift/deployment.properties` file defines default values, such as `rhamt` as the project name, 10GB as the persistent storage volume size, and 2GB as the requested memory. Review and change any default settings to your needs before running the `deploy.sh` script.

5. Execute the `deploy.sh` script to deploy the web console to OpenShift.

   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:**
   ```bash
   $ deploy.sh
   ...-> Deploy RHAMT Web Console ...
   Open WEB CONSOLE URL to start using the RHAMT web console.
   ```

   Once the script completes, you can access the web console from the `WEB_CONSOLE_URL`.

6. 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.

**Example:**
```bash
...-> Deploy RHAMT Web Console ...
Upload, build and deployment successful!
Open WEB CONSOLE URL to start using the RHAMT web console.
```

**Output:**

```
...-> Deploy RHAMT Web Console ...
Open WEB CONSOLE URL to start using the RHAMT web console.
```
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.
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.
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.

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 current options are:

- **Migration to JBoss EAP 7**
  Execute rules to migrate your applications to Red Hat JBoss Enterprise Application Platform 7.

- **Migration to JBoss EAP 6**
  Execute rules to migrate your applications to Red Hat JBoss Enterprise Application Platform 6.

- **Cloud readiness only**

Select the transformation path for your applications. The current options are:
Only execute rules to assess your applications for cloud and container environment.

If you select migration to JBoss EAP, you can also run cloud readiness rules by checking the Cloud readiness analysis checkbox.

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. See Using Custom Rules for instructions on registering and removing custom rules.

Once a custom ruleset has been registered, it may be selected for execution by clicking on the displayed rule to highlight it. Clicking a highlighted rule will deselect it for the project. During execution, all highlighted rules will be included in the analysis.

To select all of the custom rulesets click Select All, and to deselect all of the custom rulesets click Clear All.

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.
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.

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 tab 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

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.
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:
     
     
     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:

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:
     

     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 2018-04-04 12:21:24 EDT