Migration Toolkit for Applications 6.2

User Interface Guide

Use the Migration Toolkit for Applications user interface to group your applications into projects for analysis.

Migration Toolkit for Applications 6.2 User Interface Guide

Use the Migration Toolkit for Applications user interface to group your applications into projects for analysis.

Legal Notice

Abstract

This guide describes how to use the Migration Toolkit for Applications user interface to accelerate large-scale application modernization efforts across hybrid cloud environments on Red Hat OpenShift.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases. For more details, see our CTO Chris Wright's message .

CHAPTER 1. INTRODUCTION

1.1. ABOUT THE USER INTERFACE GUIDE

This guide is for architects, engineers, consultants, and others who want to use the Migration Toolkit for Applications (MTA) user interface to accelerate large-scale application modernization efforts across hybrid cloud environments on Red Hat OpenShift. This solution provides insight throughout the adoption process, at both the portfolio and application levels: inventory, assess, analyze, and manage applications for faster migration to OpenShift via the user interface.

> **NOTE**
>
> The migration solution that was provided in the Migration Toolkit for Applications 5.*x* releases (migration and modernization of Java applications) is now available with Migration Toolkit for Runtimes 1.0.

1.2. ABOUT THE MIGRATION TOOLKIT FOR APPLICATIONS

What is the Migration Toolkit for Applications?
Migration Toolkit for Applications (MTA) accelerates large-scale application modernization efforts across hybrid cloud environments on Red Hat OpenShift. This solution provides insight throughout the adoption process, at both the portfolio and application levels: inventory, assess, analyze, and manage applications for faster migration to OpenShift via the user interface.

MTA uses an extensive questionnaire as the basis for assessing your applications, enabling you to estimate the difficulty, time, and other resources needed to prepare an application for containerization. You can use the results of an assessment as the basis for discussions between stakeholders to determine which applications are good candidates for containerization, which require significant work first, and which are not suitable for containerization.

MTA analyzes applications by applying one or more rulesets to each application considered to determine which specific lines of that application must be modified before it can be modernized.

MTA examines application artifacts, including project source directories and application archives, and then produces an HTML report highlighting areas needing changes. MTA supports many migration paths including the following:

- Upgrading to the latest release of Red Hat JBoss Enterprise Application Platform

- Migrating from Oracle WebLogic or IBM WebSphere Application Server to Red Hat JBoss Enterprise Application Platform

- Containerizing applications and making them cloud-ready

- Migrating from Java Spring Boot to Quarkus

- Upgrading from OpenJDK 8 to OpenJDK 11

- Upgrading from OpenJDK 11 to OpenJDK 17

- Migrating EAP Java applications to Azure App Service

- Migrating Spring Boot Java applications to Azure App Service

For more information about use cases and migration paths, see the MTA for developers web page.

How does the Migration Toolkit for Applications simplify migration?
The Migration Toolkit for Applications looks for common resources and known trouble spots when migrating applications. It provides a high-level view of the technologies used by the application.

MTA generates a detailed report evaluating a migration or modernization path. This report can help you to estimate the effort required for large-scale projects and to reduce the work involved.

1.3. ABOUT THE USER INTERFACE

The user interface for the Migration Toolkit for Applications allows a team of users to assess and analyze applications for risks and suitability for migration to hybrid cloud environments on Red Hat OpenShift.

Use the user interface to assess and analyze your applications to get insights about potential pitfalls in the adoption process, at both the portfolio and application levels as you inventory, assess, analyze, and manage applications for faster migration to OpenShift.

CHAPTER 2. USER INTERFACE VIEWS

The Migration Toolkit for Applications (MTA) user interface has two views:

- Administration view

- Migration view

In **Administration** view, you configure the instance environment, working with credentials, repositories, HTTP and HTTPS proxy definitions, custom migration targets, and issue management.

In **Migration** view, you perform application assessments and analyses, review reports, and add applications for assessment and analysis.

CHAPTER 3. INSTALLING THE MIGRATION TOOLKIT FOR APPLICATIONS USER INTERFACE

You install the Migration Toolkit for Applications (MTA) user interface as part of the process of installing the MTA Operator on the OpenShift Container Platform.

The MTA Operator is a structural layer that manages resources deployed on Kubernetes (database, front end, back end) to automatically create an MTA instance instead of you doing it manually.

3.1. PERSISTENT VOLUME REQUIREMENTS

To successfully deploy, the MTA Operator requires 3 RWO persistent volumes (PVs) used by different components. If the **rwx_supported** configuration option is set to **true**, the MTA Operator requires an additional 2 RWX PVs that are used by Maven and the hub file storage. The PVs are described in the table below:

Table 3.1. Required persistent volumes

Name	Default size	Access mode	Description
hub database	5 GiB	RWO	Hub database
hub bucket	100 GiB	RWX	Hub file storage; required if the **rwx_supported** configuration option is set to **true**
keycloak postgresql	1 GiB	RWO	Keycloak back end database
pathfinder postgresql	1 GiB	RWO	Pathfinder back end database
cache	100 GiB	RWX	Maven m2 cache; required if the **rwx_supported** configuration option is set to **true**

3.2. INSTALLING THE MIGRATION TOOLKIT FOR APPLICATIONS OPERATOR AND THE USER INTERFACE

You can install the Migration Toolkit for Applications (MTA) and the user interface on OpenShift Container Platform versions 4.12-4.14 when you install the Migration Toolkit for Applications Operator.

Prerequisites

- 4 vCPUs, 8 GiB RAM, and 40 GB persistent storage.

- OpenShift Container Platform 4.12-4.14 installed.

- You must be logged in as a user with **cluster-admin** permissions.

Procedure

1. In the OpenShift Container Platform web console, click **Operators → OperatorHub**.

2. Use the **Filter by keyword** field to search for **MTA**.

3. Click the **Migration Toolkit for Applications** Operator and then click **Install**.

4. On the **Install Operator** page, click **Install**.

5. Click **Operators → Installed Operators** to verify that the MTA Operator appears in the **openshift-mta** project with the status **Succeeded**.

6. Click the **MTA** Operator.

7. Under **Provided APIs**, locate **Tackle**, and click **Create Instance**.
   The **Create Tackle** window opens in **Form** view.

8. Review the CR settings. The default choices should be acceptable, but make sure to check the system requirements for storage, memory, and cores.

9. To work directly with the YAML file, click **YAML** view and review the CR settings that are listed in the **spec** section of the YAML file.
   The most commonly used CR settings are listed in this table:

Table 3.2. Tackle CR settings

Name	Default	Description
cache_data_volume_size	**100 GiB**	Size requested for the cache volume; ignored when **rwx_supported=false**
cache_storage_class	Default storage class	Storage class used for the cache volume; ignored when **rwx_supported=false**
feature_auth_required	**True**	Flag to indicate whether keycloak authorization is required (single user/"noauth")
feature_isolate_namespace	**True**	Flag to indicate whether namespace isolation using network policies is enabled
hub_database_volume_size	**5 GiB**	Size requested for the Hub database volume
hub_bucket_volume_size	**100 GiB**	Size requested for the Hub bucket volume
hub_bucket_storage_class	Default storage class	Storage class used for the bucket volume

Name	Default	Description
keycloak_database_data_volume_size	**1 GiB**	Size requested for the Keycloak database volume
pathfinder_database_data_volume_size	**1 GiB**	Size requested for the Pathfinder database volume
maven_data_volume_size	**100 GiB**	Size requested for the Maven m2 cache volume; deprecated in MTA 6.0.1
rwx_storage_class	NA	Storage class requested for the Tackle RWX volumes; deprecated in MTA 6.0.1
rwx_supported	**True**	Flag to indicate whether the cluster storage supports RWX mode
rwo_storage_class	NA	Storage class requested for the Tackle RW0 volumes
rhsso_external_access	**False**	Flag to indicate whether a dedicated route is created to access the MTA managed RHSSO instance
windup_container_limits_cpu	**1**	Maximum number of CPUs the pod is allowed to use
windup_container_limits_memory	**6Gi**	Maximum amount of memory the pod is allowed to use. You can increase this limit if the pod displays **OOMKilled** errors.
windup_container_requests_cpu	**1**	Minimum number of CPUs the pod needs to run
windup_container_requests_memory	**4Gi**	Minimum amount of memory the pod needs to run

Example YAML file

```
kind: Tackle
apiVersion: tackle.konveyor.io/v1alpha1
metadata:
  name: mta
  namespace: openshift-mta
spec:
  hub_bucket_volume_size: "25Gi"
  maven_data_volume_size: "25Gi"
  rwx_supported: "false"
```

10. Edit the CR settings if needed, and then click **Create**.

11. In **Administration** view, click **Workloads → Pods** to verify that the MTA pods are running.

12. Access the user interface from your browser by using the route exposed by the **mta-ui** application within OpenShift.

13. Use the following credentials to log in:

    - **User name**: admin

    - **Password**: Passw0rd!

14. When prompted, create a new password.

3.3. INSTALLING THE MIGRATION TOOLKIT FOR APPLICATIONS OPERATOR IN A DISCONNECTED OPENSHIFT CONTAINER PLATFORM ENVIRONMENT

You can install the MTA Operator in a disconnected environment by following the generic procedure.

In step 1 of the generic procedure, configure the image set for mirroring as follows:

```
kind: ImageSetConfiguration
apiVersion: mirror.openshift.io/v1alpha2
storageConfig:
  registry:
    imageURL: registry.to.mirror.to
    skipTLS: false
mirror:
  operators:
  - catalog: registry.redhat.io/redhat/redhat-operator-index:v4.12
    packages:
    - name: mta-operator
      channels:
      - name: stable-v6.1
    - name: rhsso-operator
      channels:
      - name: stable
helm: {}
```

3.4. MEMORY REQUIREMENTS FOR RUNNING MTA ON RED HAT OPENSHIFT LOCAL

When installed on Red Hat OpenShift Local, MTA requires a minimum amount of memory to complete its analysis. Adding memory above the required minimum makes the analysis process run faster. The table below describes the MTA performance with varying amounts of memory.

Table 3.3. OpenShift Local MTA memory requirements

Memory (GiB)	Description
10	MTA cannot run the analysis due to insufficient memory

Memory (GiB)	Description
11	MTA cannot run the analysis due to insufficient memory
12	**MTA works and the analysis is completed in approximately 3 minutes**
15	MTA works and the analysis is completed in less than 2 minutes
20	MTA works quickly and the analysis is completed in less than 1 minute

The test results indicate that the minimum amount of memory for running MTA on OpenShift Local is **12 GiB**.

> **NOTE**
>
> - The tests were performed by running the MTA binary analysis through the user interface.
>
> - All the analyses used the **tackle-testapp** binary.
>
> - All the tests were conducted on an OpenShift Local cluster without the monitoring tools installed.
>
> - Installing the cluster monitoring tools requires an additional 5 GiB of memory.

3.4.1. Eviction threshold

Each node has a certain amount of memory allocated to it. Some of that memory is reserved for system services. The rest of the memory is intended for running pods. If the pods use more than their allocated amount of memory, an out-of-memory event is triggered and the node is terminated with a **OOMKilled** error.

To prevent out-of-memory events and protect nodes, use the **--eviction-hard** setting. This setting specifies the threshold of memory availability below which the node evicts pods. The value of the setting can be absolute or a percentage.

Example of node memory allocation settings

- Node capacity: **32 Gi**

- **--system-reserved** setting: **3 Gi**

- **--eviction-hard** setting: **100 Mi**

The amount of memory available for running pods on this node is 28.9 Gi. This amount is calculated by subtracting the **system-reserved** and **eviction-hard** values from the overall capacity of the node. If the memory usage exceeds this amount, the node starts evicting pods.

3.5. RED HAT SINGLE SIGN-ON

MTA delegates authentication and authorization to a Red Hat Single Sign-On (RHSSO) instance managed by the MTA operator. Aside from controlling the full lifecycle of the managed RHSSO

instance, the MTA operator also manages the configuration of a dedicated realm that contains all the roles and permissions that MTA requires.

If an advanced configuration is required in the MTA managed RHSSO instance, such as adding a provider for User Federation or integrating identity providers, users can log into the RHSSO Admin Console through the /**auth**/**admin** subpath in the **mta-ui** route. The admin credentials to access the MTA managed RHSSO instance can be retrieved from the **credential-mta-rhsso** secret available in the namespace in which the user interface was installed.

A dedicated route for the MTA managed RHSSO instance can be created by setting the **rhsso_external_access** parameter to **True** in the **Tackle CR** that manages the MTA instance.

For more information, see Red Hat Single Sign-On features and concepts .

3.5.1. Roles and Permissions

The following table contains the roles and permissions (scopes) that MTA seeds the managed RHSSO instance with:

tackle-admin	Resource Name	Verbs
	addons	delete get post put
	adoptionplans	post
	applications	delete get post put
	applications.facts	delete get post put
	applications.tags	delete get post put
	applications.bucket	delete get post put

	assessments	delete get patch post put
	businessservices	delete get post put
	dependencies	delete get post put
	identities	delete get post put
	imports	delete get post put
	jobfunctions	delete get post put
	proxies	delete get post put
	reviews	delete get post put
	settings	delete get post put
	stakeholdergroups	delete get post put

	stakeholders	delete get post put
	tags	delete get post put
	tagtypes	delete get post put
	tasks	delete get post put
	tasks.bucket	delete get post put
	tickets	delete get post put
	trackers	delete get post put
	cache	delete get
	files	delete get post put
	rulebundles	delete get post put
tackle-architect	**Resource Name**	**Verbs**

	addons	delete get post put
	applications.bucket	delete get post put
	adoptionplans	post
	applications	delete get post put
	applications.facts	delete get post put
	applications.tags	delete get post put
	assessments	delete get patch post put
	businessservices	delete get post put
	dependencies	delete get post put
	identities	get
	imports	delete get post put

	jobfunctions	delete get post put
	proxies	get
	reviews	delete get post put
	settings	get
	stakeholdergroups	delete get post put
	stakeholders	delete get post put
	tags	delete get post put
	tagtypes	delete get post put
	tasks	delete get post put
	tasks.bucket	delete get post put
	trackers	get
	tickets	delete get post put

	cache	get
	files	delete get post put
	rulebundles	delete get post put
tackle-migrator	**Resource Name**	**Verbs**
	addons	get
	adoptionplans	post
	applications	get
	applications.facts	get
	applications.tags	get
	applications.bucket	get
	assessments	get post
	businessservices	get
	dependencies	delete get post put
	identities	get
	imports	get
	jobfunctions	get
	proxies	get
	reviews	get post put

	settings	get
	stakeholdergroups	get
	stakeholders	get
	tags	get
	tagtypes	get
	tasks	delete get post put
	tasks.bucket	delete get post put
	tackers	get
	tickets	get
	cache	get
	files	get
	rulebundles	get

CHAPTER 4. CONFIGURING THE INSTANCE ENVIRONMENT

You can configure the following in **Administration** view:

- General

- Credentials

- Repositories

- HTTP and HTTPS proxy settings

- Custom migration targets

- Issue management

4.1. GENERAL

You can enable or disable the following options:

- Reviewing applications without running an assessment first

- Downloading HTML reports

- Downloading CSV reports

4.2. CONFIGURING CREDENTIALS

You can configure the following types of credentials in **Administration** view:

- Source control

- Maven

- Proxy

4.2.1. Configuring source control credentials

You can configure source control credentials in the **Credentials** view of the Migration Toolkit for Applications (MTA) user interface.

Procedure

1. In **Administration** view, click **Credentials**.

2. Click **Create new**.

3. Enter the following information:

   - Name

   - Description (Optional)

4. In the **Type** list, select **Source Control**.

5. In the **User credentials** list, select **Credential Type** and enter the requested information:

- Username/Password

  - Username

  - Password (hidden)

- SCM Private Key/Passphrase

  - SCM Private Key

  - Private Key Passphrase (hidden)

NOTE

Type-specific credential information such as keys and passphrases is either hidden or shown as [Encrypted].

6. Click **Create**.
MTA validates the input and creates a new credential. SCM keys must be parsed and checked for validity. If the validation fails, the following error message is displayed: **"not a valid key/XML file"**.

4.2.2. Configuring Maven credentials

You can configure new Maven credentials in the **Credentials** view of the Migration Toolkit for Applications (MTA) user interface.

Procedure

1. In **Administration** view, click **Credentials**.

2. Click **Create new**.

3. Enter the following information:

- Name

- Description (Optional)

4. In the **Type** list, select **Maven Settings File.**

5. Upload the settings file or paste its contents.

6. Click **Create**.
MTA validates the input and creates a new credential. The Maven **settings.xml** file must be parsed and checked for validity. If the validation fails, the following error message is displayed: **"not a valid key/XML file"**.

4.2.3. Configuring proxy credentials

You can configure proxy credentials in the **Credentials** view of the Migration Toolkit for Applications (MTA) user interface.

Procedure

1. In **Administration** view, click **Credentials**.

2. Click **Create new**.

3. Enter the following information:

   - Name

   - Description (Optional)

4. In the **Type** list, select **Proxy**.

5. Enter the following information.

   - Username

   - Password

   > **NOTE**
   >
   > Type-specific credential information such as keys and passphrases is either hidden or shown as [Encrypted].

6. Click **Create**.
   MTA validates the input and creates a new credential.

4.3. CONFIGURING REPOSITORIES

You can configure the following types of repositories in **Administration** view:

- Git

- Subversion

- Maven

4.3.1. Configuring Git repositories

You can configure Git repositories in the **Repositories** view of the Migration Toolkit for Applications (MTA) user interface.

Procedure

1. In **Administration** view, click **Repositories** and then click **Git**.

2. Toggle the **Consume insecure Git repositories**switch to the right.

4.3.2. Configuring subversion repositories

You can configure subversion repositories in the **Repositories** view of the Migration Toolkit for Applications (MTA) user interface.

Procedure

1. In **Administration** view, click **Repositories** and then click **Subversion**.

2. Toggle the **Consume insecure Subversion repositories** switch to the right.

4.3.3. Configuring a Maven repository and reducing its size

You can use the MTA user interface to both configure a Maven repository and to reduce its size.

4.3.3.1. Configuring a Maven repository

You can configure a Maven repository in the **Repositories** view of the Migration Toolkit for Applications (MTA) user interface.

> **NOTE**
>
> If the **rwx_supported** configuration option of the Tackle CR is set to **false**, the **Consume insecure artifact repositories** switch is disabled and this procedure is not possible.

Procedure

1. In **Administration** view, click **Repositories** and then click **Maven**.

2. Toggle the **Consume insecure artifact repositories** switch to the right.

4.3.3.2. Reducing the size of a Maven repository

You can reduce the size of a Maven repository in the **Repositories** view of the Migration Toolkit for Applications (MTA) user interface.

> **NOTE**
>
> If the **rwx_supported** configuration option of the Tackle CR is set to **false**, both the **Local artifact repository** field and the **Clear repository** button are disabled and this procedure is not possible.

Procedure

1. In **Administration** view, click **Repositories** and then click **Maven**.

2. Click the **Clear repository** link.

> **NOTE**
>
> Depending on the size of the repository, the size change may not be evident despite the function working properly.

4.4. CONFIGURING HTTP AND HTTPS PROXY SETTINGS

You can configure HTTP and HTTPS proxy settings with this management module.

Procedure

1. In the **Administration** view, click **Proxy**.

2. Toggle **HTTP proxy** or **HTTPS proxy** to enable the proxy connection.

3. Enter the following information:

   - Proxy host

   - Proxy port

4. Optional: Toggle **HTTP proxy credentials** or **HTTPS proxy credentials** to enable authentication.

5. Click **Insert**.

4.5. SEEDING AN INSTANCE

If you are a project architect, you can configure the instance's key parameters in the Controls window, before migration. The parameters can be added and edited as needed. The following parameters define applications, individuals, teams, verticals or areas within an organization affected or participating in the migration:

- Stakeholders

- Stakeholder groups

- Job functions

- Business services

- Tag categories

- Tags

You can create and configure an instance in any order. However, the suggested order below is the most efficient for creating stakeholders and tags.

Stakeholders:

1. Create Stakeholder groups

2. Create Job functions

3. Create Stakeholders

Tags:

1. Create Tag categories

2. Create Tags

Stakeholders and defined by:

- Email

- Name

- Job function

- Stakeholder groups

4.5.1. Creating a new stakeholder group

There are no default stakeholder groups defined. You can create a new stakeholder group by following the procedure below.

Procedure

1. In **Migration** view, click **Controls**.

2. Click **Stakeholder groups**.

3. Click **Create new**.

4. Enter the following information:

   - Name

   - Description

   - Member(s)

5. Click **Create**.

4.5.2. Creating a new job function

Migration Toolkit for Applications (MTA) uses the job function attribute to classify stakeholders and provides a list of default values that can be expanded.

You can create a new job function, which is not in the default list, by following the procedure below.

Procedure

1. In **Migration** view, click **Controls**.

2. Click **Job functions**.

3. Click **Create new**.

4. Enter a job function title in the **Name** text box.

5. Click **Create**.

4.5.3. Creating a new stakeholder

You can create a new migration project stakeholder by following the procedure below.

Procedure

1. In **Migration** view, click **Controls**.

2. Click **Stakeholders**.

3. Click **Create new**.

4. Enter the following information:

   - Email

   - Name

   - Job function – custom functions can be created

   - Stakeholder group

5. Click **Create**.

4.5.4. Creating a new business service

Migration Toolkit for Applications (MTA) uses the business service attribute to specify the departments within the organization that use the application and that are affected by the migration.

You can create a new business service by following the procedure below.

Procedure

1. In **Migration** view, click **Controls**.

2. Click **Business services**.

3. Click **Create new**.

4. Enter the following information:

   - Name

   - Description

   - Owner

5. Click **Create**.

4.5.5. Creating new tag categories

Migration Toolkit for Applications (MTA) uses tags in multiple categories and provides a list of default values. You can create a new tag category by following the procedure below.

Procedure

1. In **Migration** view, click **Controls**.

2. Click **Tags**.

3. Click **Create tag category**.

4. Enter the following information:

   - Name

   - Rank – the order in which the tags appear on the applications

   - Color

5. Click **Create**.

4.5.5.1. Creating new tags

You can create a new tag, which is not in the default list, by following the procedure below.

Procedure

1. In **Migration** view, click **Controls**.

2. Click **Tags**.

3. Click **Create tag**.

4. Enter the following information:

   - Name

   - Tag category

5. Click **Create**.

CHAPTER 5. CREATING AND CONFIGURING A JIRA CONNECTION

You can track application migrations by creating a Jira issue for each migration from within the MTA user interface. To be able to create Jira issues, you first need to do the following:

1. Create an MTA credential to authenticate to the API of the Jira instance that you create in the next step.

2. Create a Jira instance in MTA and establish a connection to that instance.

5.1. CONFIGURING JIRA CREDENTIALS

To define a Jira instance in MTA and establish a connection to that instance, you must first create an MTA credential to authenticate to the Jira instance's API.

Two types of credentials are available:

- **Basic auth** – for Jira Cloud and a private Jira server or data center

- **Bearer Token** – for a private Jira server or data center

To create an MTA credential, follow the procedure below.

Procedure

1. In **Administration** view, click **Credentials**.
   The **Credentials** page opens.

2. Click **Create new**.

3. Enter the following information:

   - **Name**

   - **Description** (optional)

4. In the **Type** list, select **Basic Auth (Jira)** or **Bearer Token (Jira)**:

   - If you selected **Basic Auth (Jira)**, proceed as follows:

     a. In the **Email** field, enter your email.

     b. In the **Token** field, depending on the specific Jira configuration, enter either your token generated on the Jira site or your Jira login password.

       > **NOTE**
       >
       > To obtain a Jira token, you need to log in to the Jira site.

     c. Click **Save**.
        The new credential appears on the **Credentials** page.

   - If you selected **Bearer Token (Jira)**, proceed as follows:

a. In the **Token** field, enter your token generated on the Jira site.

b. Click **Save**.
The new credential appears on the **Credentials** page.

You can edit a credential by clicking **Edit**.

To delete a credential, click **Delete**.

> **NOTE**
>
> You cannot delete a credential that has already been assigned to a Jira connection instance.

5.2. CREATING AND CONFIGURING A JIRA CONNECTION

To create a Jira instance in MTA and establish a connection to that instance, follow the procedure below.

Procedure

1. In **Administration** view, under **Issue Management**, click **Jira**.
The **Jira configuration** page opens.

2. Click **Create new**.
The **New instance** window opens.

3. Enter the following information:

   - Name of the instance

   - URL of the web interface of your Jira account

   - Instance type – select either **Jira Cloud** or **Jira Server/Data center** from the list

   - Credentials – select from the list
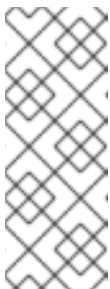
   > **NOTE**
   >
   > If the selected instance type is **Jira Cloud**, only **Basic Auth** credentials are displayed in the list.
   >
   > If the selected instance type is **Jira Server/Data center**, both **Basic Auth** and **Token Bearer** credentials are displayed. Choose the type that is appropriate for the particular configuration of your Jira server or data center.

4. By default, a connection cannot be established with a server with an invalid certificate. To override this restriction, toggle the **Enable insecure communication** switch.

5. Click **Create**.
The new connection instance appears on the **Jira configuration** page.

   Once the connection has been established and authorized, the status in the **Connection** column becomes **Connected**.

If the **Connection** status becomes **Not connected**, click the status to see the reason for the error.

The **Jira configuration** table has filtering by **Name** and **URL** and sorting by **Instance name** and **URL**.

> **NOTE**
>
> A Jira connection that was used for creating issues for a migration wave cannot be removed as long as the issues exist in Jira, even after the migration wave is deleted.

CHAPTER 6. ASSESSING AND ANALYZING APPLICATIONS

You can use the Migration Toolkit for Applications (MTA) user interface to both assess and to analyze applications.

Assessing applications refers to estimating the risks and costs involved in preparing applications for containerization, including time, personnel, and other factors. The results of an assessment can be used as the basis for discussions between stakeholders to determine which applications are good candidates for containerization, which require significant work, and which are not suitable for containerization.

Analyzing applications refers to using rules to determine which specific lines in an application must be modified before the application can be migrated or modernized.

6.1. ASSESSING APPLICATIONS

You can use the Migration Toolkit for Applications (MTA) user interface to determine the risks involved in containerizing an application.

> **NOTE**
>
> The procedure described below uses a built-in questionnaire for assessing the risks involved in containerizing an application. By default, this procedure is required prior to reviewing the application. However, you might want to skip this step and use your own questionnaire instead. In that case, use the Skipping assessment option.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Select the application you want to assess.

   > **NOTE**
   >
   > Only one application can be assessed at a time.

3. Click **Assess**.

4. Select **Stakeholders** and **Stakeholder groups** from the lists to track who contributed to the assessment for future reference.

   > **NOTE**
   >
   > You can add **Stakeholder Groups** or **Stakeholders** on the **Controls** screen of **Migration** view.

5. Click **Next**.

6. Answer each question and then click **Next**.

7. Click **Save and Review** to view the assessment.

6.1.1. Applying assessments to other applications

Many applications are similar enough to each other, and you might want to apply a completed assessment of one application to another application. This can save time and provide consistent answers to assessment questions for similar applications.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Select the application with the completed assessment to copy.

3. Click the Options menu ⋮ at the right of the selected application.

4. Select **Copy assessment** or **Copy assessment and review**.

5. Select the application(s) to which you want to apply the completed assessment.

6. Click **Copy**.

6.1.2. Skipping assessment of applications

By default, the assessment procedure is required prior to reviewing the application. However, you might want to skip assessment and use your own questionnaire instead. In that case, use the option described below.

> **NOTE**
>
> This option is available only for **Admin** and **Architect** users.

Procedure

1. In **Administration** view, click **General**.

2. Toggle the **Allow reviewing applications without running an assessment first** switch.

3. Go to **Migration** view and click **Application inventory**.
   Now the **Review** step is enabled for all applications including those that have not been assessed.

6.2. REVIEWING APPLICATIONS

You can use the Migration Toolkit for Applications (MTA) user interface to determine the migration strategy and work priority for each application.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Select the application you want to review.

> **NOTE**
>
> Only one application can be reviewed at a time.

3. Click **Review**.

4. Select **Proposed action** and **Effort estimate** from the lists. Set **Business criticality** and **Work priority**.

5. Click **Submit review**.
   The fields from **Review** are now populated on the **Application details** page.

6.3. CONFIGURING AND RUNNING AN APPLICATION ANALYSIS

You can analyze more than one application at a time against more than one transformation target in the same analysis.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Click the **Analysis** tab.

3. Select the applications you want to analyze.

4. Review the credentials assigned to the application.

5. Click **Analyze**.

6. Select the **Analysis mode** from the list. Valid options are:

   - Binary.

   - Source code.

   - Source code and dependencies.

   - Upload a local binary. This option only appears if you are analyzing a single application.

7. If you choose **Upload a local binary**, a window opens and you are prompted to **Upload a local binary**. Either drag and drop a file into the area provided or click **Upload** and then select the file to upload.

8. Click **Next**.

9. Select one or more target options for the analysis:

   - Application server migration to:

     - JBoss EAP 7

     - JBoss EAP 6

   - Containerization

   - Quarkus

   - OracleJDK to OpenJDK

   - OpenJDK – upgrades to one of the following JDK versions:

     - OpenJDK 11

- OpenJDK 17

- Linux – ensures there are no Microsoft Windows paths hard-coded into your applications

- Jakarta EE 9 – for migrating from Java EE 8 to Jakarta EE 9

- Spring Boot on Red Hat Runtimes

- Open Liberty

- Camel – for migrating from Apache Camel 2 to Apache Camel 3

- Azure

  - Azure App Service

10. Click **Next**.

11. Select one of the following **Scope** options to better focus the analysis:

    - Application and internal dependencies only.

    - Application and all dependencies, including known Open Source libraries.

    - Select the list of packages to be analyzed manually. If you choose this option, type the file name and click **Add**.

    - Exclude packages. If you choose this option, type the name of the package name and click **Add**.

12. Click **Next**.

13. In **Advanced**, you can attach additional custom rules to the analysis. Select **Manual** or **Repository**.

    > **NOTE**
    >
    > Attaching custom rules is optional if you have already attached a migration target to the analysis. If you have not attached any migration target, you must attach rules.

    - In **Manual** mode, click **Add Rules**. Then either drag and drop the relevant files or select them from their directory and click **Add**.

    - In **Repository** mode, you can add rule files from a Git or Subversion repository.

14. Set any of the following options, if needed:

    - Target

    - Source(s)

    - Excluded rules tags: Rules with these tags are not processed. Add or delete as needed.

    - Enable transaction report: Select the checkbox to generate a DIVA report that displays the call stack, which executes operations on relational database tables.

- Enable automated tagging: Select the checkbox to automatically attach tags to the application. This checkbox is selected by default.

> **NOTE**
>
> The Transactions report is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

> **NOTE**
>
> Note that the automatically attached tags are displayed only *after* you run the analysis.
>
> You can attach tags to the application manually, instead of enabling automated tagging or in addition to it.

> **NOTE**
>
> Analysis engines use standard rules for a comprehensive set of migration targets, but if the target is not included or is a customized framework, custom rules can be added. Custom rules files are validated.

15. Click **Next**.

16. In **Review**, verify the analysis parameters.

17. Click **Run**.
    Analysis status is **Scheduled** as MTA downloads the image for the container to execute. When the image is downloaded, the status changes to **In-progress.**

> **NOTE**
>
> Analysis takes minutes to hours to run depending on the size of the application and the capacity and resources of the cluster.

TIP

MTA relies on Kubernetes scheduling capabilities to determine how many analyzer instances are created based on cluster capacity. If several applications are selected for analysis, by default, only one analyzer can be provisioned at a time. With more cluster capacity, more analysis processes can be executed in parallel.

18. When analysis is complete, you can click the **Report** link to see the results of the analysis.

6.3.1. Viewing analysis details

You can view the details of an analysis by clicking the Options menu ⋮ and selecting **Analysis details**. The details are displayed in the **Analysis details for customers**window. You can choose either YAML or JSON format.

NOTE

You can view the details of an analysis only after you start running the analysis. If the status of an analysis is **Not started**, the **Analysis details** option is disabled.

6.4. CREATING CUSTOM MIGRATION TARGETS

Architects or users with **admin** permissions can create and maintain custom rulesets associated with custom migration targets. Architects can upload custom rule files and assign them to various custom migration targets. The custom migration targets are then available for selecting in the analysis configuration wizard.

Using ready-made custom migration targets makes unnecessary the cumbersome task of configuring custom rules for each analysis run. This simplifies analysis configuration and execution for non-admin users or third-party developers and makes using the MTA tool easier and more straightforward.

Prerequisites

- You must be logged in as a user with **admin** permissions.

Procedure

1. In **Administration** view, click **Custom migration targets**.

2. Click **Create new**.

3. Fill in the name and description of the target.

4. In the **Image** section, upload an image file for the target's icon. The file can be in either PNG or JPEG format, up to 1 MB. If you do not upload any file, a default icon is used.

5. In the **Custom rules** section, select either **Upload manually** or **Retrieve from a repository**.

   - If you have selected **Upload manually**, upload or drag and drop the required rule files from your local drive.

   - If you have selected **Retrieve from a repository**, proceed as follows:

     i. Choose **Git** or **Subversion**.

     ii. Fill in **Source repository**, **Branch** and **Root path**.

     iii. If the repository requires credentials, enter them in the **Associated credentials** field.

6. Click **Create**.
   The new migration target appears on the **Custom migration targets** page. It can now be used by non-admin users in **Migration** view.

6.5. TAGGING AN APPLICATION

You can attach various tags to the application that you are going to analyze. The tags allow classifying applications in multiple dimensions.

Tagging can be either automatic or manual.

6.5.1. Manual tagging

You can tag an application manually, both before or after you run an analysis.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Click the **Analysis** tab.

3. In the row of the required application, click the pen icon.
   The **Update application** window opens.

4. Select the desired tags from the **Select a tag(s)** drop-down list.

5. Click **Save**.

6.5.2. Automatic tagging

MTA translates the technology stack information that the analysis module collects into tags and automatically adds the tags to the application. Automatic tagging is especially useful when dealing with large portfolios of applications.

Automatic tagging of applications is enabled by default. You can disable it by unselecting the **Enable automated tagging** checkbox in the **Advanced** section of the **Analysis configuration** wizard.

> **NOTE**
>
> To tag an application automatically, make sure that the **Enable automated tagging** checkbox is selected *before* you run an analysis of the application.

6.5.3. Viewing the tags of an application

You can view the tags attached to a particular application.

> **NOTE**
>
> You can view the tags that were attached automatically only *after* you have run an analysis of the application.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Click the **Analysis** tab.

3. Click the name of the required application.
   A side drawer opens.

4. In the side drawer, click the **Tags** tab.
   You can see the tags attached to the application.

   The tags can be filtered by source and tag category. The sources are **Analysis** and **Manual**. The categories are displayed in a drop-down list, for example, **HTTP**, **MVC**, **Web**, **Observability**, **Persistence**, **Application Type**, **Data Center**.

6.6. REVIEWING AN ANALYSIS REPORT

An MTA analysis report contains a variety of sections, including a listing of the technologies used by the application, the dependencies of the application, and the lines of code that must be changed to successfully migrate or modernize the application.

For more information on the contents of an MTA analysis report, see the Reviewing the reports

Procedure

1. In **Migration** view, click **Application inventory**.

2. Expand the application with a completed analysis.

3. Click **Reports**.

4. Click the dependencies or source links.

5. Click the tabs to review the report.

6.6.1. Downloading an analysis report

For your convenience, you can download analysis reports. By default, this option is disabled, but you can enable it as described below.

Procedure

1. In **Administration** view, click **General**.

2. Toggle the **Enable downloads for HTML reports** and **Enable downloads for CSV reports** switches.

3. Go to **Migration** view and click **Application inventory**.

4. Open the page of the application for which you ran an analysis.

5. Click **Reports**.

6. Click the **Download report** link.
   The report is downloaded and saved in the **Downloads** directory as **report.tar.gz**.

> **NOTE**
>
> To download a report as an HTML file, you can enable the download option either before or after you run the analysis.
>
> To download a report as an CSV file, you must enable the download option *before* you run the analysis.

CHAPTER 7. WORKING WITH APPLICATIONS

You can use the Migration Toolkit for Applications (MTA) user interface to do the following:

- Add applications

- Assign application credentials

- Import a list of applications

- Download a CSV template for importing application lists

7.1. APPLICATION ATTRIBUTES

You can add applications to the Migration Toolkit for Applications (MTA) user interface manually or by importing a list of applications.

MTA user interface applications have the following attributes:

- Name (free text)

- Description (optional; free text)

- Business service (optional; chosen from a list)

- Tags (optional; chosen from a list)

- Owner (optional; chosen from a list)

- Contributors (optional; chosen from a list)

- Source code (path entered by user)

- Binary (path entered by user)

7.2. ADDING APPLICATIONS

You can add an application to the **Application Inventory** for assessment and analysis.

TIP

Before creating an application, it is helpful to set up business services, check tags and tag categories, and create additions as needed.

Procedure

1. In **Migration** view, click **Application Inventory**.

2. Click **Create new**.

3. Enter the following information or choose from a list:

   - Name

   - Description (optional)

- Business service (optional)

- Tags (optional; one or more)

- Owner (optional)

- Contributors (optional; one or more)

- Comments (optional)

4. Click the arrow to the left of **Source Code**.

5. Enter the following information or choose from a list:

    - Repository type

    - Source repository

    - Branch

    - Root path

6. Click the arrow to the left of **Binary**.

7. Enter the following information:

    - Group

    - Artifact

    - Version

    - Packaging

8. Click **Create**.

7.3. ASSIGNING APPLICATION CREDENTIALS

You can assign credentials to one or more applications.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Click the **Analysis** tab.

3. Click the Options menu ⋮ to the right of **Analyze** and select **Manage credentials**.

4. Select one credential each from the **Source credentials** list and from the **Maven settings** list.

5. Click **Save**.

7.4. IMPORTING A LIST OF APPLICATIONS

You can import a .csv file containing a list of applications and their attributes to the Migration Toolkit for Applications (MTA) user interface.

NOTE

Importing a list of applications only adds applications, it does not overwrite any existing ones.

Procedure

1. Review the import file to ensure it contains all the required information in the required format.

2. In **Migration** view, click **Application Inventory**.

3. Click the Options menu ⋮ to the right of **Review**.

4. Click **Import**.

5. Browse to the desired file and click **Open**.

6. Optional: Select **Enable automatic creation of missing entities** By default, this option is selected.

7. Verify the import has completed and check the number of rows accepted or rejected.

8. Review the imported applications by clicking the arrow to the left of the checkbox.
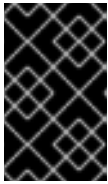
IMPORTANT

Rows accepted may not match the number of applications in the Application inventory list because some rows are dependencies. To verify, check the **Record Type** column of the CSV file for applications defined as **1** and dependencies as **2**.

7.5. DOWNLOADING A CSV TEMPLATE FOR IMPORTING APPLICATION LISTS

You can download a CSV template for importing application lists.

Procedure

1. In **Migration** view, click **Application inventory**.

2. Click the Options menu ⋮ to the right of **Review**.

3. Click **Manage imports** to open the **Application imports** page.

4. Click the Options menu ⋮ to the right of **Import** and then click **Download CSV template**.

7.6. CREATING MIGRATION WAVES

Creating a migration wave is a way to group applications that you want to migrate on a given schedule.

In addition, a migration wave enables you to track each migration by exporting a list of the wave's applications to the Jira issue management system. This automatically creates a separate Jira issue for each application of the migration wave.

Procedure

1. In **Migration** view, click **Migration waves**.

2. Click **Create new**.
   The **New migration wave** window opens.

3. Enter the following information or select from drop-down lists:

   - Name (optional; if not given, you can use the start and end dates to identify migration waves)

   - Potential start date; it must be later than the current date

   - Potential end date; it must be later than the start date

   - Stakeholders (optional)

   - Stakeholder groups (optional)

4. Click **Create**.
   The new migration wave appears in the list of existing migration waves.

5. To assign applications to a migration wave, click the Options menu (⋮) to the right of the migration wave and select **Manage applications** from the menu.
   The **Manage applications** window opens. The window displays the list of applications that are not assigned to any other migration wave.

6. Select the checkboxes of the applications that you want to assign to the migration wave and click **Save**.

   > **NOTE**
   >
   > The owner and the contributors of each application associated with the migration wave are automatically added to the migration wave's list of stakeholders.

7. To update a migration wave, select **Update** from its **Options** menu (three dots).
   The **Update migration wave** window opens.

7.7. CREATING JIRA ISSUES FOR A MIGRATION WAVE

You can use a migration wave for creating Jira issues automatically for each application assigned to the migration wave.

Procedure

1. In **Migration** view, click **Migration waves**.

2. Click the Options menu (⋮) to the right of the migration wave for which you want to create Jira issues and select **Export to Issue Manager**.
   The **Export to Issue Manager** window opens.

3. Select the instance type (Jira Cloud or Jira Server/Datacenter).

4. Select the instance, project and issue type from the lists.

5. Click **Export**.
   The status of the migration wave on the **Migration waves** page changes to **Issues Created**. To see the status of each individual application of a migration wave, click the **Status** column.

   A separate Jira issue is created for each application associated with the migration wave. The following fields of each issue are filled in automatically:

   - Title: **Migrate <application name>**

   - Reporter: Username of the token owner

   - Description: **Created by Konveyor**
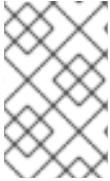
   > **NOTE**
   >
   > After you exported a migration wave to the Issue Manager and the Jira issues are created, you can no longer change them from within the MTA user interface. Even if you delete the migration wave, the Jira issues remain.

   > **NOTE**
   >
   > On the **Application inventory** page, you can see if any particular application is associated to a migration wave by opening the application's **Details** tab.
   >
   > You cannot delete an application if it is associated with a migration wave.

Revised on 2024-02-28 22:26:35 UTC