



Migration Toolkit for Applications 6.1

Release Notes

New features, known issues, and resolved issues

Migration Toolkit for Applications 6.1 Release Notes

New features, known issues, and resolved issues

Legal Notice

Copyright © 2023 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

Migration Toolkit for Applications 6.1 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. This document describes new features and improvements, known issues, and resolved issues for the Migration Toolkit for Applications, version 6.1.0.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	3
CHAPTER 1. INTRODUCTION	4
CHAPTER 2. MTA 6.1.4	5
2.1. RESOLVED ISSUES	5
CHAPTER 3. MTA 6.1.3	6
3.1. CONTAINER GRADE RELEASE	6
3.2. KNOWN ISSUES	6
CHAPTER 4. MTA 6.1.2	7
4.1. CONTAINER GRADE RELEASE	7
CHAPTER 5. MTA 6.1.1	8
5.1. NEW FEATURES AND IMPROVEMENTS	8
5.2. KNOWN ISSUES	8
5.3. RESOLVED ISSUES	8
CHAPTER 6. MTA 6.1.0	9
6.1. NEW FEATURES AND IMPROVEMENTS	9
6.2. KNOWN ISSUES	9
6.3. RESOLVED ISSUES	10

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

Migration Toolkit for Applications 6.1 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.

These release notes cover all z-stream releases of MTA 6.1 with the most recent release listed first.

CHAPTER 2. MTA 6.1.4

2.1. RESOLVED ISSUES

MTA version 6.1.4 has the following resolved issues.

CVE-2023-44487 HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack)

A flaw was found in the handling of multiplexed streams in the HTTP/2 protocol, which is utilized by Migration Toolkit for Applications (MTA). A client could repeatedly make a request for a new multiplex stream then immediately send an **RST_STREAM** frame to cancel those requests. This activity created additional workloads for the server in terms of setting up and dismantling streams, but avoided any server-side limitations on the maximum number of active streams per connection. As a result, a denial of service occurred due to server resource consumption.

The following issues have been listed under this issue:

- [MTA-1529](#)
- [MTA-1427](#)

For more details, see [CVE-2023-44487 \(Rapid Reset Attack\)](#).

CVE-2023-39325: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack in the Go language packages)

The HTTP/2 protocol is susceptible to a denial of service attack because request cancellation can reset multiple streams quickly. The server has to set up and tear down the streams while not hitting any server-side limit for the maximum number of active streams per connection. This results in a denial of service due to server resource consumption.

The following issues have been listed under this issue:

- [MTA-1429](#)
- [MTA-1447](#)
- [MTA-1482](#)

For more details, see [CVE-2023-39325 \(Rapid Reset Attack in the Go language packages\)](#).

CHAPTER 3. MTA 6.1.3

3.1. CONTAINER GRADE RELEASE

This release is a Container Grade Only (CGO) release.

3.2. KNOWN ISSUES

MTA version 6.1.3 has the following issues.

Application assessment: Save as draft does not function as expected

On the **Application assessment** form, **Save as draft** does not function as expected. [MTA-1207](#)

For a complete list of all known issues in this release, see the list of [Known Issues in Jira](#) .

CHAPTER 4. MTA 6.1.2

4.1. CONTAINER GRADE RELEASE

This release is a Container Grade Only (CGO) release.

CHAPTER 5. MTA 6.1.1

5.1. NEW FEATURES AND IMPROVEMENTS

At the time of release, there are no new features in this release.

5.2. KNOWN ISSUES

At the time of release, there are no known issues in this release.

5.3. RESOLVED ISSUES

At the time of the release, the following resolved issue has been identified as the major issue worth highlighting:

RHSSO

The release of MTA 6.1.1 resolves the issue that users experienced after the the release of version 7.6.3 of Red Hat Single Sign-On (RH-SSO), which rendered many new installations of MTA 6.x unusable. For more information on this issue, see [RHSSO-2514](#).

CHAPTER 6. MTA 6.1.0

6.1. NEW FEATURES AND IMPROVEMENTS

This section describes the new features and improvements of the Migration Toolkit for Applications (MTA) 6.1.0.

Creating custom migration targets

Administrators and architects can create and maintain custom migration targets and populate them with custom rules from a repository. Such custom migration targets are available for use by non-admin users. This simplifies the process of analysis configuration for applications with similar technologies that are common across the entire application portfolio of an organization.

Automated tagging of resources

MTA uses the technology stack information that the analysis module collects during an analysis to generate tags and to attach them automatically to applications.

Downloading HTML and CSV analysis reports

Users can download HTML and CSV reports generated by application analysis. By default, this option is disabled; it can be enabled in the new **General** menu in **Administration** view.

Reviewing an application without an assessment

Architects can review applications without running assessments first. By default, this option is disabled; it can be enabled in the new **General** menu in **Administration** view.

Support for disconnected installation

MTA fully supports disconnected installation in air-gapped OpenShift Container Platform environments.

Changes in naming

Some entities and menu entries of the MTA user interface have been renamed for clarity. The **Administrator** and **Developer** views have been renamed to **Administration** and **Migration**, respectively. **Tag Types** are now named **Tag Categories**.

6.2. KNOWN ISSUES

In this release, the following known issues have been identified.

CVE-2023-44487 HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack)

A flaw was found in the handling of multiplexed streams in the HTTP/2 protocol, which is utilized by Migration Toolkit for Applications (MTA). A client could repeatedly make a request for a new multiplex stream then immediately send an **RST_STREAM** frame to cancel those requests. This activity created additional workloads for the server in terms of setting up and dismantling streams, but avoided any server-side limitations on the maximum number of active streams per connection. As a result, a denial of service occurred due to server resource consumption.

The following issues have been listed under this issue:

- [MTA-1529](#)

- [MTA-1427](#)

To resolve this issue, upgrade to MTA 6.1.4.

For more details, see [CVE-2023-44487 \(Rapid Reset Attack\)](#)

CVE-2023-39325: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset Attack in the Go language packages)

The HTTP/2 protocol is susceptible to a denial of service attack because request cancellation can reset multiple streams quickly. The server has to set up and tear down the streams while not hitting any server-side limit for the maximum number of active streams per connection. This results in a denial of service due to server resource consumption.

The following issues have been listed under this issue:

- [MTA-1429](#)
- [MTA-1447](#)
- [MTA-1482](#)

To resolve this issue, upgrade to MTA 6.1.4.

For more information, see [CVE-2023-39325 \(Rapid Reset Attack in the Go language packages\)](#) .

Application analysis fails if the name of custom rules directory has spaces

During the configuration of an application analysis, if the user fetches custom rules from a repository using the CLI and the root path contains spaces, the CLI command is not properly composed and the analysis fails. The user must make sure that there are no spaces in the name of the directory from which custom rules are taken.

6.3. RESOLVED ISSUES

For a complete list of all issues resolved in this release, see the list of [MTA 6.1.0 resolved issues](#) in Jira.