Abstract

This document provides a high-level description of known issues and features in Red Hat Managed Integration 1.
Table of Contents

PREFACE ......................................................................................................................... 3
CHAPTER 1. VERSIONS OF COMPONENTS ..................................................................... 4
CHAPTER 2. FIXED ISSUES ............................................................................................. 5
CHAPTER 3. KNOWN ISSUES ........................................................................................ 6
CHAPTER 4. DEPRECATED FEATURES .......................................................................... 7
CHAPTER 5. NEW AND CHANGED FEATURES ............................................................. 8
These release notes list the components of Red Hat Managed Integration 1.7.0, as well as known and fixed issues in this release.

NOTE

When a Managed Integration patch or upgrade is available, you are notified and prompted to create an upgrade schedule. When prompted, see these Release Notes for details regarding changes to your cluster.
CHAPTER 1. VERSIONS OF COMPONENTS

Red Hat Managed Integration 1.7 includes the following software versions:

<table>
<thead>
<tr>
<th>Component</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Fuse Online</td>
<td>7.6</td>
</tr>
<tr>
<td></td>
<td>(Click Fuse Online Category)</td>
</tr>
<tr>
<td>Red Hat AMQ Online</td>
<td>1.4</td>
</tr>
<tr>
<td></td>
<td>(Click AMQ Online Category)</td>
</tr>
<tr>
<td>Red Hat 3scale API Management</td>
<td>2.8</td>
</tr>
<tr>
<td>Red Hat CodeReady Workspaces for OpenShift</td>
<td>2.0</td>
</tr>
<tr>
<td>Red Hat Single Sign-On</td>
<td>7.3</td>
</tr>
</tbody>
</table>
CHAPTER 2. FIXED ISSUES

The following issue is resolved in Red Hat Managed Integration 1.7.0:

* The address space messaging endpoint in Managed Integration supported TLS 1.0 and TLS 1.1, which are weak cipher suites. In this release, only TLS 1.2 is supported.
CHAPTER 3. KNOWN ISSUES

This section lists known issues with Red Hat Managed Integration 1.7.0:

- In the *Managing and protecting APIs using API management* Solution Pattern, users must have administrator privileges to create a product in 3scale. Administrator privileges are not required for other Solution Patterns.

- The *customer-admin* user cannot prevent any user with access to the Solution Explorer from changing the Solution Pattern subscription settings. Any user with access to the Solution Explorer can determine which Solution Patterns are available in a cluster.

- The following Solution Pattern is not available in this release:
  - *Low-code API development and SaaS integration*

  Ignore references to this Solution Pattern in the documentation.
CHAPTER 4. DEPRECATED FEATURES

- Support for TLS 1.0 and TLS 1.1 is removed from Red Hat Managed Integration. Only TLS 1.2 is supported in this release.
CHAPTER 5. NEW AND CHANGED FEATURES

- CodeReady Workspaces is upgraded to 2.0. Existing workspaces are not compatible with this version of CodeReady Workspaces. Red Hat recommends that you recreate any existing workspaces using CodeReady Workspaces 2.0.

- In AMQ Online, rejected messages are retried indefinitely instead of being sent to the Dead Letter Queue.

- In AMQ Online, you can sort addresses by message count.

- You can now configure AMQ Online. If you plan to use AMQ Online in Managed Integration, you need to create an AMQ Online configuration for production. You must edit and apply YAML files using the command line (CLI) tools to configure AMQ Online.

This section provides general guidance on configuring AMQ Online for production usage in Managed Integration.

Prerequisites

- You are logged in to OpenShift as the customer-admin user.

- You have experience with configuring AMQ Online.

Procedure

1. Configure AMQ Online in Managed Integration as described in Configuring AMQ Online.
   - The name of the AMQ Online project in your cluster is enmasse.
   - You must log in to the AMQ console as customer-admin.

2. Configure your address space to use an external authentication service as shown in the address space example using an external authentication service.

NOTE

The authentication services are configured by the AMQ Online service operator and are specified when creating an address space.