Red Hat OpenShift Application
Runtimes 1

RHOAR Eclipse Vert.x Release Notes

For use with Red Hat OpenShift Application Runtimes Eclipse Vert.x 3.8.1

Last Updated: 2019-09-27
Red Hat OpenShift Application Runtimes 1 RHOAR Eclipse Vert.x Release Notes

For use with Red Hat OpenShift Application Runtimes Eclipse Vert.x 3.8.1
Abstract

This Release Note contains important information related to Red Hat OpenShift Application Runtimes Eclipse Vert.x
Table of Contents

PREFACE .................................................................................................................. 3

CHAPTER 1. REQUIRED INFRASTRUCTURE COMPONENT VERSIONS ..................... 4

CHAPTER 2. SUPPORTED ECLIPSE VERT.X RUNTIME COMPONENT CONFIGURATIONS AND INTEGRATIONS ................................................................. 5

CHAPTER 3. FEATURES .................................................................................................. 6
  3.1. NEW AND CHANGED FEATURES .................................................................. 6
  3.2. DEPRECATED FEATURES .......................................................................... 6

CHAPTER 4. RELEASE COMPONENTS ........................................................................ 7
  4.1. SUPPORTED ARTIFACTS INTRODUCED IN THIS RELEASE ......................... 7
  4.2. TECHNOLOGY PREVIEW ARTIFACTS INTRODUCED IN THIS RELEASE ........ 7
  4.3. ARTIFACTS REMOVED IN THIS RELEASE .............................................. 7
  4.4. ARTIFACTS DEPRECATED IN THIS RELEASE .......................................... 7

CHAPTER 5. FIXED ISSUES .......................................................................................... 8

CHAPTER 6. KNOWN ISSUES ..................................................................................... 9
  6.1. VERT.X AMQP CLIENT: USING A DEPRECATED METHOD TO INITIALIZE AMQP_RECEIVER RESULTS IN MESSAGEHANDLER NOT LOGGING RECEIVED MESSAGES TO STANDARD OUTPUT ................................................ 9
  6.2. CONNECTION BETWEEN A RHÉL 8-BASED DATABASE APPLICATION AND A RHÉL 7-BASED MYSQL 5.7 DATABASE FAILS DUE TO TLS PROTOCOL VERSION MISMATCH .................... 10
  6.3. FALSE CONNECTION RESET BY PEER ERROR MESSAGES WHEN CALLING APPLICATION ENDPOINT ................................................................................................................. 10

CHAPTER 7. KNOWN ISSUES AFFECTING REQUIRED INFRASTRUCTURE COMPONENTS ................................................................. 11

CHAPTER 8. ADVISORIES RELATED TO THIS RELEASE ............................................ 13
PREFACE

Date of release: 2019-09-26
CHAPTER 1. REQUIRED INFRASTRUCTURE COMPONENT VERSIONS

The following versions of infrastructure components are required for all runtimes distributed as part of a RHOAR release. Red Hat does not provide support for components listed below, with the exception of components explicitly designated as supported.

<table>
<thead>
<tr>
<th>Component name</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maven</td>
<td>3.5.0</td>
</tr>
<tr>
<td>Fabric8 Maven Plugin</td>
<td>4.2.0</td>
</tr>
<tr>
<td>JDK[a][b]</td>
<td>OpenJDK 8, OpenJDK 11[c]</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 7[d]</td>
<td>7.7</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux 8[e]</td>
<td>8.0</td>
</tr>
<tr>
<td>OpenShift Container Platform (OCP)[f]</td>
<td>3.11, 4.1</td>
</tr>
<tr>
<td>Minishift</td>
<td>1.34.1 or later</td>
</tr>
<tr>
<td>CDK[g]</td>
<td>3.8.0</td>
</tr>
<tr>
<td>git</td>
<td>2.0 or later</td>
</tr>
<tr>
<td>oc command line tool</td>
<td>3.11 or later[h]</td>
</tr>
</tbody>
</table>

[a] A full JDK installation is required, as JRE does not provide tools for compiling Java applications from source.
[b] Red Hat OpenJDK is supported by Red Hat
[c] OpenJDK 9 is not supported by Red Hat.
[d] For deploying RHOAR-based applications on stand-alone RHEL in a production environment.
[e] For deploying RHOAR-based applications on stand-alone RHEL in a production environment.
[f] OCP is supported by Red Hat
[g] CDK is supported by Red Hat
[h] The version of the `oc` CLI tool should correspond to the version of OCP that you are using.
CHAPTER 2. SUPPORTED ECLIPSE VERT.X RUNTIME COMPONENT CONFIGURATIONS AND INTEGRATIONS

The following resource defines the supported configurations and integrations of Red Hat products with RHOAR Eclipse Vert.x:

- For a list of technologies that are supported for integration with RHOAR Eclipse Vert.x in production environments see the Supported Eclipse Vert.x configurations and integrations.

- For a list of RHOAR Eclipse Vert.x runtime artifacts and their versions see the Eclipse Vert.x 3.8.1 component details page.
CHAPTER 3. FEATURES

No new features or functionalities are introduced in this release.

3.1. NEW AND CHANGED FEATURES

3.2. DEPRECATED FEATURES

No features or functionalities are marked as deprecated in this release.
CHAPTER 4. RELEASE COMPONENTS

4.1. SUPPORTED ARTIFACTS INTRODUCED IN THIS RELEASE

The following artifact has been moved from Technology Preview to fully supported in this release:

- vertx-web-api-contract

4.2. TECHNOLOGY PREVIEW ARTIFACTS INTRODUCED IN THIS RELEASE

The following artifacts are provided as Technology Preview in this release.

- vertx-mail-client
- vertx-sql-client

NOTE

For more information about the support scope of Red Hat Technology Preview features, see Technology Preview Features Support Scope.

4.3. ARTIFACTS REMOVED IN THIS RELEASE

No artifacts are removed in this release.

4.4. ARTIFACTS DEPRECATED IN THIS RELEASE

No artifacts are marked as deprecated in this release.
CHAPTER 5. FIXED ISSUES

This RHOAR Eclipse Vert.x release incorporates all bugfixes from community release of versions 3.8.0 and 3.8.1. Issues resolved in the community releases are listed in the Eclipse Vert.x 3.8.0 Community Release Notes and the Eclipse Vert.x 3.8.1 Community Release Notes.
CHAPTER 6. KNOWN ISSUES

6.1. VERT.X AMQP CLIENT: USING A DEPRECATED METHOD TO INITIALIZE AMQP RECEIVER RESULTS IN MESSAGE HANDLER NOT LOGGING RECEIVED MESSAGES TO STANDARD OUTPUT

A Handler attached to an AmqpReceiver instance is set to print a message received from a sender on the same address to standard output. The Receiver receives the message, but the Handler fails to print it to standard output, even though the Handler is configured to do so.

Example

1. Initialize an AmqpReceiver instance using the following method provided by AmqpClient:

   ```java
   AmqpClient createReceiver(String address, AmqpReceiverOptions receiverOptions, Handler<AmqpMessage> messageHandler, Handler<AsyncResult<AmqpReceiver>> completionHandler);
   ```

   ```java
   AmqpClient client = AmqpClient.create(someClientOptions);
   client.createReceiver(address, 
       new AmqpReceiverOptions(),
       msg -> {
           System.out.println(msg.bodyAsString());
       },
       done -> {
           if(done.failed()){
               done.cause().printStackTrace();
           }
           System.out.println();
       });
   ```

2. Set the Handler on the AmqpReceiver instance to print received messages to standard output:

3. Create a Sender instance on the same address as the Receiver.

4. Set the Sender to send a message to the AmqpClient. The issue occurs regardless of whether you set the Sender to require an ACK from the Receiver when the Receiver receives the message.

5. Examine the log output of your application. The message sent by the Sender is expected to appear in the log output. The message does not appear in the log output.

Workaround

Initialize AmqpReceiver using the following method:

```java
AmqpClient createReceiver(String address, AmqpReceiverOptions receiverOptions, 
Handler<AsyncResult<AmqpReceiver>> completionHandler);
```
6.2. CONNECTION BETWEEN A RHEL 8-BASED DATABASE APPLICATION AND A RHEL 7-BASED MYSQL 5.7 DATABASE FAILS DUE TO TLS PROTOCOL VERSION MISMATCH

Description

Attempting to open a TLS-secured connection using OpenSSL between a database application container built on a RHEL 8-based OpenJDK builder image and a database container built on a RHEL 7-based MySQL 5.7 container image results in a connection failure due to a `javax.net.ssl.SSLHandshakeException` at runtime: For more detail, view the issue in JIRA.

```
Caused by: javax.net.ssl.SSLHandshakeException: No appropriate protocol (protocol is disabled or cipher suites are inappropriate)
```

Cause

The issue occurs due to a difference in the latest supported TLS protocol version between RHEL 7 and RHEL 8. The TLS implementation on RHEL 7 supports TLS protocol versions 1.0 (deprecated), 1.1, and 1.2. The TLS implementation on RHEL 8 also supports TLS protocol version 1.3, which is also the default TLS version used in RHEL 8-based builder images. This discrepancy may cause a TLS protocol version mismatch between application components while negotiating a TLS handshake, which in turn causes the connection between the application and database containers to fail.

Workaround

To prevent the issue described above, manually specify a TLS protocol version that is supported on both operating system versions in your database connection string. For example:

```
jdbc:mysql://testdb-mysql:3306/testdb?enabledTLSProtocols=TLSv1.2
```

6.3. FALSE CONNECTION RESET BY PEER ERROR MESSAGES WHEN CALLING APPLICATION ENDPOINT

Making an HTTP request on an endpoint of a Vert.x application using either curl or a Java HTTP client, produces the following error in the logs after each request:

```
io.vertx.core.net.impl.ConnectionBase
SEVERE: java.io.IOException: Connection reset by peer
```

This behavior is caused by the interaction of the Netty application framework and the HAPerxy load-balancer used by OpenShift. The error occurs due to existing HTTP connections being re-used by HAPerxy without closing. Even though the error message is logged, no error condition occurs. HTTP requests are handled correctly and the application responds as expected.
CHAPTER 7. KNOWN ISSUES AFFECTING REQUIRED INFRASTRUCTURE COMPONENTS

- **Fabric8 Maven Plugin Issue #1640**: Pushing an image into a custom repository during an s2i build with FMP 4.1.0 results in a `DuplicateKeyException`.

**Affected components and component versions**

This issue affects Fabric8 Maven Plugin 4.1.0.

**Description**

Fabric8 Maven Plugin does not process `ImageConfiguration` unless it also contains a `BuildImageConfiguration`. Without a recognizable `BuildImageConfiguration`, Fabric8 Maven Plugin repeatedly calls the s2i image generators to create another default `ImageConfiguration` that contains the expected `BuildImageConfiguration`. This results in more than one `ImageConfiguration` being specified for the given s2i build, which in turn results in a `DuplicateKeyException` when FMP attempts to push the image to the registry specified in the `pom.xml` configuration file. This leads to image build failures when a new image build is triggered by a change in the deployment configuration of a pod on OpenShift.

**Workaround**

To prevent Fabric8 Maven Plugin from generating a duplicate `ImageConfiguration`, place the image configuration inside a `build` section in the `pom.xml` configuration file of your project, as shown in the examples below. This in turn prevents the `DuplicateKeyException` when new image build is triggered by a change in the deployment configuration of the pod.

```xml
<configuration>
  <images>
    <image>
      <name>
        artifactrepository.somecompany.com:18444/demo-boot/demo-boot:1.0
      </name>
      <build>
        <from>
          fabric8/S2I_BASE_IMAGE_NAME
        </from>
        <assembly>
          <basedir>
            /deployments
          </basedir>
          <descriptorRef>
            artifact-with-dependencies
          </descriptorRef>
        </assembly>
        <env>
          <JAVA_LIB_DIR>
            /deployments
          </JAVA_LIB_DIR>
          <JAVA_MAIN_CLASS>
            org.example.class.name.Main
          </JAVA_MAIN_CLASS>
        </env>
        ...
      </build>
    </image>
    ...
  </images>
</configuration>
```
</images>
...
</configurtation>
CHAPTER 8. ADVISORIES RELATED TO THIS RELEASE

The following advisories have been issued to document enhancements, bugfixes, and CVE fixes included in this release.

- RHEA-2019:2879