Open Liberty 2021

Release Notes for Open Liberty 21.0.0.1 on Red Hat OpenShift Container Platform

Release Notes for Open Liberty 2021 on Red Hat OpenShift Container Platform

Last Updated: 2021-01-26

Open Liberty 2021 Release Notes for Open Liberty 21.0.0.1 on Red Hat OpenShift Container Platform

Release Notes for Open Liberty 2021 on Red Hat OpenShift Container Platform

Legal Notice

Abstract

These release notes contain the latest information about new features, enhancements, fixes, and issues contained in Open Liberty 2021 on Red Hat OpenShift Container Platform release.

Table of Contents

CHAPTER 1. FEATURES

With Open Liberty 21.0.0.1 you can now make use of the new **nbfOffset** attribute, allowing for "not-before" timed payloads via JWT Builder. Also included is new behaviour for HTTP redirects that permits the use of fully relative linking.

In Open Liberty 21.0.0.1:

- Scheduled payloads with JWT Builder
- Relative linking for HTTP Redirects
- Notable bugs fixed in this release

1.1. RUN YOUR APPS USING 21.0.0.1

If you're using Maven, here are the coordinates:

```
<dependency>
    <groupId>io.openliberty</groupId>
    <artifactId>openliberty-runtime</artifactId>
    <version>21.0.0.1</version>
    <type>zip</type>
</dependency>
```

Or for Gradle:

```
dependencies {
    libertyRuntime group: 'io.openliberty', name: 'openliberty-runtime', version: '[21.0.0.1,)'
}
```

Or if you're using Docker:

```
FROM open-liberty
```

1.1.1. Scheduled payloads with JWT Builder

New in Open Liberty 21.0.0.1, the **jwtBuilder** element has been enhanced with a new attribute called **nbfOffset** which can be used to configure an NBF claim for a JWT payload. The time set for the **nbfOffset** will be added to the current time and the result will determine when Json Web Tokens will start to be accepted for processing.

To configure the "not-before" claim using **jwtBuilder**, add the following to your **sever.xml** configuration file.

<jwtBuilder nbfOffset="1800s" />

If the JWT was issued at the current time, then the token can only be used after 1800 seconds have passed from the current time.

jwtBuilder is a part of the **jwt-1.0** feature, to add the feature to your project add the following to the **server.xml**:

```
<server>
```

```
  <featureManager>
    <feature>jwt-1.0</feature>
  </featureManager>
</server>
```

For more information:

- Open Liberty JWT Builder Documentation
- Building JSON Web Tokens in Liberty

1.2. RELATIVE LINKING FOR HTTP REDIRECTS

Included in Open Liberty 21.0.0.1 is an enhancement for the **servlet-4.0** feature, within Open Liberty the **sendRedirect()** is used to direct a client to a new page or location away from the original page. Previously, Open Liberty would always convert the provided relative URL in the **sendRedirect()** function to an absolute URL. This could lead to problems for applications that took advantage of reverse proxy servers.

To solve the problems presented, Open Liberty 21.0.0.1 has introduced a new **redirecttorelativeurl** web container property that will tell the application whether or not to construct absoulte URLs from relative redirect links. This property can be set in the **server.xml** file:

```
<server>
  ...
    <webContainer redirecttorelativeurl="true"/>
  ...
</server>
```

For more information:

- Open Liberty Servlet Documentation

1.3. NOTABLE BUGS FIXED IN THIS RELEASE

We've spent some time fixing bugs in 21.0.0.1, including the following issues:

- Improved recovery when core components are reinstalled at runtime
  An external contributor reported a flaw in Open Liberty's detection of changes to the JARs that compose the server implementation. When such changes were detected Liberty would force the JAR to be uninstalled and installed again. In most cases this allowed the runtime to recover and function properly. In specific cases, where some core component was re-installed, Liberty would not properly recover and it would result in some Java packages to be unavailable for class loading. For example, on Java 11 the package **javax.xml.soap** would become unavailable to the application class loaders.

  The most common environment where this occurred was running Open Liberty in OpenShift . This behavior has now been corrected for Open Liberty 21.0.0.1.

- OAuth user registry lookups may use incorrect custom cache key
  In previous releases, a flaw existed where a previously authenticated user's **Subject** might not be found in the authentication cache during an OAuth authentication flow, when using a custom user registry. The cache key used to retrieve user claims from the authentication cache was

based on the realm and username, but the correct cache key might be a combination of the OAuth provider name and the OAuth token object itself. The behavior has been corrected and the appropriate cache key should now be used.

For more information visit the Open Liberty Documentation .

- Add HTTP/2 IOException for misbehaving client error case
  It was previously possible for the HTTP/2 channel to throw a **NullPointerException** when it attempted to write out HTTP headers on a connection that had been terminated due to a connection error. Beginning in Open Liberty 21.0.0.1, the HTTP/2 channel will now throw a more informative **IOException** for this scenario. Read more about Open Liberty's support for HTTP/2.

- CONTAINER_NAME env variable is not reflected in logstashCollector-1.0
  Starting from Open Liberty 20.0.0.9, JSON logs created by the **logstashCollector-1.0** feature do not properly reflect the value set for the environment variable **CONTAINER_NAME**. The value set for **CONTAINER_NAME** should be reflected in the **serverName** field of the JSON logs, but the default server name from **wlp.server.name** is shown instead. This behaviour has been corrected for Open Liberty 21.0.0.1, visit the Logstash Collector Documentation for more information.

- Stop the ACME Certificate Checker Task when the server is stopping
  Support for the Automatic Certificate Management Environment (ACME) protocol was added in Open Liberty 20.0.0.10, enabling automatic fetching of browser-trusted TLS certificates from an ACME certificate authority. This release resolves a bug where the background task scheduled to check for expiring or revoked certification remains scheduled after the server enters quiesce phase. The task is now cancelled when the server is stopping. Read more about Open Liberty's support for the ACME protocol .

- Enable MyFaces 2.3.7 for Open Liberty
  The **jsf-2.3** feature in Open Liberty makes use of Apache MyFaces JavaServer Faces implementation. With the release of Apache MyFaces 2.3.7 a number of improvements and bug fixes have been made, for more information visit the Apache MyFaces 2.3.7 changelog.

- Dynacache initialization issue when ID is missing
  An external user discovered that the initialization of a **distributedMap** fails with a NullPointerException if the **id** element is not present in the **distributedMap** configuration. A clearer message should have been displayed to indicate the required **id** element is missing. To address this the **distributedMap** definition has been modified to mark the **id** element as required.

  The configuration runtime will now issue an error message:

  > CWWKG0058E: The element distributedMap with the unique identifier default-0 is missing the required attribute id.

  and the **distributedMap** will not be put into service. This new behaviour is introduced in Open Liberty 21.0.0.1.

CHAPTER 2. RESOLVED ISSUES

See the Open Liberty 21.0.0.1 issues that were resolved for this release .

CHAPTER 3. FIXED CVES

For a list of CVEs that were fixed in Open Liberty 21.0.0.1, see security vulnerabilities.

CHAPTER 4. KNOWN ISSUES

See the list of issues that were found but not fixed during the development of 21.0.0.1 .