Fault Management Foundation

Confidential, Draft
RFP-0034

5 Pages

Abstract

This is a proposal for adding support for performing fault management on an OSGi platform.

0 Document Information

0.1 Table of Contents

0.2 Status

This document suggests the following changes and extensions to the OSGi specification for the Open Services Gateway Initiative, and requests discussion. Distribution of this document is unlimited within OSGi.

1. Alternative to forced restart of all bundles when restarting the platform.

2. Addition of a bundle supervision service interface.

3. Optionally a new bundle management bundle with a run level concept.

0.3 Terminology and Document Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY" and "OPTIONAL" in this document are to be interpreted as described in [1].

`Source code is shown in this typeface.`

0.4 Revision History

The last named individual in this history is currently responsible for this document.

Revision	Date	Comments
1.00 A	Nov 15 2001	Initial.
1.00 B	Dec 21 2001	RFP number (34) assigned to the document. Copyright changed to OSGi.

1 Introduction

This is a proposal for adding support for performing fault management on an OSGi platform.

2 Motivation and Rationale

Fault handling support in the current OSGi specification is lacking. There is no standardized way of supervising bundles except for checking that the state of the bundle is "ACTIVE". A bundle may be marked as "ACTIVE" even though it is not functioning. This may be detected by an active bundle supervisor that periodically asks bundles for their internal state (OK or ERROR). It is then up to the bundle to check its internal state before responding.

When the framework is restarted, it always restores the state it had when it was stopped (crashed). I.e. the bad state is restored and it is likely that the problem (crash) re-occurs.

If something is wrong and a bundle crashes there are only two possibilities: restart the entire framework or restart the bundle. Traditional systems categorize services (bundles in OSGi terms) in a hierarchy enabling a fault manager to put the system in a safer state when a problem occurs. One such categorization is to use run levels like in traditional operating systems. Basic (trusted) services are placed on low run levels and (untrusted) user services on high run levels. When the fault manager decides to change run level, it should notify the system operator who may take an action to solve the problem.

3 Technical Discussion

3.1 Proposed Specification Change

Section 2.18.1 of the OSGi Release 2 specification reads:

> … A bundle's state is persistently recorded in the OSGi environment. When the Framework is restarted, all installed bundles previously recorded as being started must be started as described in the `Bundle.start` method. …

We would like to add an option that disables the forced restarting of all previously active bundles, and instead just starts one specified bundle (the bundle management bundle) that is responsible for starting bundles that are specified to be active. Those bundles may be the ones that were active before but must not be. The bundle management bundle may for example select to start a safe subset of the bundles.

3.2 Proposed Specification Addition

We would like to have a standardized way for bundles to express that they want to be supervised. A supervised bundle is one that gets periodically called by a supervising bundle like a fault manager.

This may be realized by specifying a service interface that a bundle that wants supervision publishes as an OSGi service. The interface needs one method with a boolean return value.

3.3 Benefits of this Proposal

These changes makes it possible to implement a bundle management bundle offering fault management functionality that uses a run level concept to keep track of the active bundles and their internal state.

It might be of interest to specify those management bundles and the run levels, but the proposed changes are enough to enable their implementation in a standardized way.

4 Security Considerations

The bundle management bundle will need admin permission.

5 Document Support

5.1 References

[1]. Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, RFC2119, March 1997.

5.2 Author's Address

Name	Gunnar Ekolin, Jan Sparud
Company	Gatespace AB
Address	Stora Badhusgatan 18-20 SE-411 21 Göteborg Sweden
Voice	+46 31 743 98 00
e-mail	{ekolin,sparud}@gatespace.com

5.3 Acronyms and Abbreviations

5.4 End of Document