

GT 4.2.0 WS MDS Trigger Service: System Administrator's Guide

DRAFT

GT 4.2.0 WS MDS Trigger Service: System Administrator's Guide

Introduction

This guide contains advanced configuration information for system administrators working with the WS MDS Trigger Service. It provides references to information on procedures typically performed by system administrators, including installation, configuring, deploying, and testing the installation.

This information is in addition to the basic Globus Toolkit prerequisite, overview, installation, security configuration instructions in [Installing GT 4.2.0](#) and [WS MDS System Administrator's Guide](#). Read through these guides before continuing!

DRAFT

Table of Contents

Trigger Service How-tos	5
1. Building and Installing	1
2. Configuring the Aggregator Framework	2
1. Configuration overview	2
2. Syntax of the interface	2
3. Additional configuration for the Trigger Service	4
1. Additional configuration for the Trigger Service	4
4. Deploying	5
1. Manually registering the Trigger Service	5
5. Testing	6
6. Security Considerations	7
1. WS MDS Aggregator Services (Index Service and Trigger Service) Security Considerations	7
7. Debugging	8
1. Logging in Java WS Core	8
8. Troubleshooting	10
1. No triggers displayed in mds-trigger-view	10
2. Trigger never fires	10
3. Error Messages	10
4. General troubleshooting information	10
Glossary	12
Index	13

List of Tables

8.1. WS MDS Trigger Service Error Messages 10

DRAFT

Trigger Service How-tos

C

configuration interface,
aggregator sinks,
aggregator sources,
disable publishing,
overview,
Trigger Service-specific,
configuring,
aggregator sinks,
aggregator sources,
disabling publishing,
overview,
Trigger Service-specific,

D

debugging
logging,
deploying,

E

errors,

L

logging
CEDPS-compliant,
debugging,

S

security considerations,

T

testing,
troubleshooting,

Chapter 1. Building and Installing

The Trigger Service is installed as part of the standard Globus Toolkit installation.

DRAFT

Chapter 2. Configuring the Aggregator Framework

WS MDS aggregator services (such as MDS Index, MDS Trigger and MDS Archive Tech Preview) inherit their configuration system from the *Aggregator Framework* module.

The Aggregator Framework does not have its own service -side configuration, although services which are based on the framework have their own service-side configuration options (such as *MDS Index* and *MDS Trigger*) which are documented in the per-service documentation.

Registrations to a working Aggregator Framework are configured for the `mds-servicegroup-add(1)` tool. This tool takes an XML configuration file listing registrations, and causes those registrations to be made.

In general, configuration of aggregator services involves configuring the service to get information from one or more sources in a Grid. The mechanism for doing this is defined by (inherited from) the Aggregator Framework and described in this section.

1. Configuration overview

Configuring an Aggregating Service Group to perform a data aggregation is performed by specifying an AggregatorContent object as the content parameter of a ServiceGroup `add` method invocation. An AggregatorContent object is composed of two `xsd:any` arrays: AggregatorConfig and AggregatorData:

- The AggregatorConfig `xsd:any` array is used to specify parameters that are to be passed to the underlying AggregatorSource when the ServiceGroup`add` method is invoked. These parameters are generally type-specific to the implementation of the AggregatorSource and/or AggregatorSink being used.
- The AggregatorData `xsd:any` array is used as the storage location for aggregated data that is the result of message deliveries to the AggregatorSink. Generally, the AggregatorData parameter of the AggregatorContent is not populated when the ServiceGroup `add` method is invoked, but rather is populated by message delivery from the AggregatorSource.

2. Syntax of the interface

2.1. Configuring the Aggregator Sources

For detailed information on configuring the three types of aggregator sources provided by the Globus Toolkit, see [Aggregator Sources Reference](#).

- [Chapter 6, Configuring Execution Aggregator Source](#)
- [Chapter 4, Configuration file: parameters for the query aggregator source](#)
- [Chapter 5, Configuration file: parameters for the subscription aggregator source](#)

2.2. Configuring the Aggregator Sink

An aggregator sink may require sink-specific configuration (for example, the MDS *Trigger Service* requires sink-specific configuration; the MDS *Index Service* does not). See the documentation for the specific *aggregator service* being used for details on sink-specific documentation.

2.2.1. Disabling the publishing of the aggregator configuration on the server side

It is now possible to disable the publishing of the aggregator configuration along with the aggregated data. The following optional parameter can be added to the *AggregatorConfiguration* section of the service `jndi-config.xml` file:

```
<parameter>
  <name>publishAggregatorConfiguration</name>
  <value>>false</value> </parameter>
```

By default, this option is disabled and the aggregator configuration information is published.

DRAFT

Chapter 3. Additional configuration for the Trigger Service

1. Additional configuration for the Trigger Service

The set of possible actions (programs) that can be executed by the Trigger Service is specified in the file `$GLOBUS_LOCATION/etc/globus_wsrft_mds_trigger/jndi-config.xml`. The `executableMappings` parameter contains a comma-separated list of name=value pairs. The left hand side of each name/value pair is the name assigned to the trigger action; this name can be used in trigger definitions. The right hand side of each name/value pair is the path name (relative to `$GLOBUS_LOCATION/libexec/trigger` of the file to execute).

The sources of information used by the Trigger Service are configured using the `mds-servicegroup-add` command; see the [Aggregator Framework](#) documentation or the [Trigger Service Easy HOWTO](#) for more details and examples.

Triggers themselves are created using the [command line clients](#).

Chapter 4. Deploying

This component is deployed as part of the standard toolkit installation. By default, there are no trigger actions set to fire on container startup, as these must be configured and registered manually.

1. Manually registering the Trigger Service

To manually register the example described in [Chapter 2. Configuring the Aggregator Framework](#) (above) do the following:

1. At this point, we're ready to make a registration with the `TriggerRegistrationService` by running a command similar to the following:

```
$GLOBUS_LOCATION/bin/mds-servicegroup-add \  
    $GLOBUS_LOCATION/etc/globus_wsrp_mds_trigger/trigger-registration-example.xml
```

You should see output similar to the following if your environment has been configured properly:

```
Processing configuration file...  
INFO: Processed 1 registration entries  
INFO: Successfully registered https://127.0.0.1:8443/wsrp/services/DefaultIndexService \  
to servicegroup at https://127.0.0.1:8443/wsrp/services/TriggerRegistrationService
```

Chapter 5. Testing

To determine if the registration was made properly, you can query the TriggerRegistrationService using a tool like `$GLOBUS_LOCATION/bin/wsrf-query` and visually inspect the output.

For example, running:

```
$GLOBUS_LOCATION/bin/wsrf-query -s \  
    https://127.0.0.1:8443/wsrf/services/TriggerRegistrationService "/*"
```

should yield output similar to the following for the example above:

...

```
<ns1:Content xsi:type="ns11:AggregatorContent" xmlns:ns11="http://mds.globus.org/aggrega  
<ns11:AggregatorConfig>  
  <agg:GetResourcePropertyPollType xmlns:agg="http://mds.globus.org/aggregator/types" xm  
  <agg:PollIntervalMillis>30000</agg:PollIntervalMillis>  
  <agg:ResourcePropertyName>wssg:Entry</agg:ResourcePropertyName>  
</agg:GetResourcePropertyPollType>  
</ns11:AggregatorConfig>  
<ns11:AggregatorData/>  
</ns1:Content>
```

...

Chapter 6. Security Considerations

The security considerations for the [Aggregator Framework](#) also apply to the Trigger Service:

1. WS MDS Aggregator Services (Index Service and Trigger Service) Security Considerations

By default, the *aggregator sources* do not use authentication credentials -- they retrieve information using anonymous SSL authentication or no authentication at all, and thus retrieve only publicly-available information. If a user or administrator changes that configuration so that a service's aggregator source uses credentials to acquire non-privileged data, then that user or administrator must configure the service's aggregator sink to limit access to authorized users.

DRAFT

Chapter 7. Debugging

Because WS MDS is built on Java WS Core, it uses the same sys admin logging, described below:

1. Logging in Java WS Core

The following information applies to Java WS Core and all services built on Java WS Core.

Java WS Core server side has two types of loggers. One logger is used for development logging and by default writes to standard out. The other logger includes system administration information and is [CEDPs best practices](#)¹ compliant.

On client side, only developer logging is available and is configured using `log4j.properties`.

1.1. Development Logging in Java WS Core

The following information applies to Java WS Core and those services built on it.

Logging in the Java WS Core is based on the [Jakarta Commons Logging](#)² API. Commons Logging provides a consistent interface for instrumenting source code while at the same time allowing the user to plug-in a different logging implementation. Currently we use [Log4j](#)³ as a logging implementation. Log4j uses a separate configuration file to configure itself. Please see Log4j documentation for details on the [configuration file format](#)⁴.

1.1.1. Configuring server side developer logs

Server side logging can be configured in `$GLOBUS_LOCATION/container-log4j.properties`, when the container is stand alone container. For tomcat level logging, refer to [Logging for Tomcat](#)⁵. The logger `log4j.appender.A1` is used for developer logging and by default writes output to the system output. By default it is set for all warnings in the Globus Toolkit package to be displayed.

Additional logging can be enabled for a package by adding a new line to the configuration file. Example:

```
#for debug level logging from org.globus.package.FooClass
log4j.category.org.globus.package.name.FooClass=DEBUG
#for warnings from org.some.warn.package
log4j.category.org.some.warn.package=WARN
```

1.1.2. Configuring client side developer logs

Client side logging can be configured in `$GLOBUS_LOCATION/log4j.properties`. The logger `log4j.appender.A1` is used for developer logging and by default writes output to the system output. By default it is set for all warnings in the Globus Toolkit package to be displayed.

¹ <http://cedps.net/index.php/LoggingBestPractices>

² <http://jakarta.apache.org/commons/logging/>

³ <http://logging.apache.org/log4j/>

⁴ [http://logging.apache.org/log4j/docs/api/org/apache/log4j/PropertyConfigurator.html#doConfigure\(java.lang.String,org.apache.log4j.spi.LoggerRepository\)](http://logging.apache.org/log4j/docs/api/org/apache/log4j/PropertyConfigurator.html#doConfigure(java.lang.String,org.apache.log4j.spi.LoggerRepository))

⁵ <http://tomcat.apache.org/tomcat-5.5-doc/logging.html>

1.2. Configuring system administration logs

The specific logger to edit will be `log4j.logger.sysadmin` in `$GLOBUS_LOCATION/container-log4j.properties`. There you can configure the following properties:

```
log4j.appender.infoCategory=org.apache.log4j.RollingFileAppender
log4j.appender.infoCategory.Threshold=INFO
log4j.appender.infoCategory.File=var/containerLog
log4j.appender.infoCategory.MaxFileSize=10MB
log4j.appender.infoCategory.MaxBackupIndex=2
```

Above implies the logging file is rolling with each file size limited to 10MB and the logging information is stored in `$GLOBUS_LOCATION/var/containerLog`.

1.3. Sample log file

The [sample log file](#)⁶ contains many log entries for various scenarios in the Java WS container.

⁶ <http://www.globus.org/toolkit/docs/4.2/4.2.0/common/javawscore/sample-container-log.txt>

Chapter 8. Troubleshooting

For a list of common errors in GT, see [Error Codes](#).

1. No triggers displayed in mds-trigger-view

I created a trigger using the `mds-trigger-create`, but I don't see any triggers when I type `mds-trigger-view`! Where are the triggers? Why is nothing happening?

Did you set up a trigger registration? (See the Trigger Service [Admin Guide](#)) The trigger has been created (unless there was an error), but you will not see it and you cannot access it if the trigger registration has not been set up.

2. Trigger never fires

I'm sure the registration was made properly, but the trigger script never fires. OR I followed all of the above steps, but where are the triggers? Why is nothing happening?

Once you've completed the trigger registration, you can now create individual triggers. Trigger creation is performed using a client. See the [User's Guide](#) for more information on clients.

3. Error Messages

Table 8.1. WS MDS Trigger Service Error Messages

Error Code	Definition	Possible Solutions
Error ; nested exception is: org.apache.commons.httpclient.NoHttpResponseException: The server xxx.x.x.x failed to respond	Happens when trying to create a trigger for the Trigger Service. The above error is accompanied by the following error in container: [JWSCORE-192] Error processing request java.io.IOException: Token length 1347375956 > 33554432. FIXME - what causes this?	Be sure that you have properly edited the <code>client-config-settings</code> file under <code>globus_wsrf_mds_trigger</code> . The <code>DefaultServiceAddress</code> parameter should properly reflect the service prefix from your container, e.g.: <code>https://127.0.0.1:8444/wsrf/services/</code> . The services you wish to monitor should also be consistent.
WS MDS is built on Java WS Core, please see Java WS Core Error Codes for more error code documentation.		

4. General troubleshooting information

- In general, if you want to investigate a problem on your own please see [Chapter 10. Debugging](#) for details on how to turn on debugging.
- Most of the command line clients have a `-debug` option that will display more detailed error messages, including the error stack traces.

- Search the mailing lists¹ such as gt-user@globus.org² or jwscore-user@globus.org³ (before posting a message).
- If you think you have found a bug please report it in our Bugzilla⁴ system. Please include as much as detail about the problem as possible.

DRAFT

¹ <http://www.globus.org/email-archive-search.php>

² <mailto:gt-user@globus.org>

³ <mailto:jwscore-user@globus.org>

⁴ <http://bugzilla.globus.org/bugzilla/>

Glossary

A

Aggregator Framework	A software framework used to build services that collect and aggregate data. WS MDS Services (such as the Index and Trigger services) are built on the Aggregator Framework, and are sometimes called Aggregator Services.
aggregator services	Services that are built on the Aggregator Framework, such as the WS MDS Index Service and Trigger Service.
aggregator source	A Java class that implements an interface (defined as part of the Aggregator Framework) to collect XML-formatted data. WS MDS contains three aggregator sources: the query aggregator source, the subscription aggregator source, and the execution aggregator source.

I

Index Service	An aggregator service in WS MDS that serves as a registry similar to UDDI, but much more flexible. Indexes collect information and publish that information as WSRF resource properties.
---------------	--

T

Trigger Service	An aggregator service (in WS MDS) that collects information and compares that data against a set of conditions defined in a configuration file. When a condition is met, or triggered, the specified action takes place (for example, an email is sent to a system administrator when the disk space on a server reaches a threshold).
-----------------	--

Index

C

- configuration interface, 2
 - aggregator sinks, 2
 - aggregator sources, 2
 - disable publishing, 3
 - overview, 2
 - Trigger Service-specific, 4
- configuring, 2
 - aggregator sinks, 2
 - aggregator sources, 2
 - disabling publishing, 3
 - overview, 2
 - Trigger Service-specific, 4

D

- debugging
 - logging, 8
- deploying, 5

E

- errors, 10

L

- logging
 - CEDPS-compliant, 8
 - debugging, 8

S

- security considerations, 7

T

- testing, 6
- troubleshooting, 10