

# Cert Check Information Provider

DRAFT

## Cert Check Information Provider

### Abstract

This provider will monitor the life of a remote certificate. It connects to an SSL TCP listener and obtains the certificate from it. It then checks the certificate for subject, start date, end data, and email address. All of this information is put in the Index Service if it is successfully obtained. This provider is an execution aggregator provider. These providers are quite useful as is and additionally serve as an example of how to create others. The perl script and configuration file can be modified to the user's liking once installed. This provider has a perl script and an XML configuration file. The perl script is used to obtain information and format the information into XML output. The output is written to stdout, where it is gathered and put into the Index Service. The XML file is of a common format that is explained [here](#). After installing the package, the XML configuration files will be copied to `$GLOBUS_LOCATION/etc/globus_ws-rf_mds_index/default_providers/` where the `DefaultIndexService` will find them and use them to register the provider.

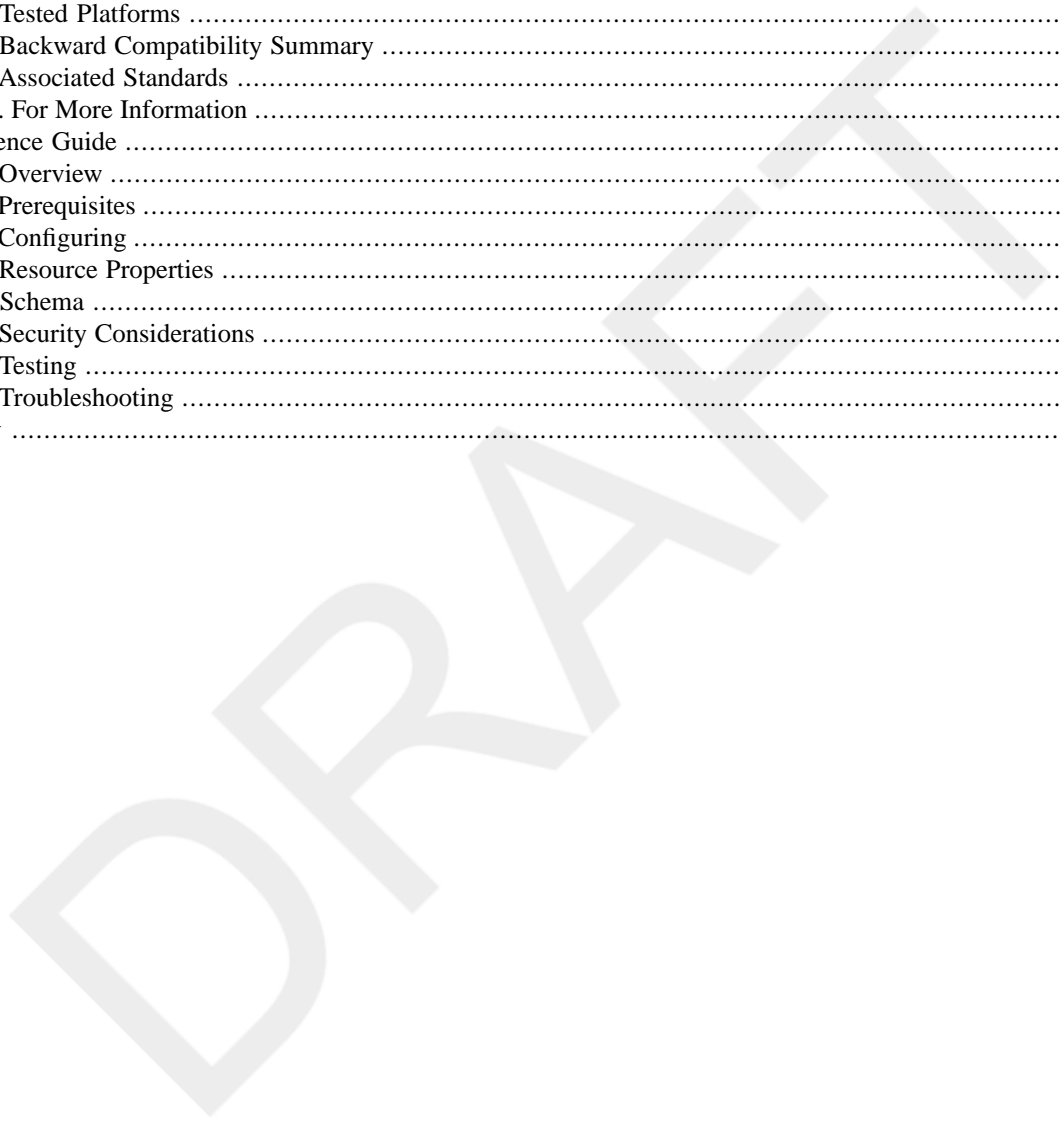
You can download a PDF version of Cert Check Information Provider information [here](#)<sup>1</sup>.

---

<sup>1</sup> cert\_check.pdf

# Table of Contents

- 1. Release Notes ..... 1
  - 1. Component Overview ..... 1
  - 2. Feature Summary ..... 1
  - 3. Changes Summary ..... 1
  - 4. Bug Fixes ..... 1
  - 5. Known Problems ..... 1
  - 6. Technology Dependencies ..... 1
  - 7. Tested Platforms ..... 2
  - 8. Backward Compatibility Summary ..... 2
  - 9. Associated Standards ..... 2
  - 10. For More Information ..... 2
- 2. Reference Guide ..... 3
  - 1. Overview ..... 3
  - 2. Prerequisites ..... 3
  - 3. Configuring ..... 3
  - 4. Resource Properties ..... 4
  - 5. Schema ..... 4
  - 6. Security Considerations ..... 4
  - 7. Testing ..... 4
  - 8. Troubleshooting ..... 5
- Glossary ..... 6



# Chapter 1. GT 4.2.0 Release Notes: Cert Check Info Information Provider

## 1. Component Overview

This provider will monitor the life of a remote certificate. It connects to an SSL TCP listener and obtains the certificate from it. It then checks the certificate for subject, start date, end data, and email address. All of this information is put in the Index Service if it is successfully obtained. This provider is an execution aggregator provider. These providers are quite useful as is and additionally serve as an example of how to create others. The perl script and configuration file can be modified to the user's liking once installed. This provider has a perl script and an XML configuration file. The perl script is used to obtain information and format the information into XML output. The output is written to stdout, where it is gathered and put into the Index Service. The XML file is of a common format that is explained [here](#). After installing the package, the XML configuration files will be copied to `$GLOBUS_LOCATION/etc/globus_ws-rf_mds_index/default_providers/` where the `DefaultIndexService` will find them and use them to register the provider.

## 2. Feature Summary

Features new in release 4.2.0:

- This provider monitors the life of a remote certificate.

## 3. Changes Summary

This is a new information provider for GT 4.2.0.

## 4. Bug Fixes

There are no fixed bugs for this information provider.

## 5. Known Problems

- There are currently no bugs for this information provider.

## 6. Technology Dependencies

This information provider depends on the following GT components:

- [Java WS Core](#)

This information provider depends on the following 3rd party software:

- A working Perl installation

## 7. Tested Platforms

Tested Platforms for this information provider:

- N/A

Tested containers for this information provider

- Java WS Core container

## 8. Backward Compatibility Summary

This is a new information provider with this version.

## 9. Associated Standards

Associated standards for this Information Provider:

- N/A

## 10. For More Information

See [Chapter 2, GT 4.2.0: Cert Check Information Provider Reference](#) for more information about this information provider.

# Chapter 2. GT 4.2.0: Cert Check Information Provider Reference

## 1. Overview

This provider will monitor the life of a remote certificate. It connects to an SSL TCP listener and obtains the certificate from it. It then checks the certificate for subject, start date, end data, and email address. All of this information is put in the Index Service if it is successfully obtained. This provider is an execution aggregator provider. These providers are quite useful as is and additionally serve as an example of how to create others. The perl script and configuration file can be modified to the user's liking once installed. This provider has a perl script and an XML configuration file. The perl script is used to obtain information and format the information into XML output. The output is written to stdout, where it is gathered and put into the Index Service. The XML file is of a common format that is explained [here](#). After installing the package, the XML configuration files will be copied to `$GLOBUS_LOCATION/etc/globus_wsrf_mds_index/default_providers/` where the `DefaultIndexService` will find them and use them to register the provider.

This is an execution aggregator source-based information provider.

## 2. Prerequisites

1. A working Perl installation

## 3. Configuring

The following configuration is required for this information provider:

1. In order to grant permission to the installed perl scripts the user must edit the file: `$GLOBUS_LOCATION/etc/globus_wsrf_mds_index/jndi-config.xml` such that the tags:

```
<parameter>
  <name>executableMappings</name>
  <value>
    aggr-test=aggregator-exec-test.sh, pingexec=example-ping-exec
  </value>
</parameter>
```

includes the new provider. For example:

```
<parameter>
  <name>executableMappings</name>
  <value>
    cert-info=cert-check.pl
  </value>
</parameter>
```

2. This provider will monitor the life of a remote certificate. It connects to an ssl TCP listener and obtains the certificate from it. It then checks the cert for subject, start date, end data, and email address. All of this information is put in the index if it is successfully obtained. To change what server is monitored edit the file:

GLOBUS\_LOCATION/etc/globus\_wsrf\_mds\_index/default\_providers/cert-info-reg.xml

and change the line:

```
<RegistrantEPR
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/03/addressing"
  xmlns:agg="http://mds.globus.org/aggregator/types">
  <wsa:Address>https://www.SITE.COM:8443</wsa:Address>
</RegistrantEPR>
```

from "https://www.SITE.COM:8443" to the ssl server of your choice.

## 4. Resource Properties

- Data appears as part of the ServiceGroupEntry RP

### 4.1. Namespace URI

TODO: Include the Namespace URI, or provide a link to the Java API Documentation, which is required to construct the QName for the subscription to the Topic.

## 5. Schema

- N/A

## 6. Security Considerations

General security considerations associated with the container and all MDS services apply. See: [Aggregator Framework](#).

### 6.1. 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.

## 7. Testing

N/A

## 8. Troubleshooting

N/A

DRAFT

# Glossary

## A

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.

DRAFT