GridShibForGTInstall

GridShib for Globus Toolkit Installation

A lightweight alternative to installing the full Globus Toolkit is to only install the Java WS Core component of GT4, and then install GridShib for GT on top of that. In fact, this is the only option under Windows, which does not support the full Globus Toolkit. So the following "Quick Start" guide shows how to layer GridShib for GT on top of Java WS Core on Windows.

This tutorial gives detailed instructions for installing, configuring, and using Java WS Core 4.0.4, GridShib for GT v0.6.0, and GridShib SAML Tools v0.1.4 on Windows. Software requirements include JDK 1.4.2 (or higher) and Ant 1.6 (or higher), which we assume are already installed on Windows.

1. Install the binary version of Java WS Core 4.0.4 on Windows.

   > *The binary version of Java WS Core is simplest, but the source version works just as well.*

   a. Extract the ZIP archive to any folder on your hard drive (say, c:\globus).
   b. Open a Command Prompt window, change directory to the installation directory, and set the `GLOBUS_LOCATION` environment variable (which is *case sensitive*, even on Windows in this case):

   ```
   > cd c:\globus\ws-core-4.0.4-bin\ws-core-4.0.4
   > set GLOBUS_LOCATION=%CD%
   > echo %GLOBUS_LOCATION%
   ```

   c. For debugging purposes, add the following line to %GLOBUS_LOCATION%\container-log4j.properties:
   `log4j.category.org.globus.gridshib.gt=DEBUG`

   d. As a crude test, start the container (with transport-level security disabled):

   ```
   > bin\globus-start-container -nosec
   Starting SOAP server at: http://141.142.251.212:8080/wsrf/services/
   With the following services:

   [1]: http://141.142.251.212:8080/wsrf/services/AdminService
   [2]: http://141.142.251.212:8080/wsrf/services/AuthzCalloutTestService
   [3]: http://141.142.251.212:8080/wsrf/services/ContainerRegistryEntryService
   [4]: http://141.142.251.212:8080/wsrf/services/ContainerRegistryService
   [5]: http://141.142.251.212:8080/wsrf/services/CounterService
   [6]: http://141.142.251.212:8080/wsrf/services/ManagementService
   [7]: http://141.142.251.212:8080/wsrf/services/NotificationConsumerFactoryService
   [8]: http://141.142.251.212:8080/wsrf/services/NotificationConsumerService
   [9]: http://141.142.251.212:8080/wsrf/services/NotificationTestService
   [10]: http://141.142.251.212:8080/wsrf/services/PersistenceTestSubscriptionManager
   [11]: http://141.142.251.212:8080/wsrf/services/SampleAuthzService
   [12]: http://141.142.251.212:8080/wsrf/services/SecureCounterService
   [13]: http://141.142.251.212:8080/wsrf/services/SecurityTestService
   [14]: http://141.142.251.212:8080/wsrf/services/ShutdownService
   [15]: http://141.142.251.212:8080/wsrf/services/SubscriptionManagerService
   [16]: http://141.142.251.212:8080/wsrf/services/TestAuthzService
   [17]: http://141.142.251.212:8080/wsrf/services/TestRPCService
   [18]: http://141.142.251.212:8080/wsrf/services/TestService
   [19]: http://141.142.251.212:8080/wsrf/services/TestServiceRequest
   [20]: http://141.142.251.212:8080/wsrf/services/TestServiceWrongWSDL
   [21]: http://141.142.251.212:8080/wsrf/services/Version
   [22]: http://141.142.251.212:8080/wsrf/services/WidgetNotificationService
   [23]: http://141.142.251.212:8080/wsrf/services/WidgetService
   [24]: http://141.142.251.212:8080/wsrf/services/gsi/AuthenticationService
   ```

   Press Ctrl-C to abort the container.
2. Install a trusted certificate

   > *In what follows, we will use a GridShib CA-issued end-entity certificate (EEC) to authenticate to GT services. We will also issue proxy certificates using a GridShib CA-issued EEC. Thus the container needs to be configured to trust certificates issued by the GridShib CA.*

   a. Download the public certificate of the GridShib CA.
   b. Extract the ZIP archive to folder "%USERPROFILE%\.globus\certificates":

   ```
   > dir "%USERPROFILE%\.globus\certificates"
   ...
   02/19/2007  10:15 PM             1,667 bfcd1f28.0
   02/19/2007  10:15 PM               239 bfcd1f28.signing_policy
   ```

3. Obtain a user certificate and stop the container normally.
   a. In the previous Command Prompt window, start the container again:

   ```
   > echo %GLOBUS_LOCATION%
   > bin\globus-start-container -nosec
   Starting SOAP server at: http://141.142.251.212:8080/wsrf/services/
   With the following services...
   ```

b. Open another Command Prompt window and try to stop the container:
   ```
   > cd c:\globus\ws-core-4.0.4-bin\ws-core-4.0.4
   > set GLOBUS_LOCATION=%CD%
   > echo %GLOBUS_LOCATION%
   > bin\globus-stop-container
   Error: ; nested exception is:
   GSSException: Defective credential detected [Caused by:
   Proxy file (C:\DOCUME~1\TOMSCA~1\LOCALS~1\Temp\x509up_u_tom scavo) not found.]
   ```
c. Press Ctrl-C to abort the container.
d. Obtain a short-term X.509 end-entity credential from the online GridShib CA.
e. In the first Command Prompt window, start the container as before.
f. In the second Command Prompt window, try to stop the container again:
   ```
   > bin\globus-stop-container
   Error: ; nested exception is:
   java.net.ConnectException: Connection refused: connect
   ```
g. Finally, stop the container normally, authenticating with your GridShib CA-issued credential via Secure Message:
   ```
   > bin\globus-stop-container -s http://localhost:8080/wsrf/services/ShutdownService -m msg
   ```

4. Start and stop a secure container.

   > *For the rest of this tutorial, we require a secure container.*

   a. In the first Command Prompt window, start the container:
   ```
   > echo %GLOBUS_LOCATION%
   > bin\globus-start-container
   Starting SOAP server at: https://141.142.250.163:8443/wsrf/services/
   With the following services...
   ```
   b. In the second Command Prompt window, stop the container:
   ```
   > echo %GLOBUS_LOCATION%
   > bin\globus-stop-container
   ```

5. Request the `SecureCounterService`, authenticating with your EEC via Secure Conversation.
   a. In the first Command Prompt window, start the container:
   ```
   > echo %GLOBUS_LOCATION%
   > bin\globus-start-container
   Starting SOAP server at: https://141.142.250.163:8443/wsrf/services/
   With the following services...
   ```
   b. In the second Command Prompt window, request a service:
   ```
   > echo %GLOBUS_LOCATION%
   > bin\counter-client -m conv -z none
       -s https://localhost:8443/wsrf/services/SecureCounterService
   Got notification with value: 3
   Counter has value: 3
   Got notification with value: 13
   ```
   c. In the second Command Prompt window, stop the container:
   ```
   > bin\globus-stop-container
   ```

6. Install GridShib for GT v0.6.0 on Windows.
   a. Download the GS4GT v0.6.0 source distribution (ZIP archive) from the GridShib web site. (A GZIP archive is also available for UNIX users.)
   b. Double-click the ZIP archive and extract the source files into a folder of your choice (say, c:\gridshib).
   c. In the second Command Prompt window, type the following commands:
   ```
   > cd c:\gridshib\gridshib-gt-0_6_0-src\gridshib-gt-0_6_0
   > echo %GLOBUS_LOCATION%
   > ant deploy
   > ant deploy-echoservice
   ```

7. Request the `ShibEchoService`, authenticating with your EEC.

   > *Note: An EEC obtained from the GridShib CA contains a bound SAML assertion with no attributes. Thus you will see one "attribute" in the logs, namely, the value of the `NameIdentifier` element of the assertion.*

   a. In the first Command Prompt window, start the container:
   ```
   > echo %GLOBUS_LOCATION%
   > bin\globus-start-container
   Starting SOAP server at: https://141.142.250.163:8443/wsrf/services/
   With the following services...
   ```
   b. In the second Command Prompt window, copy your EEC to a preconfigured location and request the service:
   ```
   > %GLOBUS_LOCATION%\bin\shibecho -d -z none
       -s https://localhost:8443/wsrf/services/ShibEchoService
   ```
   You should receive one attribute in the response.
   c. In the second Command Prompt window, stop the container.
8. Install GridShib SAML Tools v0.1.4 on Windows. (See the Installation Notes for detailed information about GridShib SAML Tools.)

> *Note: We will configure the SAML Tools to sign proxy certificates using your GridShib CA-issued EEC by default.*

   a. Download the GridShib SAML Tools v0.1.4 source distribution (ZIP archive) from the GridShib web site. (A GZIP archive is also available for UNIX users.)
   b. Double-click the ZIP archive and extract the source files into a folder of your choice (say, c:\gridshib).
   c. In a third Command Prompt window, type the following commands:

```
> cd c:\gridshib\gridshib-saml-tools-0_1_4
> set GRIDSHIB_HOME=%CD%
> ant install
```

   d. Uncomment the following lines in %GRIDSHIB_HOME%\etc\gridshib\tools\gridshib-saml-issuer.properties:

```
# an EEC issued by the GridShib CA
certLocation=file:/%TEMP%/x509up_u_%USERNAME%
keyLocation=file:/%TEMP%/x509up_u_%USERNAME%
```

   Replace the placeholders `%TEMP%` and `%USERNAME%` with their actual values, changing the backslashes to forward slashes for proper URL syntax.

9. Reconfigure the `ShibEchoService`.

> *By default, the `ShibEchoService` is configured to accept all attributes (i.e., no authorization). We now expand the authorization chain to include* Attribute Acceptance Policy *and* Attribute-based Authorization Policy. *These policy checks are enabled by `AttributeAcceptancePIP` and `SAMLAttributePDP`, respectively.*

   a. In %GLOBUS_LOCATION%\etc\gridshib-gt-echo-0_6_0\echo-service-security-descriptor.xml, comment out this line

```
<authz value="shibecho:org.globus.gridshib.SAMLAssertionPushPIP"/>
```

   and uncomment this line

```
<authz value="shibecho:org.globus.gridshib.SAMLAssertionPushPIP
              shibecho:org.globus.gridshib.AttributeAcceptancePIP
              shibecho:org.globus.gridshib.SAMLAttributePDP"/>
```

   This enables `AttributeAcceptancePIP` and `SAMLAttributePDP` in the authz chain.

10. Configure the `AttributeAcceptancePIP`.

> *In the current version of GridShib for GT, Attribute Acceptance Policy boils down to a list of* trusted SAML authorities. *Attributes are accepted from a SAML issuer if and only if the issuer's `entityID` is on this list. By default, the GridShib CA's `entityID` is on this list. We now add a proxy issuer to the list of trusted SAML authorities.*

   a. Obtain the Subject DN of your GridShib CA-issued EEC:

```
> %GLOBUS_LOCATION%\bin\rfc2253dn
```

   b. Add the *RFC 2253 form* of your Subject DN to the trusted SAML authorities file %GLOBUS_LOCATION%\etc\gridshib-gt-echo-0_6_0\trusted-saml-authorities.txt.

11. Request the `ShibEchoService`, authenticating with a level 1 proxy credential.

> *Since the GridShib SAML Tools issue an assertion with two attributes by default, you will see a total of four (4) attributes in the logs, the `NameIdentifier` from the assertion bound to the EEC, plus two attributes and a `NameIdentifier` bound to the level 1 proxy.*

   a. In the third Command Prompt window, issue a level 1 proxy:

```
> %GRIDSHIB_HOME%\bin\gridshib-saml-issuer --user trscavo
    --authn --x509 --outfile c:\temp\testcredential.pem
    --authnMethod urn:oasis:names:tc:SAML:1.0:am:password --address 255.255.255.255
```

   b. In the first Command Prompt window, start the container.
   c. In the second Command Prompt window, set the proxy path and request the service:

```
> set X509_USER_PROXY=c:\temp\testcredential.pem
> %GLOBUS_LOCATION%\bin\shibecho -d -z none
    -s https://localhost:8443/wsrf/services/ShibEchoService
```

   You should receive four attributes in the response.
   d. In the second Command Prompt window, stop the container.

12. Reconfigure the `ShibEchoService`.

> A master PDP *controls other PIPs and PDPs. For example, the `GridShibPushPDP` is functionally equivalent to the authz chain configured previously.*

   a. In %GLOBUS_LOCATION%\etc\gridshib-gt-echo-0_6_0\echo-service-security-descriptor.xml, comment out this line

```
<authz value="shibecho:org.globus.gridshib.SAMLAssertionPushPIP
              shibecho:org.globus.gridshib.AttributeAcceptancePIP
              shibecho:org.globus.gridshib.SAMLAttributePDP"/>
```

and uncomment this line

```
<authz value="shibecho:org.globus.gridshib.GridShibPushPDP"/>
```

This enables the master PDP `GridShibPushPDP`.

13. Request the `ShibEchoService`, authenticating with a level 1 proxy credential *via Secure Message*.

    > *The previous request defaulted to transport-level security. To pass the SAML assertions at the message level, all that's needed is a simple command-line switch.*

    a. In the first Command Prompt window, start the container.
    b. In the second Command Prompt window, request the service:

    ```
    > %GLOBUS_LOCATION%\bin\shibecho -d -z none -m msg
        -s https://localhost:8443/wsrf/services/ShibEchoService
    ```

    You should receive four attributes in the response.

    c. In the second Command Prompt window, stop the container.

14. Reconfigure the `ShibEchoService`.

    a. In %GLOBUS_LOCATION%\etc\gridshib-gt-echo-0_6_0\echo-service-security-descriptor.xml, comment out this line

    ```
    <authz value="shibecho:org.globus.gridshib.GridShibPushPDP"/>
    ```

    and uncomment this line

    ```
    <authz value="shibecho:org.globus.gridshib.SAMLAssertionPushPIP
                  shibecho:org.globus.gridshib.AttributeAcceptancePIP
                  shibecho1:org.globus.gridshib.SAMLAttributePDP
                  shibecho2:org.globus.gridshib.SAMLAttributePDP"/>
    ```

    This enables `SAMLAttributePDP` *twice* in the authz chain. Each invocation of `SAMLAttributePDP` is associated with its own policy file. (See %GLOBUS_LOCATION%\etc\gridshib-gt-echo-0_6_0\server-config.wsdd for the policy file configuration.)

15. Reconfigure the GridShib SAML Tools.

    a. Create config file c:\temp\gridshib-saml-issuer.properties with the following lines:

    ```
    # an emailAddress name identifier
    Format=urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    formatting.template=%PRINCIPAL%@gmail.com
    # FriendlyName="mail"
    Attribute.EMAIL.Namespace=urn:mace:shibboleth:1.0:attributeNamespace:uri
    Attribute.EMAIL.Name=urn:mace:dir:attribute-def:mail
    Attribute.EMAIL.Value=trscavo@gmail.com
    # a level 1 proxy issued by the GridShib SAML Tools
    certLocation=file:/C:/temp/testcredential.pem
    keyLocation=file:/C:/temp/testcredential.pem
    ```

16. Request the `ShibEchoService`, authenticating with a level 2 proxy credential.

    > *In the previous exercise, the GridShib SAML Tools have been configured to issue a level 2 proxy signed by a level 1 proxy. The level 2 proxy contains one attribute, so you should see a total of six attributes in the logs, three (3) `NameIdentifier` values and three (3) attribute values.*

    a. In the third Command Prompt window, issue a level 2 proxy:

    ```
      > %GRIDSHIB_HOME%\bin\gridshib-saml-issuer --user trscavo
          --authn --x509 --outfile c:\temp\testcredential.pem
          --authnMethod urn:oasis:names:tc:SAML:1.0:am:password --address 255.255.255.255
          --config file:/c:/temp/gridshib-saml-issuer.properties
    ```

    b. In the first Command Prompt window, start the container.
    c. In the second Command Prompt window, request the service as before. You should receive six attributes in the response.
    d. In the second Command Prompt window, stop the container.