Grid Grouper Authorization Plug-In For GridFTP w/ Java Authorization

Introduction

This plug-in is an add-on for the GridFTP w/ Java Authorization software. For information on that software, please refer to the User Documentation.

Grid Grouper Authorization Plug-In Configuration

Grid Grouper is a group management tool in caGrid (1). The authorization plug-in uses grid grouper membership expressions to determine authorization for a particular action and path on the GridFTP server.

The Grid Grouper plug-in is added on to the default installation by unzipping the plug-in distribution into $GRIDFTP_ROOT. You should end up with the directory $GRIDFTP_ROOT/caGrid-1.0-gridftpauthz. The grid grouper configuration is specified on the classpath, in the "properties" directory. The configuration file is properties\org\cagrid\gridftp\authorization\plugin\gridgrouper\gridgrouper_auth_config.xml. You need to do two things in order to use the plug-in:

1. Customize and install the GridFTP Java Authorization configuration
    a. Make sure your GRIDFTP_ROOT environment variable is set to where you installed the GridFTP w/ Java Authorization package.
    b. Unzip the Grid Grouper plug-in distribution into this directory
    c. `cd caGrid-1.0-gridftpauthz`
    d. `cd conf`
    e. `ant`
    f. If necessary, back up your current java authorization configuration (back up $GRIDFTP_JAVA_AUTH_CONF)
    g. `cp gridftp_java_auth.cfg $GRIDFTP_JAVA_AUTH_CONF`
2. Modify your grid grouper configuration
    a. Modify the configuration file, adding and removing rules as desired
    b. Validate the configuration against the schema.

Grid Grouper Configuration File Format

The configuration file format is relatively straightforward. You can use the schemas in the build/schema directory to validate your configuration after you modify it. The grid grouper

configuration schema is in build/schema/gridgrouper-config.xsd. That schema imports another schema in the xsd subdirectory.

The configuration contains multiple `<rule>`s, each of which is a plug-in rule for purposes of finding the grid grouper expression to use for a specific GridFTP transfer. Each rule consists of an action, a path, and a grid grouper MembershipExpression. The following is an overview of the plug-in configuration. Refer to the schema for more details.

The plug-in uses the action and path of the file or directory included in a GridFTP request. The action is one of the GridFTP actions defined in the schema. They are currently "read", "write", "lookup", "create", "delete", "chdir", or "*". The "*" action acts as a wildcard, matching any action. Please refer to the Developer Documentation for details on how these actions are used for each GridFTP request. The path is a path to a file or directory, using standard Unix filename conventions. For paths that refer to any file in a directory structure, end the path with *. As an example, to make a rule for all files in `/tmp`, make sure the path for the rule is `/tmp/*`. Finally, write the grid grouper membership expression that you want to use for this rule.

Here is an example configuration file:

```
<?xml version="1.0" encoding="UTF-8"?>
<GridFTPGrouperConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.cagrid.org/1/gridftpauthz gridgrouper-config.xsd"
 xmlns="http://www.cagrid.org/1/gridftpauthz">
<rule>
        <action>*</action>
        <path>/tmp/*</path>
        <MembershipExpression xmlns="http://cagrid.nci.nih.gov/1/GridGrouper"
xmlns:ns1="http://cagrid.nci.nih.gov/1/GridGrouper" ns1:logicRelation="AND">
                <MembershipQuery ns1:MembershipStatus="MEMBER_OF">
                        <GroupIdentifier>
        <gridGrouperURL>https://training.cagrid.org:8443/wsrf/services/cagrid/GridGrou
per</gridGrouperURL>
                                <GroupName>training:trainees</GroupName>
                        </GroupIdentifier>
                </MembershipQuery>
        </MembershipExpression>
</rule>
</GridFTPGrouperConfig>
```

This rule matches any action on any file or directory in the /tmp directory hierarchy, including files in /tmp and all files and directories under /tmp. The grid grouper membership expression is a simple "MEMBER_OF" query for a group named "trainees" in the "training" stem.

When testing the plug-in, you can check the GridFTP output log and the C authz implementation log for details on how the plug-in is working. See the section entitled "**Error! Reference source not found.**" for more information on where the logs are written.

Grid Grouper Configuration Rule Precedence

The plug-in implements the concept of rule precedence. The rule that has a path that most closely matches the requested path is the one that is used. Then, if two rules only differ by the action specified, the rule for the action that matches exactly is the rule that will eventually be used.

For example, take the following two rules:

```
<rule>
        <action>*</action>
        <path>/tmp/*</path>
        <MembershipExpression>
                …
        </MembershipExpression>
</rule>
<rule>
        <action>read</action>
        <path>/tmp/mydir/*</path>
        <MembershipExpression>
                …
        </MembershipExpression>
</rule>
```

For a request specifying a path of `/tmp/mydir/foo`, the second rule will take precedence because the path in the second rule is the closest match to the requested path.

Then, as an example of precedence when the path in two rules is exactly the same, take the two following rules:

```
<rule>
        <action>*</action>
        <path>/tmp/*</path>
        <MembershipExpression>
                …
        </MembershipExpression>
</rule>
<rule>
        <action>read</action>
        <path>/tmp/*</path>
        <MembershipExpression>
```

```
            …
        </MembershipExpression>
</rule>
```

The rules only differ by the action specified. Therefore, for a request specifying the `read` action and any path under /tmp (e.g., /tmp/foo), the second rule will take precedence over the first. However, for a `write` action, the first rule matches.

Grid Grouper Plug-in FAQ

Question: When I run the Grid Grouper authorization plugin, the GridFTP log file shows the following output:

```
ERROR  isMember, ; nested exception is:
        org.globus.common.ChainedIOException:
Authentication failed [Caused by: Failure unspecified at GSS-API
level [Caused by: Unknown CA]]
```

What is the problem?

Answer: The problem is that the JVM running the Java authorization code doesn't recognize Grid Grouper's CA. Make sure that the user running the gridftp server has the Grid Grouper's CA certificate in ~/.globus/certificates.

Works Cited

1. Grid Grouper. *caGrid Wiki.* [Online] http://www.cagrid.org/mwiki/index.php?title=GridGrouper:Main.