NORDUGRID-TECH-26
23/11/2012

The NorduGrid GridFTP Server

Description and Administrator's Manual

A. Konstantinov*, D. Cameron

*aleks@fys.uio.no

Contents

1 Introduction

The NorduGrid [1] GridFTP service (GFS) consists of a standard Globus GridFTP server with NorduGrid modifications on top. The GFS provides a means to map GSI identities to local usernames, and thus can expose a local filesystem to the Grid using a highly configurable set of authorization policies. Local file access in the GFS is implemented through plugins (shared libraries). There are 3 plugins provided:

- *fileplugin.so*: provides plain file access and can be used to enable a Storage Element with highly configurable access control,
- *gaclplugin.so*: uses GACL [4] to control access to the local file system,
- *jobplugin.so*: provides an interface (virtual directory and virtual operations) to submit,cancel, clean, renew credentials and obtain information about jobs controlled by A-REX, ARC's job processing service.

This document concentrates on the first two plugins, which provide file-handling capabilities of the GFS, in particular how to set up a Storage Element (SE) to allow Grid access to data. Information on the job-handling part of the GFS can be found in *"ARC Computing Element: System Administrator Guide"* [3]. This guide provides all the details for setting up an ARC Computing Element and many parts of this manual refer the reader to it for more information.

2 Authorization

The GFS can use a highly-configurable set of rules to permit access and perfrom mapping from grid identities to local users. The concept of authorization groups and VOs is described in detail in [3], in the section *"Access control: users, groups, VOs"*.

3 Configuration

The GFS configuration is done through a single INI-style configuration file, and the default location of this file is:

- */etc/arc.conf*

A different configuration file location can be specified by the environment variable ARC_CONFIG. The configuration file consists of empty lines, lines containing comments (lines starting with #) or configuration commands. It is separated into sections. Each section starts with a string containing

- *[section name/subsection name/subsubsection name]*.

Each section continues until the next section or until the end of the file. The configuration file can have commands for multiple services/modules/programs. Each service has its own section named after it. The GFS uses the *[gridftpd]* section and sub-sections, along with other authorization-related sections. Commands in section *[common]* apply to all services configured in the configuration file. Command lines have the format

- *name="arguments string"*.

An example configuration is shown in Section 5.

3.1 General Configuration Parameters

General configuration is documented in [3], in the section *"Commands in the [gridftpd] section"*.

3.2 Plugin Configuration

Subsections of the *[gridftpd]* section specify plugins which serve the virtual FTP path (similar to the UNIX mount command). The name of the subsection is irrelevant but it is useful to use a name related to the plugin, e.g. [gridftpd/files] for the *fileplugin*. Inside the subsection, the following commands are supported:

- ***plugin***=*library_name* – use plugin *library_name* to serve virtual path.
- ***path***=*path* – virtual path to serve.

The GFS comes with 3 plugins: *fileplugin.so, gaclplugin.so* and *jobplugin.so*.

3.2.1 JobPlugin

jobplugin commands are described in [3], in the section *"Commands to configure the jobplugin"*.

3.2.2 FilePlugin

fileplugin.so supports the following options:

- ***mount***=*path* – defines the place on local filesystem to which file access operations apply.
- ***dir***=*path options* – specifies access rules for accessing files in *path* (relative to virtual and real path) and all the files below.
  options is a list of the following keywords:
  - ***nouser*** – do not use local file system rights, only use those specified in this line.
  - ***owner*** – check only file owner access rights.
  - ***group*** – check only group access rights.
  - ***other*** – check only "others" access rights.

  The options above are exclusive. If none of the above are specified, the usual UNIX access rights are applied.
  - ***read*** – allow reading files.
  - ***delete*** – allow deleting files.
  - ***append*** – allow appending files (does not allow creation).
  - ***overwrite*** – allow overwriting of existing files (does not allow creation, file attributes are not changed).
  - ***dirlist*** – allow obtaining list of the files.
  - ***cd*** – allow to make this directory current.
  - ***create*** *owner:group permissions_or:permissions_and* - allow creating new files. File will be owned by *owner* and owning group will be *group*. If '*' is used, the user/group to which connected user is mapped will be used. The permissions will be set to *permissions_or* & *permissions_and* (the second number is reserved for future usage).
  - ***mkdir*** *owner:group permissions_or:permissions_and* - allow creating new directories.

3.2.3 GACLPlugin

gaclplugin.so supports the following options:

- ***gacl***=*gacl* – GACL XML.
- ***mount***=*path* – local path served by plugin.

The GACL XML may contain variables which are replaced with values taken from the client's credentials. The following variables are supported:

$subject – subject of user's certificate (DN),

$voms – subject of VOMS[2] server (DN),

$vo – name of VO (from VOMS certificate),

$role – role (from VOMS certificate),

$capability – capabilities (from VOMS certificate),

$group – name of group (from VOMS certificate) .

Additionally, the root directory must contain a *.gacl* file with initial ACLs. Otherwise the rule will be "deny all for everyone".

4 Running the service

An initialization script *gridftpd* for the GFS is provided in *$ARC_LOCATION/etc/init.d* (or equivalent depending on architecture).

```
Usage: gridftpd {start|stop|status|restart|reload|condrestart}
```

Upon starting and depending on the configured log level, messages will be logged in the log file specified in the configuration file.

5 Configuration Example

In this example the fileplugin is used to expose the local directory "/home/grid" to the Grid where it can be accessed through the URL "gsiftp://myhost.org/files". All users specified in the gridmap file have full read/write access.

```
[common]
hostname="myhost.org"
gridmap="/etc/grid-security/grid-mapfile"

[gridftpd]
debug="3"
encryption="no"
allowunknown="no"
maxconnections="200"

[gridftpd/files]
path="/files"
plugin="fileplugin.so"
mount="/home/grid"
dir="/ nouser read delete cd dirlist create *:* 664:664 mkdir *:* 775:775"
```

Acknowledgements

This work was supported in parts by: the Nordunet 2 program, the EU KnowARC project (Contract nr. 032691) and the EU EMI project (Grant agreement nr. 261611).

References

[1] The NorduGrid Collaboration. Web site. URL `http://www.nordugrid.org`.

[2] R. Alfieri et al. From gridmap-file to VOMS: managing authorization in a Grid environment. *Future Gener. Comput. Syst.*, 21(4):549–558, 2005. ISSN 0167-739X.

[3] O. Smirnova F. Paganelli, Zs. Nagy et al. *ARC Computing Element System Administrator Guide*. The NorduGrid Collaboration. URL `http://www.nordugrid.org/documents/arc-ce-sysadm-guide.pdf`. NORDUGRID-MANUAL-20.

[4] A. McNab. The GridSite Web/Grid security system: Research Articles. *Softw. Pract. Exper.*, 35(9): 827–834, 2005. ISSN 0038-0644.