Table of Contents

THIS PAGE IS OUTDATED.

Please go to the new gLExec Service Reference Card

gLExec on WN, CE and anywhere else

Functional description

gLExec is a program that acts as a light-weight 'gatekeeper'. gLExec takes Grid credentials as input. gLExec takes the local site policy into account to authenticate and authorize the credentials. gLExec will switch to a new execution sandbox and execute the given command as the switched identity. gLExec is also capable of functioning as a light-weight control point which offers a binary yes/no result called the logging-only mode.

It is used on the Worker Node in the context of Multi User Pilot Jobs and on a CE in the context of CREAM.

The main gLExec home page with useful how-to's, debugging hints and a FAQ is located at:
https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/GLExec

Daemons running

None. The SCAS daemon is usually on a separate node (type).

Init scripts and options (start|stop|restart|...)

No init scripts are needed for the gLExec.

In the Manual pages of gLExec we've explained all the command line options of the executable:
https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Man_pages_of_gLExec

Configuration files location with example or template

The glexec.conf configuration file path is set at compile due to the security implication related to operating gLExec in a safe way.

The default location of the glexec.conf file is: /opt/glite/etc/glexec.conf

Note: for OSG users who get gLExec via VDT the path is: /etc/glexec.conf

Logfile locations (and management) and other useful audit information

The build-in log file location for glexec is /var/log/glexec/glexec_log. This can be changed at compile time or altered using the glexec.conf file.

- Syslog available: yes

In the Manual pages of gLExec's glexec.conf we've explained all the possibilities of configuring the log file location:

https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Man_pages_of_gLExec

Open ports

There are no open ports created. The only network related interaction results from the syslog client-side interface and the SCAS client-side interface. In both case gLExec acts as a networked client.

Possible unit test of the service

There are several tips and hints that we've listed to test the functionality of gLExec. Those can be found at: https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Debugging_hints

Where is service state held (and can it be rebuilt)

To lower administrative maintenance we advice to use a service like SCAS, Argus or GUMS to be used in conjunction with the gLExec on Worker Nodes scenarios. The mapping state will be held at the respective back-end mapping service.

gLExec could still be installed with node-local mappings. An /etc/grid-security/gridmapdir/ will keep the mapping state as like an LCG-CE.

Cron jobs

N/a.

Security information

Access control Mechanism description (authentication & authorization)

Proxy certificate verification in the verify proxy plugin. LCAS framework, using the user_ban plugin. The LCAS VOMS plugin can be used to whitelist or blacklist*. The * is that this requires the use of GACL to express it. Offloading possibility for the authorization decision to a SCAS, Argus or GUMS service.

How to block/ban a user

We recommend to ban a user at a SCAS, Argus or GUMS service. A node local mapping is still supported. gLExec features LCAS and a user_ban plugin. Enter a DN in the configured file and the DN will be banned for use on that host.

Network Usage

When gLExec is configured to use Syslog, the node local Syslog configuration might lead to network interaction. On a Worker Node installation it is recommended to use a SCAS, Argus or GUMS service. These authorization (and mapping) service feature mutual authentication using SSL and a SOAP over HTTP with SAML2-XACML2 authorization statements.

Firewall configuration

Outbound connection for syslog and outbound connection (SSL) to the SCAS, Argus or GUMS service node. Typically TCP port 8443. In this case 'Outbound' means, from the node to the central service node, not the outside world.

Security recommendations

File permissions

For all run-modes of gLExec, the gLExec must be "executable" for all users.

Versions up to 0.6.8-3

*For running gLExec in "'setuid"' mode, "preferably" use the following mode ("'setuid"' and "'setgid"'):

```
-r-sr-sr-x 1 root   root   12345 2010-02-29 12:34 glexec
-rw-r----- 1 root   glexec   123 2010-02-29 12:34 glexec.conf
```

*In case "setgid" is not possible, "preferably" use the following mode (only "'setuid"'):

```
-r-sr-xr-x 1 root   root   12345 2010-02-29 12:34 glexec
-rw-r--r-- 1 root   glexec   123 2010-02-29 12:34 glexec.conf
```

*For running gLExec in "'logging only"' mode, "preferably" use the following mode:

```
-r-xr-xr-x 1 root   root   12345 2010-02-29 12:34 glexec
-rw-r--r-- 1 root   glexec   123 2010-02-29 12:34 glexec.conf
```

Note that these settings are also possible on a NFS mount.

Version 0.7.0-2

*For running gLExec in "'setuid"' mode, "preferably" use the following mode (only "'setuid"'):

```
-rws--x--x 1 root   root   12345 2010-02-29 12:34 glexec
-r-------- 1 glexec root     123 2010-02-29 12:34 glexec.conf
```

*For running gLExec in "'logging only"' mode, "preferably" use the following mode:

```
-rwx--x--x 1 root   root   12345 2010-02-29 12:34 glexec
-r--r--r-- 1 glexec root     123 2010-02-29 12:34 glexec.conf
```

Note that these settings are also possible on a NFS mount.

File permission verification

To prevent a wrong installation of gLExec, which could lead to easy exploitation of the computer system, an out side source must be able to verify the installation. Consider the use of tripwire, rpm --verify or something similar. At the moment rpm --verify will not work as the gLExec package has not been packaged with the setuid or setgid permission bits.

Security incompatibilities

Unknown. If there is any, please let the developers of gLExec know about problems or incompatibilities.

List of externals (packages are NOT maintained by Red Hat or by gLite)

In combination with the SCAS-Client LCMAPS plug-in the saml2-xacml2-c-lib package is required. This maintained by Globus, but repackaged via org.glite.

Other security relevant comments

Environment Variables

There are two detailed overviews made about the use of environment variables by gLExec.

The following overview handles the safety features with respect to environment variables. It handles the MALLOC_* and LD_* familiy environment variables and how gLExec deals with some of the common shell

environment variables, like HOME:

https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Need_to_Know%27s#Safety_features

This overview handles proxy file handling via the environment variables. Which variables services which purposes and so on:

https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Proxy_file_handling_in_gLExec

Whitelist

The gLExec executable can only be used by users in the whitelist. There are two ways of getting in the whitelist. The build-in method can be used in absence of a glexec.conf configuration file. The build-in method is to look at the user's primary and secondary Unix group that are currently associated with the user. One of the groupnames must be equal to 'glexec'. This will allow the user to continue running gLExec. The other (more advertised) method is to configure the line **user_white_list** in the glexec.conf configuration file.

The user_white_list line holds a list of comma separated user names that are allowed to call gLExec. When the name starts with a dot, e.g. .pool, the name denotes a pool account and matches all user names starting with pool, followed by one or more digits. Thus .pool matches the regular expression: glexec[0-9]+.

Typically in our infrastructure the poolaccount that a especially setup to allow for pilot job framework execution are listed in the whitelist only.

Note: also root is 'just an account' and needs to be whitelist in the special case that you wish to test or use gLExec with root privileges.

Utility scripts

We're gathering a list of simple and more complex test scripts on the follow page to test gLExec in various ways: https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/Debugging_hints

Location of reference documentation for users

We're writing the following wiki for both system administrators and users:
https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/GLExec

Location of reference documentation for administrators

We're writing the following wiki for both system administrators and users:
https://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/GLExec

-- OscarKoeroo - 01 Jun 2009

This topic: EGEE > GLExec
Topic revision: r5 - 2012-08-27 - unknown