



EUROPEAN MIDDLEWARE INITIATIVE

GLExec

Document version:	1.0.0
EMI Component Version:	0.8.10
Date:	April 28, 2011

This work is co-funded by the EC EMI project under the FP7 Collaborative Projects Grant Agreement Nr. INFSO-RI-261611.

NAME

glexec - execute a command as another user based on grid credentials

SYNOPSIS

glexec <command> [*arguments*]

glexec <-h/-v/-V>

DESCRIPTION

gLExec allows a permitted user to execute a command as another normal user, where the identity change is based on a X.509 proxy certificate. Whether a user is permitted is determined using the gLExec configuration file. The authentication and authorization is done by LCAS and LCMAPS. Only when the user is authorized and a valid mapping has been established will gLExec execute the specified command with its arguments. The command can either be specified as an absolute path, or will be taken relative to the current working directory after the identity change.

gLExec can be installed in either user-switching or logging-only mode. In logging only mode, no actual user-switch is performed, and hence the target executable will be run with the same credentials and permissions as the calling user, but the mapping as it would have been done, will be logged. Furthermore gLExec will still fail in this mode if either LCAS or LCMAPS denies or fails.

gLExec clears all environment variables except those starting with **GLEEXEC_** and those explicitly whitelisted in the **glexec.conf(5)**. Variables starting with **MALLOC_** cannot be whitelisted and will always be lost. Furthermore, note that the variable **LD_LIBRARY_PATH** is ignored for setuid applications. To overcome these limitations, one can use the `glexec_wrapenv.pl` and `glexec_unwrapenv.pl` scripts.

A number of variables will be set up by gLExec for the target environment. See further under **ENVIRONMENT** for individual details.

OPTIONS

- h** Displays usage information.
- v** Displays the version of gLExec.
- V** Displays the compile-time defaults. Only available for users root or glexec.

ENVIRONMENT -- for gLExec**GLEEXEC_CLIENT_CERT**

should point to a file containing a valid proxy on which the user switch will be based. This is typically a proxy of the payload user. The file should be readable/writable *only* by the calling user. If a relative path is specified it is taken relative to the current working directory at the time gLExec is called.

X509_USER_PROXY

should point to a file containing a valid proxy used to authenticate at an authorization service such as a SCAS or PEPd. This is a proxy of the pilot job user. **NOTE:** gLExec will reset this variable to a suitable proxy for the payload user.

GLEEXEC_SOURCE_PROXY

when set, the file it points to will be copied for use as proxy by the payload user. The file should be readable/writable *only* by the calling user. If a relative path is specified it is taken relative to the current working directory at the time gLExec is called. When unset it will default to the file pointed to by **GLEEXEC_CLIENT_CERT**. **NOTE:** the automatic copying of a proxy for the payload user and setting up of the corresponding environment variables can be disabled by setting the configuration option **create_target_proxy** to 'no'.

GLEEXEC_TARGET_PROXY

when set, the contents of GLEEXEC_SOURCE_PROXY or its default value will be copied to this location, with the credentials of the target user. The path has to be *absolute*. When unset, its default depends on the gLExec running mode, in user switching mode its default is a unique file-name /tmp/x509up_u<uid>.glexec.XXXXXXX where <uid> will be the target uid and XXXXXXX will be 6 random letters. In logging only mode its default value will be equal to GLEEXEC_SOURCE_PROXY or its default, but *no* file will be copied. **NOTE:** the automatic copying of a proxy for the payload user and setting up of the corresponding environment variables can be disabled by setting the configuration option **create_target_proxy** to 'no'.

SSL_CLIENT_CERT (deprecated)

gLExec does *NOT* use this variable, use GLEEXEC_CLIENT_CERT instead. It is the old style of passing a certificate, whereby the variable contained the whole certificate and not a path to a certificate.

ENVIRONMENT -- for executable

The following environment variables are set up during the execution of gLExec with sensible values for the execution environment of the requested command:

PATH

/usr/local/bin:/usr/bin:/bin

HOME

in switching mode, set to the home directory of the mapped user, e.g. /home/pool0001, in logging only mode it is set to the home directory of the calling user.

USER**LOGNAME**

in switching mode, both are set to the username of the mapped user. In logging only mode both are set to that of the calling user.

X509_USER_PROXY

set to value of GLEEXEC_TARGET_PROXY or its default. When in logging only mode GLEEXEC_TARGET_PROXY is unset, no file will be copied and this variable will point to the same location as (the default of) GLEEXEC_SOURCE_PROXY.

IMPORTANT: although for the payload users, this variable is equal in value to GLEEXEC_TARGET_PROXY, payload users should *NOT* rely on GLEEXEC_TARGET_PROXY but *only* use this X509_USER_PROXY variable.

GLEEXEC_TARGET_PROXY (deprecated)

Do not rely on this in the target environment. For the target user this variable has the same value as X509_USER_PROXY. It is only set for backwards compatibility and it is foreseen to be no longer set in a future version.

RETURN VALUES

Upon successful execution of a program, the return value from **gLExec** will simply be the return value of the program that was executed. Otherwise, **gLExec** quits with the following limited range of return values:

201 - Client error:

This error code is triggered when the user (caller of gLExec) has to change something in order for gLExec to be able to succeed. Some example situations: the input files (like proxy certificates) might have the wrong permissions or do not exist; the executable to be executed doesn't exist or has unacceptable file permissions.

202 - Internal **gLExec** error:

This error code has to be handled by the system administrator of the machine. This might be due to wrong permission bits on the configuration file, initialization errors of LCAS and/or LCMAPS or other system specific errors that can only be addressed by somebody with sufficient rights on the machine.

203 - Authorization error:

Everything went ok, but the user is not authorized. This could be triggered because the calling process was not in the white list and therefore not privileged to use **gLExec**. The other reason is that LCAS and/or LCMAPS failed to authorize the (real) user and gain an account mapping.

204 - Child return value overlap:

This error code is triggered when **gLExec** is in linger mode (activated by default) and when the called child process returns an exit code that overlaps with one of the error code numbers 201, 202, 203 and 204.

126 - Shell returns that the executable can't be executed:

This error code is triggered when the `execve()` call failed to execute the command, because of permission, execution or system problems found during the call for the executable that was tried to be set up. The shell code is not caught, but forwarded as an error code from the actual child process.

128+n - Child exited due to signal *n*.**INSTALLATION**

NOTE: this section is exclusively valid from **gLExec** version 0.7 and higher.

The preferred ownership for the **glexec** executable is `root.root` or `root.glexec`. For the config file, the preferred ownership is `glexec.root`.

For *switching mode*, the preferred set of permissions for the executable is 4711 and for the config file 0400:

```
-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 *logging only mode*, the preferred set of permissions for the executable is 0711 and for the config file 0444:

```
-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
```

These setups also work when either or both are installed on **NFS** mounts with *root-squash* enabled.

FILES

`/etc/glexec.conf`

BUGS

Reading and writing of proxy files will generally be done with either `flock(2)` or `fcntl(2)` locks. However be aware that these mechanisms do not always reliably work on NFS file systems. See `flock(2)` for more details.

LIBRARY PATH NOTES

The effective library path of the system and shell must be able to locate the required runtime libraries for **gLExec** itself, LCAS, LCMAPS and their dynamically loaded plug-ins. In an ideal world this would mean to have all the required libraries be installed in system native locations on the file system. In practice it is

usually necessary to add the paths **/opt/globus/lib/** and **/usr/lib64** to the run-time library search paths.

For gLExec versions 0.8 and higher, the location of the LCAS and LCMAPS dynamic libraries can be specified in the `glexec` configuration file. However, note that these are not used to resolve second level dependencies (i.e. those needed by LCAS and LCMAPS themselves).

Since gLExec is a setuid application, `LD_LIBRARY_PATH` is ignored, see `ld.so(8)`, so this leaves adding the path to the `/etc/ld.so.conf{.d/glite}` file or directory or hoping for a correctly applied set of `RPATH` values in the libraries. When using a version built by ETICS, only the `ld.so.conf` option is available since ETICS strips the `RPATH` values in the libraries. If you build all the components from source without ETICS, these `RPATHs` take precedence.

SEE ALSO

glexec.conf(5), *execve(2)*, *flock(2)*, *fcntl(2)*, *ld.so(8)*, *glexec_wrapenv.pl(1)*, *glexec_unwrapenv.pl(1)*

<http://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/GLExec>

AUTHORS

Written by Oscar Koeroo & Mischa Sallé (from Jan 2009)

Written by Gerben Venekamp (until Jan 2009)

COPYRIGHT

Copyright © 2009-2010 EGEE

NAME

glexec.conf - configuration file for gLExec

DESCRIPTION

The gLExec configuration file is a standard .ini file and by default located at */etc/glexec.conf*. All gLExec specific settings have to be listed under the [glexec] tag and although other tags are allowed, non other than [glexec] are taken into account.

The following key value pairs are currently understood by gLExec.

[glexec]

linger = {yes,no}

Controls the behaviour of gLExec when executing the real user job. gLExec either forks, runs the real user job in the child and wait for it to return, i.e. gLExec is said to linger, or gLExec will load the image of the real user job over that of itself, in which case it does not linger. Default: *yes*.

lock_mechanism = {flock,fcntl,disabled} (deprecated)

Use **target_lock_mechanism** instead.

target_lock_mechanism = {flock,fcntl,disabled}

This option specifies the type of file locking used when writing the target proxy. By default **flock(2)** will be used. In addition **fcntl(2)** can be selected, which works better over NFS. Thirdly the locking mechanism can be disabled.

input_lock_mechanism = {flock,fcntl,disabled}

This option specifies the type of file locking used when reading the input proxies, i.e. the GLEEXEC_CLIENT_CERT and the GLEEXEC_SOURCE_PROXY. By default **flock(2)** will be used. In addition **fcntl(2)** can be selected, which works better over NFS. Thirdly the locking mechanism can be disabled.

log_destination = {syslog,file}

Tells where gLExec, LCAS and LCMAPS should send logging information to. For value *file* see also next key **log_file**.

NOTE: In logging-only mode, only *syslog* is allowed and will automatically be selected. Also in case opening of the logfile fails, the error will be logged to *syslog*.

The default is *syslog*.

log_level = {0,...,5}

Set the log level of gLExec. Higher means more logging, highest level includes debug information. See also **diff_syslog_levels**. Default is level 3.

syslog_facility

When set to a valid syslog facility, this will be used instead of the built in default. See **syslog(3)** for valid values. Default: *LOG_DAEMON*.

diff_syslog_levels = {yes,no}

When **log_destination** is *syslog*, gLExec by defaults logs all messages on syslog level *LOG_ERR*, **log_level** then only determines how much is logged. When this option is enabled, **log_level** is also translated into the corresponding syslog level. Default: *no*.

log_file Specify which file gLExec should use in case *file* has been chosen as log destination. This key has only meaning when the key **log_destination** is set to *file*. See also **lcas_log_file** and **lcmaps_log_file**. Default: */var/log/glexec/glexec_log*.

log_file_group

When creating **log_file** and parent directories, use this group. The log file is created using permissions 0640, parent directories using 0750. Default: *GID 0*.

silent_logging = {yes,no}

Turn off/on logging of gLExec. Default: *No*.

omission_private_key_white_list

List of comma separated user names that do not have to present a private key in their certificate when calling gLExec (note: this applies only to the certificate or proxy that will be used for authentication and authorization of the users calling gLExec, i.e. the GLEEXEC_CLIENT_CERT, and *not* the one that can be copied by gLExec).

preserve_env_variables

List of comma separated environment variables that gLExec need to preserve in addition to the set of environment variables that is preserved by default. Each name is matched as a whole, case-sensitive, string match.

NOTE: Please note that not all environment variables can be preserved due to the way the linker might work. In case of setuid executables, LD_LIBRARY_PATH is normally ignored by the dynamic runtime linker, see ld.so(8) and hence gLExec has no means of preserving it. In addition, all variables starting with MALLOC_ are removed for security reasons and cannot be preserved.

pedantic_security_checks = {yes,no}

This option will enable a set of pedantic security checks: It will check whether the executable is NOT world writable and if the executable and directory are owned by either the calling user, target user (only in switching mode) or root. Default: *No*.

prohibit_exec_via_symlink = {yes,no}

This option will disallow the execution of a command or executable that is symlinked. Default: *No* (which will allow the execution of a symlink)

user_identity_switch_by = {glexec,lcmaps}

Determine where the target user identity is enforced. It takes either the value of *glexec*, which means gLExec will do the actual switching to the target uid, or *lcmaps*, in which case the actual switching is left to LCMAPS. In case the *lcmaps* value is used, please take note of the **BUGS** section. Default: *glexec*.

user_white_list

List of comma separated user names that are allowed to call gLExec, e.g. **oscar,mischa,root**

A single * is interpreted as everyone. Note that it cannot be used as part of a name.

When the name starts with a dot, e.g. **.dteam**, the name denotes a pool account and matches all user names starting with dteam, followed by one or more digits. Thus **.dteam** matches the regular expression: `dteam[0-9]+`. See also **group_white_list**.

group_white_list

All users belonging to this group are allowed to call gLExec, even if they are not in the **user_white_list**, see above. Default: *glexec*.

backlog_path

When a directory is specified for this option, backlog entries will be created. A backlog entry has a filename consisting of the username of the calling user followed by colon and the process id of glexec; it has as contents the username of the target user.

NOTE: in order to create backlog entries, it is also necessary to configure gLExec to do the switch, see **user_identity_switch_by**.

create_target_proxy

By default, gLExec will setup environment variables pointing to a valid and reachable proxy for the payload user, using the values of the variables GLEEXEC_SOURCE_PROXY and GLEEXEC_TARGET_PROXY or their defaults, see **glexec(1)** for details. By setting this option to 'no' gLExec will ignore these variables, not copy a proxy file and not set the X509_USER_PROXY for the payload user. Default: *yes*.

certdir The value of this option will be set as X509_CERT_DIR environment variable for internal use by LCAS and LCMAPS. If it does not point to an existing and absolute directory it will be ignored.

vomsdir

The value of this option will be set as X509_VOMS_DIR environment variable for internal use by LCAS and LCMAPS. If it does not point to an existing and absolute directory it will be ignored.

use_lcas = {yes,no}

Make use of the LCAS framework or bypass it.

NOTE: for LCMAPS versions < 1.4.23 it is still necessary to have LCAS installed, for later versions of LCMAPS, this restriction is lifted.

Default: *yes*.

lcas_libdir

Directory where to look for the LCAS dynamic libraries. When unset or set to a non-existing and/or relative directory, the default search mechanism for the dynamic linker is used (e.g. ld.so.conf). When set future versions of LCAS will also look for the plugins in the directory <lcas_libdir>/modules.

lcas_db_file

Override the built in location of the LCAS configuration file. Default: */etc/lcas/lcas-glexec.db*.

lcas_log_file

Override the built in location of the LCAS output log file. It can be the same as **lcmaps_log_file**, in which case both LCMAPS and LCAS use the same file to log to. Only used when logging destination is file, see **log_destination**. Default: */var/log/glexec/lcas_lcmaps.log*.

lcas_debug_level = {0,..,5}

Override the built in (debug) log level for LCAS. Default: *0*.

lcmaps_libdir

Directory where to look for the LCMAPS dynamic libraries. When unset or set to a non-existing and/or relative directory, the default search mechanism for the dynamic linker is used (e.g. ld.so.conf). When set versions of LCMAPS >= 1.4.25 will also look for the plugins in the directory <lcmaps_libdir>/modules.

lcmaps_db_file

Override the built in location of the LCMAPS configuration file. Default: */etc/lcmaps/lcmaps-glexec.db*.

lcmaps_voms_verification = {yes,no}

Turn on/off verification of VOMS attributes by LCMAPS versions >= 1.4.21. Default: *yes*.

lcmaps_get_account_policy

Specify one or multiple LCMAPS plugin evaluation policies to be executed. This setting discards all other policies configured in the lcmaps.db file. Use the policy names as written in the lcmaps.db file. In case of multiple policies, use the colon-character as a delimiter (the parsing of this string is performed by LCMAPS, not in gLExec). Example: "vomspolicy:oldstylepolicy"

NOTE: The order of the configured policies is ignored by LCMAPS. The setting "policy1:policy2" is equivalent to "policy2:policy1". The execution order is based on the order in which they appear in the lcmaps configuration file (see **lcmaps_db_file**), which is read from top to bottom.

lcmaps_log_file

Override the built in location of the LCMAPS output log file. It can be the same as **lcas_log_file**. Only used when logging destination is file, see **log_destination**. Default: */var/log/glexec/lcas_lcmaps.log*.

lcmaps_debug_level = {0,..,5}

Override the built in (debug) log level for LCMAPS. Default: *0*.

EXAMPLES

Glexec can be deployed in different scenarios and with each of these scenarios the content of the configuration files involved need to be changed.

Full mode:

The first scenario in which gLExec can be deployed is the most common one and that is where gLExec has set its suid bit and is called full mode. In full mode one can choose to log to syslog or to log to file. It is important that gLExec is installed with the following permissions and ownership:

```
-rws--x--x  1  root   root  12345   2010-02-24  11:07  glexec
-r-----   1  glexec root   123    2010-02-24  11:07  glexec.conf
```

The following example configuration file for gLExec can be use in case of full mode and logging to syslog:

```
[glexec]
silent_logging      = no
log_destination    = syslog
log_level          = 5
user_white_list    = .dteam
linger             = yes
user_identity_switch_by = lcmaps
```

The following example config file can be used for LCAS:

```
pluginname=@moduledir@/lcas_userban.mod,pluginargs=ban_users.db
pluginname=@moduledir@/lcas_voms.mod,pluginargs="-vomsdir /etc/grid-security
```

The following example config file can be used for LCMAPS:

```
path = @moduledir@

poolaccount = "lcmaps_poolaccount.mod"
" -override_inconsistency"
" -gridmapfile <grid-mapfile>"
" -gridmapdir <gridmapdir>"

verify_proxy = "lcmaps_verify_proxy.mod"
" -certdir /etc/grid-security/certificates"

posix_enf = "lcmaps_posix_enf.mod"

glexec_get_account:
verify_proxy -> poolaccount
poolaccount -> posix_enf
```

In case logging to file is wanted, the following slightly altered gLExec configuration file can be used:

```
[glexec]
silent_logging      = no
log_destination    = file
log_file           = /var/log/glexec/glexec.log
log_level          = 5
user_white_list    = .dteam
linger             = yes
user_identity_switch_by = lcmaps
```

The following example config file can be used for LCAS:

```
pluginname=@moduledir@/lcas_userban.mod,pluginargs=ban_users.db
pluginname=@moduledir@/lcas_voms.mod,pluginargs="-vomsdir /etc/grid-security
```

The following example config file can be used for LCMAPS:

```
path = @moduledir@

poolaccount = "lcmaps_poolaccount.mod"
" -override_inconsistency"
" -gridmapfile <grid-mapfile>"
" -gridmapdir <gridmapdir>"

verify_proxy = "lcmaps_verify_proxy.mod"
" -certdir /etc/grid-security/certificates"

posix_enf = "lcmaps_posix_enf.mod"

glexec_get_account:
verify_proxy -> poolaccount
poolaccount -> posix_enf
```

Logging only mode:

gLExec can also run in logging only mode. In this mode gLExec will operate in almost the same manner as in full mode with the difference that the suid bit of gLExec cannot be set. As a result of that, the identity switch can not take place due to missing privileges of the process and as far as logging goes only syslog can be used. Use the following permissions:

```
-rwx--x--x  1  root   root  12345   2010-02-24  11:07  glexec
-r--r--r--  1  glexec root   123     2010-02-24  11:07  glexec.conf
```

In case of the LCMAPS configuration the posix_enf plugin cannot be called as the process now lacks proper privileges to do the identity switching. This means that for the gLExec configuration nothing has to change as compared to the previous examples, but that in case of LCMAPS, the posix_enf plugin needs to be removed.

The gLExec configuration file might look like this:

```
[glexec]
silent_logging      = no
log_destination     = syslog
log_level           = 5
user_white_list     = .glexec
linger              = yes
user_identity_switch_by = lcmaps
```

The following example config file can be used for LCAS:

```
pluginname=@moduledir@/lcas_userban.mod,pluginargs=ban_users.db
pluginname=@moduledir@/lcas_voms.mod,pluginargs="-vomsdir /etc/grid-security
```

The following example config file can be used for LCMAPS:

```
path = @moduledir@

poolaccount = "lcmaps_poolaccount.mod"
```

```

" -override_inconsistency"
" -gridmapfile <grid-mapfile>"
" -gridmapdir <gridmapdir>"

verify_proxy = "lcmaps_verify_proxy.mod"
" -certdir /etc/grid-security/certificates"

posix_enf = "lcmaps_posix_enf.mod"

glexec_get_account:
verify_proxy -> poolaccount

```

Null mode:

This mode has been discussed as one of the modes of gLExec. In this mode gLExec does not even log as opposed to the logging only mode. In this mode gLExec is virtually non existent. Actually, this mode can be implemented by the following script:

```
#!/bin/sh
exec $@
```

and as can be seen, gLExec is completely taken out of the equation and hence there is no need to configure either LCAS or LCMAPS as these libraries will not be called for.

INSTALLATION

NOTE: this section is exclusively valid from gLExec version 0.7 and higher.

The preferred ownership for the gLExec executable is root.root or root.glexec. For the config file, the preferred ownership is glexec.root.

For *switching mode*, the preferred set of permissions for the executable is 4711 and for the config file 0400:

```
-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 *logging only mode*, the preferred set of permissions for the executable is 0711 and for the config file 0444:

```
-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
```

These setups also work when either or both are installed on **NFS** mounts with *root-squash* enabled.

FILES

/etc/glexec.conf

BUGS

LCMAPS has the ability to switch to a different uid through its posix_enf plugin (which is part of the basic plugin set). When this plugin is called from within a privileged environment, it performs the same user identity switching as gLExec does. Versions up to and including 1.3.7 of this posix_enf plugin were too strict in their checking for root capabilities. Since gLExec is not executed as real user root, but only effectively runs as root via its suid bit, the posix_enf plugin up to and including version 1.3.7 will fail. This has been fixed for later versions of the posix_enf plugin.

SEE ALSO

glexec(1), flock(2), fcntl(2), syslog(3) ld.so(8)

<http://www.nikhef.nl/pub/projects/grid/gridwiki/index.php/GLExec>

AUTHORS

Written by Oscar Koeroo & Mischa Sallé (from January 2009)

Written by Gerben Venekamp (until January 2009)

COPYRIGHT

Copyright © 2008-2010 EGEE

Table of Contents

gLExec on WN, CE and anywhere else.....	1
Functional description.....	1
Daemons running.....	1
Init scripts and options (start stop restartl.....)	1
Configuration files location with example or template.....	1
Logfile locations (and management) and other useful audit information.....	1
Open ports.....	1
Possible unit test of the service.....	2
Where is service state held (and can it be rebuilt).....	2
Cron jobs.....	2
Security information.....	2
Access control Mechanism description (authentication & authorization).....	2
How to block/ban a user.....	2
Network Usage.....	2
Firewall configuration.....	2
Security recommendations.....	2
File permissions.....	2
Versions up to 0.6.8-3.....	3
Version 0.7.0-2.....	3
File permission verification.....	3
Security incompatibilities.....	3
List of externals (packages are NOT maintained by Red Hat or by gLite).....	3
Other security relevant comments.....	3
Environment Variables.....	3
Whitelist.....	4
Utility scripts.....	4
Location of reference documentation for users.....	4
Location of reference documentation for administrators.....	4

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 glxec.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 glxec.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 glxec is /var/log/glexec/glexec_log. This can be changed at compile time or altered using the glxec.conf file.

- Syslog available: yes

In the Manual pages of gLExec's glxec.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 outside 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 is 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_* family 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 glxec.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 'glxec'. This will allow the user to continue running gLExec. The other (more advertised) method is to configure the line **user_white_list** in the glxec.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: glxec[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 whitelisted 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: r4 - 15-Apr-2010 - 22:08:12 - OscarKoeroo

 Copyright &© by the contributing authors. All material on this collaboration platform is the property of the contributing authors.

Ideas, requests, problems regarding TWiki? Ask a support question or Send feedback