LHC COMPUTING GRID

LCG - CONFIGURATION AND MANAGEMENT OF THE GRID-MAP-FILE

Document identifier:	**LCG-GIS-MI-GMF**
EDMS id:	**none**
Version:	**v2.0**
Date:	**21-Jun-2004**
Section:	**LCG Grid Infrastructure Support**
Document status:	**ACTIVE**
Author(s):	Antonio Retico, Alessandro Usai Antonio.Retico@cern.ch Alessandro.Usai@cern.ch
File:	**GMF**

Abstract: *Configuration and management of the grid-map-file*

CONTENTS

1. GSI ACCESS CONTROL LIST (GRID-MAPFILE) 4

2. CONFIGURATION OF THE FILE *edg-mkgridmap.conf* 5

2.1. EDIT THE GENERAL CONFIGURATION FILE 5
2.2. EDIT LOCAL ACL FILE 7
2.3. RUN THE SCRIPT 7

3. CONFIGURATION OF THE DAEMON CRON JOB 8

REFERENCES

[1] D. 1.2.8.1. edg-lcas reference manual, 2003. http://www.dutchgrid.nl/DataGrid/wp4/lcas/edg-lcas-1.1/apidoc/latex/ref\%man.pdf

[2] E. DataGrid. Grid-mapfile, 2004. authorization team <sec-grid@infn.it>.

[3] F. Donno and H. Stockinger. Lcg-manual-installation, 2004. Document identifier: CERN-LCG-GDEIS-412774.

[4] L. Poncet. Cvs user guide, 2004. http://grid-deployment.web.cern.ch/grid-deployment/cgi-bin/index.cgi?va\%r=documentation

[5] A. Retico. Lcg manual installation guides, 2004. http://www.cern.ch/grid-deployment/gis/release-docs/MIG-index.html.

[6] A. Retico and A. Usai. Lcg ce manual software installation and configuration, 2004. http://www.cern.ch/grid-deployment/gis/release-docs/CE-index.html

[7] A. Retico and A. Usai. Lcg grid-mapfile handling on lcg nodes, 2004. http://www.cern.ch/grid-deployment/gis/release-docs/GMF-index.html

[8] A. Retico and A. Usai. Lcg ui manual software installation and configuration, 2004. http://www.cern.ch/grid-deployment/gis/release-docs/UI-index.html

[9] A. Retico and A. Usai. Lcg wn manual software installation and configuration, 2004. http://www.cern.ch/grid-deployment/gis/release-docs/WN-index.html

[10] A. Retico, A. Usai, and O. Keeble. Lcg se manual software installation and configuration, 2004. http://www.cern.ch/grid-deployment/gis/release-docs/SE-index.html

1. GSI ACCESS CONTROL LIST (GRID-MAPFILE)

The GSI (Grid Security Infrastructure) makes use of an ACL, the *grid-mapfile* for user authentication purposes.
The grid-mapfile is a plain text file, the purpose of which is to map a GSI (Grid Security Infrastructure) Credential to a local user's login name.
The file

/etc/grid-security/grid-mapfile

must contain, for each user authorized by GSI, a line structured as follows:

```
"<GSI Credential>" .<VOname>
```

the meaning of the attributes above is:

GSI Credential: it is the subject of the user X509 certificate issued by the local GSI administrator. Usually the *usercert.pem* is stored into the */.globus/* directory.
The piece of information in the subject can be directly retrieved from the certificate by the following command:

```
> grid-cert-info -subject -file ~/.globus/usercert.pem
```

<**VOname**>**:** it is the group name by which the VO pertaining to the user is mapped.

Should the holder of the GSI credential be member of more than a VO, additional lines (one for each VO which the user is member of) have to be added to the grid-mapfile.

Some examples of entries in the grid-mapfile follow:

```
"/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=Alessandro Manzoni/Email=alessandro.manzoni@cnaf.infn.it" .dteam
"/O=CESNET/O=Czech Technical University in Prague/CN=Ivan Lendl" .atlas
"/O=Grid/O=CERN/OU=cern.ch/CN=Flash Gordon" .alice
"/O=doesciencegrid.org/OU=People/CN=Jonny B. Good 60237" .dteam
"/O=dutchgrid/O=users/O=sara/CN=Ron Howard" .dteam
```

Since grid-mapfiles resident on different nodes have to be kept synchronized over the whole grid, an automatic mechanism for its update based on ldap has been built. The correct way to set up a grid-mapfile is to edit the *edg-mkgridmap.conf* configuration file and then to schedule the launch of the update tool, as shown in the following sections.

2. CONFIGURATION OF THE FILE *edg-mkgridmap.conf*

2.1. EDIT THE GENERAL CONFIGURATION FILE

The file

/opt/edg/etc/edg-mkgridmap.conf

contains a list of the ldap servers which provide the final users information. These servers are then queried and the information contained in the grid-map-file is checked and updated accordingly. If this file is not configured the grid-map-file will be overwritten with ”default information” from ”default ldap servers” every time the script

/opt/edg/sbin/edg-mkgridmap

is run. Since the script is typically run as a cron job, it is therefore important to edit this file accordingly.
An example of a generic line of the configuration file follows:

```
group ldap://grid-vo.nikhef.nl/ou=lcgadmin,o=lhcb,dc=eu-datagrid,dc=org lhcbsgm
```

The line above identifies a trusted Virtual Organization (VO) which provides a LDAP database of its authorized users. There is a LDAP database for every VO and consequently there should be a similar line for every wanted VO.
The final entry in the line, i.e. ”lhcbsgm” refers to a single authorized user.

However the final entry in the line can be also preceded by a ”.”, e.g.

```
group ldap://lcg-vo.cern.ch/ou=lcg1,o=dteam,dc=lcg,dc=org .dteam
```

which has the effect of making all the *dteam* users be taken, e.g. dteam001, dteam002 etc.

All the allowed directives are the following:

- **group URI [lcluser]**
  Non optional.
  The Group directive has been discussed above. This directive selects the VO directories. *lcluser*, if specified, is the local username to be inserted in the grid-mapfile for the users belonging to the group. If lcluser is not specified, the default local user is implicitly used.
  Specify *AUTO* as *lcluser* or *default_lcluser* for automatic generation of local usernames.
  As already said, specify “.” or “.[PREFIX]” (eg .cms) as *lcluser* or *default_lcluser* to enable dynamic allocation of local usernames (Andrew McNab’s *gridmapdir* patch).

- **default_lcluser** <**lcuser**>
  Optional.
  Defaul user to be used. If <lcuser> is not present the *lcuser* is taken by default to be ”.” .

- **auth URI**
  Optional.
  With auth you can specify an LDAP server URI (Universal Resource Identifier) of an authorized VO.
  If the certificate subject of a user is not present in the authorized VO the user will not be inserted in the *grid-mapfile*. If auth is omitted, this feature is disabled.

- **allow pattern_to_match and deny pattern_to_match**
  Optional.
  Allow and deny directives (which are in the end ACL, i.e. Access Control Lists) may contain wildcards; the test is done on the user certificate subject. Parsing stops at the first match.
  If there is at least an allow, there is an implicit *deny* * at the end, otherwise there is an implicit *allow* *. Parsing is not case sensitive.
  Notice that a directive such as

  *allow *INFN**

  has the effect of allowing everyone from INFN access your site but no one else including you!!!!
  With the ACL commented out, only those users listed by the VO servers in the groups you specify have access.

- **gmf_local grid-mapfile-local**
  Optional.
  With *gmf_local* you can specify a *grid-mapfile-local* useful to add static entries in *grid-mapfile*.
  Altough the parameter is optional, once it has been set up, the specified file has to be provided (maybe void), in order for the configuration tool to work.

If you have doubts about the values to be configured into the files above listed and you have a reference site, please ask them for indications.
Otherwise, send a message to the ”LCG-ROLLOUT@cclrclsv.RL.AC.UK” mailing list.
A template file for */opt/edg/etc/edg-mkgridmap.conf* is provided by the *edg-mkgridmap-conf* rpm. A production example of the configuration file follows:

```
###############################################################################
# EDG Virtual Organisations
# eg 'group ldap://grid-vo.cnaf.infn.it/ou=testbed1,o=infn,c=it .infngrid'

# Map VO members  alicesgm
group ldap://grid-vo.nikhef.nl/ou=lcgadmin,o=alice,dc=eu-datagrid,dc=org alicesgm

# Map VO members  alice
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=alice,dc=eu-datagrid,dc=org .alice

# Map VO members  atlassgm
group ldap://grid-vo.nikhef.nl/ou=lcgadmin,o=atlas,dc=eu-datagrid,dc=org atlassgm

# Map VO members  atlas
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=atlas,dc=eu-datagrid,dc=org .atlas

# Map VO members  cmssgm
group ldap://grid-vo.nikhef.nl/ou=lcgadmin,o=cms,dc=eu-datagrid,dc=org cmssgm

# Map VO members  cms
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=cms,dc=eu-datagrid,dc=org .cms
```

```
# Map VO members  lhcbsgm
group ldap://grid-vo.nikhef.nl/ou=lcgadmin,o=lhcb,dc=eu-datagrid,dc=org lhcbsgm

# Map VO members  lhcb
group ldap://grid-vo.nikhef.nl/ou=lcg1,o=lhcb,dc=eu-datagrid,dc=org .lhcb

# Map VO members  dteamsgm
group ldap://lcg-vo.cern.ch/ou=lcgadmin,o=dteam,dc=lcg,dc=org dteamsgm

# Map VO members  dteam
group ldap://lcg-vo.cern.ch/ou=lcg1,o=dteam,dc=lcg,dc=org .dteam

###############################################################################
# List of auth URIs
# eg 'auth ldap://marianne.in2p3.fr/ou=People,o=testbed,dc=eu-datagrid,dc=org'
# If these are defined then users must be authorized in one of the following
# auth servers.

# A list of authorized users.
auth ldap://lcg-registrar.cern.ch/ou=users,o=registrar,dc=lcg,dc=org

###############################################################################
# DEFAULT_LCLUSER: default_lcluser lcluser
# default_lcuser .

###############################################################################
# ALLOW and DENY: deny|allow pattern_to_match
# allow *INFN*

###############################################################################
# Local grid-mapfile to import and overide all the above information.
# eg, gmf_local /opt/edg/etc/grid-mapfile-local

gmf_local /opt/edg/etc/grid-mapfile-local
```

2.2. EDIT LOCAL ACL FILE

The file

/opt/edg/etc/grid-mapfile-local

may be used as a local access control list. This list will then be imported in the local mapfile by the *edg-mkgridmap* utility.
The syntax to edit the above file is the one described in 1..

A template for the file */opt/edg/etc/grid-mapfile-local* is provided by the *edg-mkgridmap* rpm.

WARNING: if the *gmf_local* variable is used in configuration (see 2.1.), the file */opt/edg/etc/grid-mapfile-local* MUST be created, or the creation script (see 2.3.) will not work.
If you need the local ACL set up this feature, altough you so not have entries yet to put in. You can just copy the template in order to have the configuration working.

```
> cp /opt/edg/etc/grid-mapfile-local.template /opt/edg/etc/grid-mapfile-local
```

2.3. RUN THE SCRIPT

```
> /opt/edg/sbin/edg-mkgridmap > /etc/grid-security/grid-mapfile
```

in order to generate the *grid-makefile*.

3. CONFIGURATION OF THE DAEMON CRON JOB

Edit the crontab

```
> crontab -e
```

and add the following line:

```
26 1,7,13,19 * * * /opt/edg/sbin/edg-mkgridmap --output=/etc/grid-security/grid-mapfile --safe
```

CHANGE HISTORY

The details in the History concerning version numbers before 2.10 have been removed for readability reasons. They can be retrieved, if needed, from the version 2.9 of this document

Table 1: Change History

version	*date*	*description*
v1.0	2/Feb/04	First Release
v1.1	2/Feb/04	
v1.2	6/Feb/04	
v1.3	9/Feb/04	
v1.4	1/Mar/04	2.1. use of *gmf_local* parameter improved
v1.5	1/Mar/04	2.3. output redirected
v1.6	1/Apr/04	cvs references changed
v2.0	21/Jun/04	Document re-styling