LCMAPS (and VOMS) integration for Globus services

D. H. van Dok (Nikhef) and M. Sallé (Nikhef)

2013-04-09

LCMAPS (and VOMS) integration for Globus services

This is a demonstration of the installation of Globus services with VOMS based authentication and accounting, using the LCMAPS framework. The integration with the Globus GSI authorization callout was the focus of our work in the IGE project, and some key results are highlighted here.

About this training

This training is aimed at people who wish to set up Globus Toolkit services such as GridFTP and GSI-SSH and make use of the flexible mapping options of the LCMAPS framework, which includes support for VOMS.
Because time is short this will not be a hands-on, installation from scratch; some of this material was prepared in advance.

Basic system installation

This presentation is based on a CentOS 6 machine.
It is *nearly* the same for CentOS 5 or Debian.

Configuration of software repositories

- **IGE 3**
  See
  http://www.ige-project.eu/downloads/software/releases/downloads
  Unfortunately no ready-made repo file. Just copy & paste from the website.
- **EGI trustanchors (a.k.a. the IGTF CA distribution)**
  `cd /etc/yum.repos.d/ && wget`
  http://repository.egi.eu/sw/production/cas/1/current/repo-files/EGI-trustanchors.repo
- **EPEL**
  `rpm -i`
  http://download.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm

- importing the gpg keys
  `rpm --import` http://repo-rpm.ige-project.eu/RPM-GPG-KEY-IGE
  `rpm --import` http://repository.egi.eu/sw/production/cas/1/GPG-KEY-EUGridPMA-RPM-3

Installation of services and middleware

```
yum -y install ca_policy_igtf-{classic,mics,slcs}
yum -y install gsi-openssh-server
yum -y install globus-ftp-server-progs
```

Host certificate

Installed (of course) in

`/etc/grid-security/host{key,cert}.pem`

Make sure the **key** is mode `-r--------`.

Configuration files

Grid mapfile in

```
/etc/grid-security/grid-mapfile
```

with user's DN and local account.
Set the default port of gsissh:

```
sed -i 's/#Port 22/&\nPort 2200/' /etc/gsissh/sshd_config
```

Ready to roll!

(demo)

LCMAPS installation

```
yum install lcas-lcmaps-gt4-interface
gt4-interface-install.sh install
yum install lcmaps-plugins-basic lcmaps-plugins-voms
```

Add lines to the /etc/sysconfig/globus-gridftp-server

```
export LLGT_RUN_LCAS=no
export LLGT_LIFT_PRIVILEGED_PROTECTION=1
```

Add more lines to /etc/sysconfig/gsisshd

```
export LLGT_RUN_LCAS=no
export LLGT_LIFT_PRIVILEGED_PROTECTION=1
```

```
/etc/init.d/gsisshd restart
/etc/init.d/globus-gridftp-server restart
```

VOMS FQAN mapping

Extend the grid-mapfile with the FQANs for the supported VOs.

```
cat >> /etc/grid-security/grid-mapfile <<EOF
"/ige-project.eu" .egcf
"/ige-project.eu/*" .egcf
EOF
```

Setting up pool accounts

```
groupadd -g 9000 egcf
mkdir /etc/grid-security/gridmapdir
for i in `seq -f "%02g" 0 99` ; do
    useradd -g egcf -N -u 90$i egcf$i
    touch /etc/grid-security/gridmapdir/egcf$i
done
```

VOMS server identity

Put the LSC file in /etc/grid-security/vomsdir/ige-project.eu/

```
mkdir /etc/grid-security/vomsdir/ige-project.eu
cat > /etc/grid-security/vomsdir/ige-project.eu/\
  vomrs01.grid.tu-dortmund.de.lsc <<EOF
/C=DE/O=GermanGrid/OU=TU-Dortmund/CN=vomrs01.grid.tu-dortmund.de
/C=DE/O=GermanGrid/CN=GridKa-CA
EOF
```

LCMAPS policies (basic)

```
good = "lcmaps_dummy_good.mod"

vomspoolaccount  = "lcmaps_voms_poolaccount.mod"
    "-gridmapfile /etc/grid-security/grid-mapfile"
    "-gridmapdir /etc/grid-security/gridmapdir"

default:
vomspoolaccount -> good
```

(demo)

LCMAPS policies (add fallback)

We've lost our original mapping to the local user account. But with an extra policy line we can get it back.

```
localaccount = "lcmaps_localaccount.mod"
    "-gridmapfile /etc/grid-security/grid-mapfile"

default:
vomspoolaccount -> good | localaccount
localaccount -> good
```

(demo)

LCMAPS policies (add banning)

Banning used to be done by LCAS, but LCMAPS has a plug-in for that.

```
bandn = "lcmaps_ban_dn.mod"
        "-banmapfile /etc/grid-security/ban_users.db"

default:
bandn -> vomspoolaccount
vomspoolaccount -> good | localaccount
localaccount -> good
```

Add a DN to the `ban_users.db`

(demo)

Additional policy options (skip)

- (Secondary) group mapping based on VOMS
- Banning based on FQANS (e.g. VOMS subgroup)
- ARGUS call-out
- ... much more

Customizing the logging

Logs go to syslog, but the default log level is limited to notices, warnings and errors. If something goes wrong and debugging is needed, add the following:
`/etc/sysconfig/globus-gridftp-server:`

```
export LCMAPS_DEBUG_LEVEL=5
export LLGT_LOG_FACILITY=LOG_LOCAL5
```

(Specifically for CentOS 6:)

```
# rate limiter bites us
cat > /etc/rsyslog.d/lcmaps.conf <<'EOF'
local5.*   /var/log/lcmaps.log
$SystemLogRateLimitInterval 2
$SystemLogRateLimitBurst 1000
EOF
```

Additional debugging tools

Install the llrun tool
rpm -i http://software.nikhef.nl/dist/mwsec/rpm/epel6/x86_64/llrun-0.1.3-1.el6.x86_64.rpm
(demo)

Wrapping up

- LCMAPS can be set up in many, many ways to accomodate almost every imaginable (and unimaginable) policy.
- https://wiki.nikhef.nl/grid/Site_Access_Control
- Just ask! grid-mw-security-support@nikhef.nl