

EGEE tutorial for administrators

Bologna, June 06-08 2007

Site setup using AFS pool account users

C. Sciò, G. Bracco, A. Santoro

ENEA INFO, C.R. ENEA Frascati
V. E. Fermi 45 Frascati ROMA (Italy)
bracco@frascati.enea.it

Reference

[1] <http://www.afs.enea.it/project/eneaegee/html/>

[2] EGEE Technical Note EGEE-TR-2006-006
"AFS Pool Account Users - GSSKLOG and
LCMAPS extension to support AFS users as
EGEE pool account users" Bracco, G;
Giammarino, L; Migliori, S; Sciò, C.

<http://doc.cern.ch/archive/electronic/egee/tr/egee-tr-2006-006.pdf>

Outline

- Requirement
- AFS Users as Pool Account Users:
modified software components for compatibility with AFS
 - Token required for locally mapped users: **lcmaps**
 - Token granting for VO users: **gssklog/gssklogd**
- Modified yaim functions

Requirement

- Usual INFN-grid installation.
- Standard SLC OpenAFS packages.
- The patched lcms_afs module.
- The patched gssklog-0.11 package.
- k5start package to perform cron jobs
- Some modified yaim functions.

We assume that OpenAFS has been installed correctly.

lcmaps_afs modules (1)

LCAS [Local Centre Authorization Service] and **LCMAPS** [Local Credential Mapping Service] are the **EGEE services** that make the connection between GRID users certificates and local UNIX userids on the local site. The systems support:

- The standard globus X509 certificate
 - **gridmap file**: [*distinguished_name local_userid*]
"/O=dutchgrid/O=users/O=sara/CN=Dutch User" griduser
- The extension of X509 certificate holding VO information [VOMS service]
 - **gridmap file**: [*VO_data voms_pool_account_prefix*]
"/VO=enea/GROUP=/enea" .enea

"voms pool account": predefined local users which are dynamically assigned to the members of the VO when running job on the site.
[e.g. for VO **enea** pool users are **enea001**, **enea002**, ..., **enea020**]

pool accounts can be used also with standard X509 certificates:
"/O=dutchgrid/O=users/O=sara/CN=Dutch User" .dteam

lcmaps_afs modules (2)

LCMAPS [Local Credential Mapping Service] is a modular service.

A **lcmaps_afs** module exists with the purpose to obtain an AFS tokens for the local mapped user using gssklog but **the standard module is not compatible with VOMS** “pool account”

A modified module has been prepared to achieve compatibility:
gssklog is invoked always with -principal parameter

Note: due to the software architecture of the CE the relevant user processes on the CE can not be started in the same PAG shell; in fact they are managed by two independent services:

- **authorization and user mapping** are managed by lcas/lcmaps

The reliability of a “**user based**” token instead that a “PAG based” token is delegated to the CE middle-ware architecture.

gssklogd/gssklog (1)

Gssklog package has been developed by Doug Engert (ANL) to obtain an AFS token using a GSS [Generic Security Service] implementation.

It has been used together with Globus Toolkit GSSAPI to obtain an AFS token from a X509 certificate.[ftp://achilles.ctd.anl.gov/pub/DEE](http://achilles.ctd.anl.gov/pub/DEE)

The package include a daemon: [gssklogd] and a client [gssklog].

gssklogd runs on a server where the AFS cell keyfile is available and requires a service certificate and key. A map file is also required [/etc/grid-security/afsgrid-mapfile](#) containing the **X509 distinguished name** and the **AFS userid(s)**:

["/O=Grid/O=Globus/OU=anl.gov/CN=John Doe" jdoe,altuser](#)

The client **gssklog** requires the proxy file generated by the globus command **grid-proxy-init**; an AFS token is obtained by the command:

gssklog -server [server_address](#) -principal jdoe

gssklogd/gssklog (2)

EGEE uses of an extension of X509 certificate to hold VO information [VOMS] and the proxy is generated using command:

`voms-proxy-init -voms VO_name`

gssklogd has been modified to provide tokens for **pool account users** on the basis of the content of the VO information contained in the user certificate. The daemon requires now also the VO certificate.

The **afsggrid-mapfile** syntax has been extended, e.g. for ENEA VO:

`"/VO=enea" .enea/020/`

The client **gssklog** provides always the principal name:

`gssklog -server server_address -principal enea004`

Some users requires pool account without having VOMS extension

`"/O=dutchgrid/O=users/O=sara/CN=Dutch User" .dteam`

gssklogd/gssklog (3)

New information are required by the patched version of the gssklogd daemon:

- The name of a directory containing the certificates of the Virtual Organizations

provided by a new argument parameter [-V]

- The syntax of the afsgrid-mapfile has been extended to include VO and pool accounts

`"/VO=enea" .enea/020/`

After `ig_update 24` sgm users are not (yet) supported

Cron Jobs (1)

We need to perform cron jobs in AFS space to:

- Update certificates in AFS space
- Update modified gridmap-file for gssklogd
- Perform all root operations that handle users home directories

Cron Jobs (2)

How cron jobs securely acquire an AFS token inside a pagsh?

We use Russ Allbery's k5start

- Create an AFS cron_user in PTS
- Add cron_user to the appropriate AFS ACLs
- Create a keytab file readable locally only by cron_user
- `k5start -qtU -f cron_user.keytab cronjob.sh`

Modified Yaim Functions

Modifications are needed to maintain compatibility with different ig-node-info.def profiles.

Add a new metapackage could be a better solution.

- config_add_glite_env
- config_lcmaps
- config_users

It's possible to replace nfs filesystem use with afs one.

- config_nfs_sw_dir_client (optional)
- config_nfs_sw_dir_server (optional)

Config_users

- 1) Takes care to create groups and users for the grid accounts. But users are already configured globally on AFS. Local /etc/passwd is automatically updated on all nodes by Enea-grid middleware.
- 2) Insert into the cron service a modified invocation of the "cleanup-grid-accounts.sh"

Config_add_glite_env

Add glite_setenv.sh to all pool accounts.
Needed only once per user.

Config_lcmaps

A modified config_lcmaps is needed to generate
a correct LCMAFS policyfile lcmaps.db

Status

- An EGEE Technical Note has been written and submitted to JRA1: Title “AFS Pool Account users”
- The patched source of lcms_afs module [lcmaps_afs.c] is available
- A patch to the standard gssklog-0.11 package is available.
- The patch to gssklog package has been presented to the AFS Best Practices Workshop 2006 [<http://pmw.org/afsbpw06>] and submitted to Doug Engert.
- EGEE,06 Conference, Geneva 25-29/9/2006 "AFS pool account users and GRID interoperability"

Bibliography

[1] <http://www.afs.enea.it/project/eneaegee/html/>

[2] ENEA & EGEE Software page:

<http://www.afs.enea.it/project/eneaegee/software/index.html>

[3] EGEE Technical Note EGEE-TR-2006-006 "AFS Pool Account Users - GSSKLOG and LCMAPS extension to support AFS users as EGEE pool account users" Bracco, G; Giammarino, L; Migliori, S; Sciò, C.

<http://doc.cern.ch/archive/electronic/egee/tr/egee-tr-2006-006.pdf>

[4] LCAS/LCMAPS packages, <http://www.nikhef.nl/grid/lcaslcmaps>

http://www.dutchgrid.nl/DataGrid/wp4/lcmaps/edg-lcmaps_gcc3_2_2-0.0.23

[5] GSSKLOG package, D. Engert

<ftp://achilles.ctd.anl.gov/pub/DEE/gssklog-0.11.tar>

[6] K5START manual pages:

<http://www.eyrie.org/~eagle/software/kstart/k5start.html>