

*EU-IndiaGrid Workshop
Taipei, November 2nd 2007*

The ENEA gateway approach providing EGEE/gLite access to unsupported platforms and operating systems

G. Bracco, S. Migliori, A. Quintiliani, A. Santoro, C. Sciò (*)

bracco@frascati.enea.it

C.R. ENEA Frascati, V. E. Fermi 45 Frascati ROMA (Italy)

(*) Esse3Esse, Roma, Italy

Outline

- ENEA-GRID and EGEE/EGEEII: a gateway implementation providing **access to AIX** resources from the EGEE infrastructure
- Status of ENEA-INFO, the ENEA EGEE site
- Can the same approach be applied in other contexts?
 - how to implement the ENEA gateway approach when OpenAFS is not available in the local site
- Conclusions

Annex: technical details about authentication/authorization issues, related to AFS compatibility

ENEA

[Italian National Agency for New Technologies, Energy and Environment]

12 Research sites and a **Central Computer and Network Service** (ENEA-INFO) with **6 computer centres** managing multi-platform resources for serial & parallel computation and graphical post processing.



ENEA GRID

INFO-ENEA computational resources:

- **Hardware**: ~100 hosts and ~650 cpu : IBM SP; SGI Altix & Onyx; Linux clusters 32/ia64/x86_64; Apple cluster; Windows servers. Most relevant resources: IBM SP5 192 cpu; 3 frames of IBM SP4 96 cpu
- **Software**: commercial codes (fluent, ansys, abaqus..); elaboration environments (Matlab, IDL, SAS..)

ENEA GRID [<http://www.afs.enea.it/project/eneagrid>] mission:

- provide an **unified user environment** and a homogeneous access method for all ENEA researchers, irrespective of their location.
- optimize the utilization of the available resources

ENEA GRID architecture

GRID functionalities (unique authentication, authorization, resource access and resource discovery) are provided using “mature”, multi-platform components:

Distributed File System: **OpenAFS**

Resource Manager: **LSF Multicluster [www.platform.com]**

Unified user interface: **Java & Citrix Technologies**

These components constitute the ENEA-GRID Middleware.

OpenAFS

- user homes, software and data distribution
- integration with LSF
- user authentication (Kerberos 5) /authorization

ENEA EGEE site implementation (1)

ENEA activity in EGEE has been focused:

- ◆ on providing access to AIX resources in a framework of interoperability with ENEA-GRID
- ◆ on minimizing the invasiveness of the GRID middle-ware on the hosting infrastructure
- ◆ on minimizing the firewall requirements for Worker Nodes

This resulted in the following targets for the ENEA EGEE site implementation:

- ◆ Provide access to the main ENEA-GRID resources, not to a small subset of dedicated machines
- ◆ EGEE users => mapped to standard dedicated ENEA-GRID AFS users, (required a solution for the authentication interoperability)
- ◆ Access to AIX platform => **NO Middleware on Worker Nodes**

ENEA EGEE site implementation (2)

Implementation architecture:

- ◆ UI & SE: Linux, Standard EGEE/gLite configuration
- ◆ CE: Linux, a few modifications to implement the “gateway” setup
- ◆ A “Proxy WN” - a Linux machine with standard WN packages installed
- ◆ WN: any platform/OS with support for AFS/LSF
 - WN share user homes with CE/Proxy WN using AFS
 - WN delegate all grid commands concerning file transfer to/from GRID to the Proxy WN by means of the LSF **lsrun** command.
 - AFS security and quota management guarantees reliability
- ◆ Many proxy WNs can be defined for scalability issues, if required
- ◆ WN can be completely behind a firewall; only the other elements (CE, SE, UI) and the proxy WN must be in a DMZ

ENEA EGEE site implementation (3)

How:

- ♦ Any WN middleware command concerning file transfer is wrapped with a `lsrun` script.
- ♦ The wrapped WN middleware is located in AFS.
- ♦ The relevant PATHs in the environment of the EGEE job on the WN are modified so that the wrapped middleware is used
 - LSF job-starter script for the EGEE dedicated queues
- ♦ EGEE GRID users require an AFS token:
 - gssklogd modified to be compatible with EGEE middleware
 - EGEE middleware on the CE must properly call gssklog.

EGEE Standard site layout

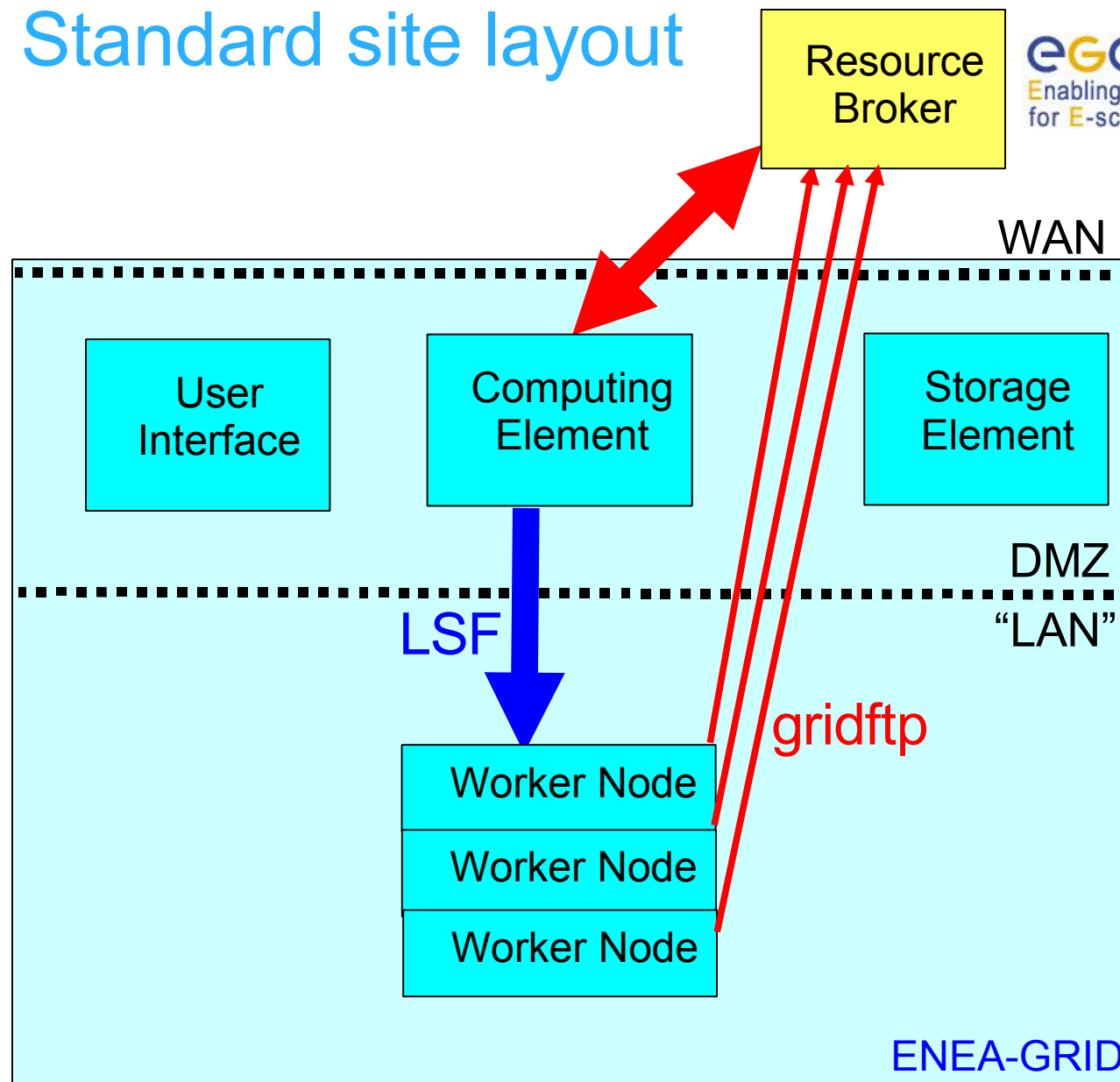
egEE
Enabling Grids
for E-science

User Interface

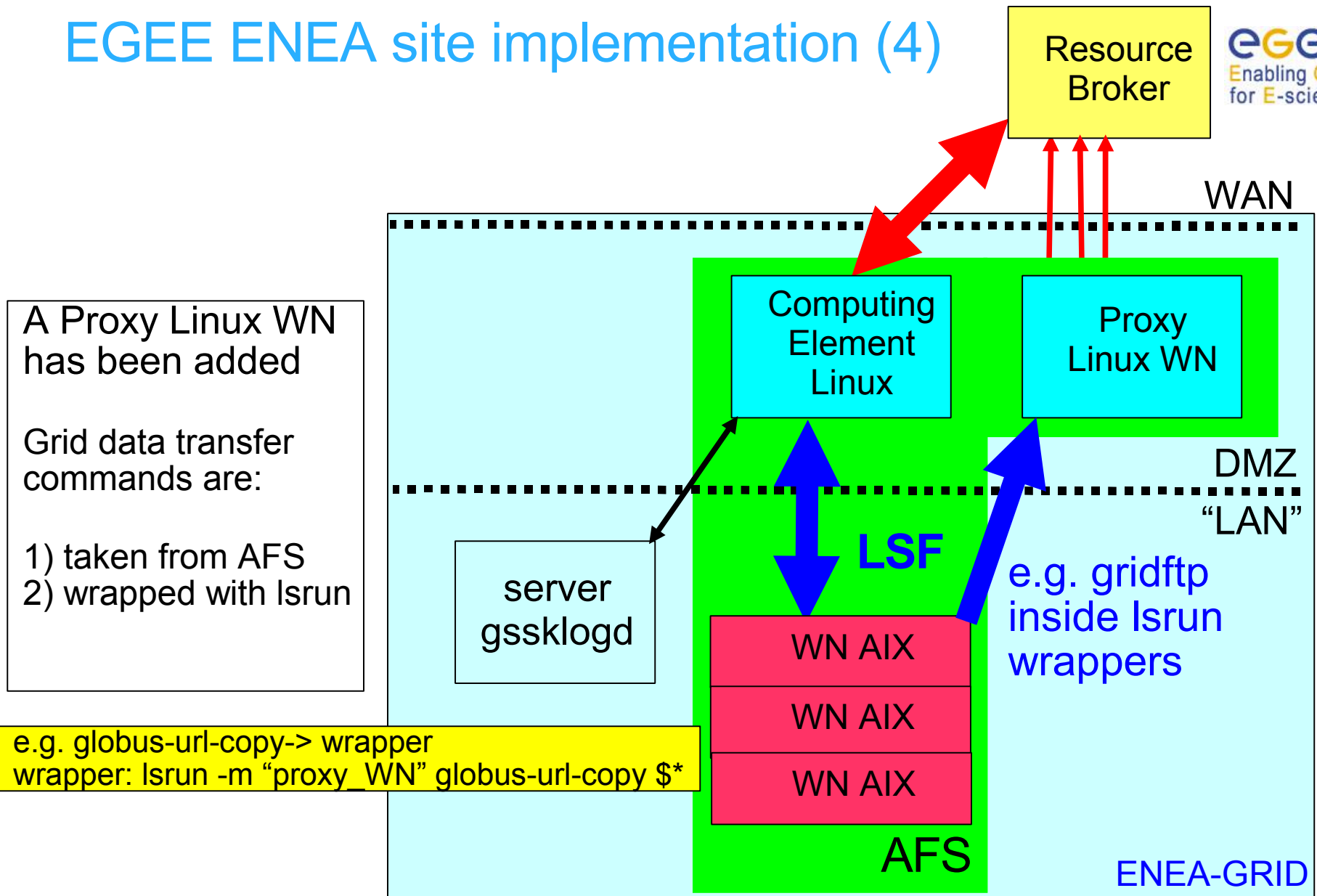
Storage Element

Computing Element: accepts jobs sent by the RB and submits them to the local batch system (LSF)

Worker Nodes: they perform the computation and the WN middleware sends back job results to RB



EGEE ENEA site implementation (4)



EGEE ENEA site implementation: status

ENEA site: Glite 3.0 certified in the production GRID both for Linux & AIX

CE for Linux WN: egce.frascati.enea.it

WN: 14 Linux P4, 1.8 Ghz, 1 GB

CE for AIX WN: egceaix.frascati.enea.it

WN: 96 cpu AIX SP4, 1.9 Ghz, 1GB/cpu

Documentation:

EGEE Technical Note EGEE-TR-2007-001

"The gateway approach providing EGEE/gLite access to non-standard architectures"

Bracco, G; Migliori, S; Sciò, C. ; Santoro , A.;

<http://doc.cern.ch/archive/electronic/egee/tr/egee-tr-2007-001.pdf>

LIMITS of the gateway approach

- **Not a completely standard site** [but EGEE Certification job runs well]
 - GRID API are not available
 - Some WN monitoring components are unavailable

Can the same gateway approach be applied in other contexts? YES

The ENEA gateway approach is based on:

1) the availability of **a shared file system** on the site WN and on the GRID proxy WN:

- The ENEA gateway implementation takes advantage on the OpenAFS availability in ENEA-GRID infrastructure
- The same result can also be achieved using other shared file system, as NFS or GPFS (standard UNIX file systems: **no authentication/authorization issues as in the case of OpenAFS!**)

2) the adoption of **a remote execution tool** for the implementation of the wrapped GRID commands:

- The ENEA gateway implementation makes use of the lsruncmd command of LSF
- The same result can also be achieved using other remote execution commands, e.g. rsh or ssh

Conclusion

- The ENEA gateway approach has been successfully applied to provide EGEE/gLite access to **AIX resources** belonging to ENEA-GRID, an infrastructure based on AFS and LSF
<http://www.afs.enea.it/project/eneaegee>
- The approach can be applied (and it has already also been tested in ENEA) for **other platforms** still unsupported by gLite middle-ware and it is now included on the Web page of EGEE porting activity: <http://grid.ie/porting> ref. AIX
- **The same approach can also be applied in other contexts**, where AFS & LSF are not available, by using other standard tools as NFS and ssh. The implementation in that case is even simpler, as the authentication and authorization issues due to AFS do not arise.

Annex

The following slides describe the details of the components that have been modified to solve the authentication/authorization problems in the implementation of the interoperability between EGEE infrastructure and ENEA-GRID:

- lcms
- gssklog/gssklogd package.

Annex: lcms (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

Annex: Lcmaps (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
- **job submission** is managed by the edg-gatekeeper

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

Annex: 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>

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

Annex: 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
```

Annex: conclusion

- Documentation: an EGEE Technical Note

EGEE Technical Note EGEE-TR-2006-006

"AFS Pool Account Users"

Bracco, G; Giammarino, L; Migliori, S; Sciò, C.;

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

- 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.