Contribution ID: **14** Type: **demo presentation**

Secure Storage

Wednesday 9 May 2007 19:30 (20 minutes)

Describe the scientific/technical community and the scientific/technical activity using (planning to use) the EGEE infrastructure. A high-level description is needed (neither a detailed specialist report nor a list of references).

The scientific and technical community using the EGEE
infrastructure and
involved in the Secure Storage project is composed by a public
research centre,
INFN, and a private company, UNICO S.R.L. (http://www.unicosrl.it/).
The aim of the activity is to design a secure storage service.
This means to
create a mechanism to store in a secure way and in an encrypted
format the
data deployed on the grid storage elements. This stored data will
be accessible
and readable only by their owners.

Report on the experience (or the proposed activity). It would be very important to mention key services which are essential for the success of your activity on the EGEE infrastructure.

A secure version of some lcg-utils commands and a keystore
service has been
developed:
lcg-scr: encrypts a file and uploads it on a storage element,
registering its
Logical File Name in a LFC catalog. Moreover, it stores the key
used to encrypt
the file in the keystore. An ACL will be associated to each key
on the repository.
This ACL will contain all users authorized to access the file.
lcg-scp: downloads an encrypted file, gets the key to decrypt the
file from the
keystore, decrypts the file and then store it on a local
file-system.
The keystore service stores the key and the associated ACL
received by the lcg-
scr commands on its repository and provides the key to the
lcg-scp command.
The communications between the commands and the keystore is
established on
a secure GSI authenticated channel. The keystore provides the key
to the lcg-
scp command only if the request is coming from an authorized user
(thanks to
the GSI authentication, it knows the distinguished name of the user).

With a forward look to future evolution, discuss the issues you have encountered (or that you expect) in using the EGEE infrastructure. Wherever possible, point out the experience limitations (both in terms of existing services or missing functionality)

The main issues encountered in using the EGEE infrastructure
during the
development of the secure storage service are the following:
We cannot use the last version (and then more secure) of the
OpenSSL library
for a library conflict with OpenSSL version used by Globus.
The development of a GSI Client in C language was been hard. The
Globus GSI
API are not very intuitive.

Describe the added value of the Grid for the scientific/technical activity you (plan to) do on the Grid. This should include the scale of the activity and of the potential user community and the relevance for other scientific or business applications

One of the main benefit of the Grid Infrastructure is the
possibility to use
distributed storage space. A community could want to use storage
elements
owned by an external organization to delegate the management of this
machines and to avoid to buy specialized hardware. In this way
the community
could rent the storage space as needed and minimize human and
hardware
costs.
In the case of confidential data this scenario is not feasible.
Indeed, the
community should satisfy strongly privacy requirements, as in the
case, for
example, it have to manage medical or financial data. To store
the confidential
data in a storage element managed by an external organization a
mechanism
to prevent the administrator of the machine accessing the data is
required.
This is the “insider abuse”problem and the Secure Storage
project provides a
solution to this problem.

Authors: Dr SCARDACI, Diego (INFN Catania); Mr SCUDERI, Giordano (UNICO S.R.L.); Dr CALANDUCCI, Tony (INFN Catania)

Presenter: Dr SCARDACI, Diego (INFN Catania)

Session Classification: Poster and Demo Session