EGEE User Forum

Contribution ID: **65** Type: **Oral contribution**

G-PBox: A framework for grid policy management

Thursday 2 March 2006 17:00 (30 minutes)

Sharing computing and storage resources among multiple Virtual Organizations which group people from different institutions often spanning many countries, requires a comprehensive policy management framework.
This paper introduces G-PBox, a tool for the management of policies which integrates with other VO-based tools like VOMS, an attribute authority and DGAS an accounting system, to provide a framework for writing, administering and utilizing policies in a Grid environment.

Summary

Introduction
One of the most innovative concept of Grid computing is the Virtual Organization (VO) which represents a distributed community of users sharing a common goal.
The VO is key to administering the allocation of grid resources and data access but is also influencing all aspects of the Grid environment from authentication and authorization to accounting. It has, for example, been included in the attributes of the user certificate.
VOs and resource owners share contracts to regulate resource usage. These contracts or policies can be difficult to enforce or manage just by formal agreements and some institutions might be reluctant to participate in collaborative efforts because of the lack of an automatic enforcement of policies.

G-PBox
Current Grid middleware software allows resource owners control over their own resources only. It is necessary that VO administrators are able to issue agreements on resource usage with resources owners.
G-PBox helps manage the administrative domain of a VO (but also the domain of a resource owner), storing all policies concerning the domain itself.
A distribution mechanism allows policies to be delivered to their intended targets and repositories to be synchronized.

G-PBoxes form a network which allows the creation of policies on any administrative domain.
An authoritative mechanism permits to grant a domain control over other domains.
Policies are described in the XACML language, a high level language for encoded data exchange.
The actual usability by G-PBox of a specific category of policies may depend on the availability of external information such as the ones provided by an accounting tool or an information system. The communication with these external tools is performed through a plug-in mechanism.

G-PBox INTERNAL interactions
G-PBox interacts with resource owners and VOs through a Policy Enforcement Point (PEP).
PEPs have been implemented for the LCG Resource Broker (RB) and the LCG Computing Element (CE) using the LCAS/LCMAPS plugin technology.

A PEP for a LCG Storage Element (SE) should use the same CE LCAS plugin features.
An example of interaction with the RB is how to apply policies to the matchmaking process performed by the resource broker (RB). The first such request we got was to have a RB capable of splitting resources in a series of classes, each with its own priority, and then split job assignment to resources based on such priority and the user's VOMS credentials.
The chosen solution was to require a resource to publish a tag describing their class in the information system , and then write policies associating a specific group/role combination to a class of resources. At this point, the PEP plugin for the RB only had to contact the G-PBox and provide it with the following parameters: the action (job-submission), the credentials of the user and a list of suitable resources, each with its associated tag. It would then obtain as a result a set of allow/deny answers for each resource describing whether the user was allowed to submit a job or not.
Another PEP we implemented was a PEP for the Computing Element (CE), whose job was to take over grid user mapping to local accounts based on given policies.

G-PBox EXTERNAL interactions
Among the external components required or necessary for the implementation of a specific feature, we can underline:
- VOMS: An attribute authority, is a required component for the basic functionality of G-PBox
- DGAS or any other accounting system is necessary to implement policies which need accounting data

VOMS handles the authorization part of the security mechanism allowing a user to provide authorization data as she tries to access a resource provider. The type of data VOMS handles is information about a user's relationship with the virtual organizations she belongs to. This information is described by VOMS using the concept of groups a user belongs to, roles a user is allowed to impersonate and capabilities a user should present a resource provider for special processing needs.
DGAS implements Resource Usage Metering, Accounting and Account Balancing (through resource pricing) in a distributed Grid environment. Accounting requires accurate Usage Metering which is performed by lightweight sensors installed on the Computing Elements.

FUTURE plans
G-PBox is a relatively young tool and is still in the development process. The first testing experience of the G-PBox framework, related to different groups of a VO and enforced by a Grid Resouce Broker and checked by the CEs, demonstrated the effectiveness of such an approach. Other policies, like CPU fair sharing and storage quota management, have been required and are going to be implemented.
The current G-PBox v1.0 is included in the gLite distribution from release 1.5.

References

[1] V. Ciaschini, A. Ferraro, A. Ghiselli, G. Rubini, R. Zappi, A. Caltroni. G-PBox: a policy framework for Grid environments. In Proceedings CHEP04, September 2004.
[2] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A . Frohner, A. Gianoli, K. Lorentey, F. Spataro. VOMS, an Authorization System for Virtual Organizations. 1st European Across Grids Conference, Santiago de Compostela, February 13-14, 2003.
[3] A. Guarise. DataGrid Accounting System - Architecture v 1.0. DataGrid-01-TED-0126-1_0 - Feb. 14, 2003.
[4] OASIS eXtensible Access Control Markup Language (XACML)Version2.0, http://www.oasis-open.org/ committees/tc_home.php?wg_abbrev=xacml
[5] The Distributed Grid Accounting System (DGAS), http://www.to.infn.it/grid/accounting/main.html
[6] VOMS at INFN Authorization Working Group, http://grid-auth.infn.it
[7] The G-PBox Home Page at INFN, http://infnforge.cnaf.infn.it/gpbox

Primary authors: Mr CALTRONI, Andrea (INFN); Mr FERRARO, Andrea (INFN-CNAF)

Co-authors: Mrs GHISELLI, Antonia (INFN-CNAF); Mr RUBINI, Gian Luca (INFN-CNAF); Mr CIASCHINI, Vincenzo (INFN-CNAF)

Presenter: Mr CALTRONI, Andrea (INFN)

Session Classification: 2a: Workload management and Workflows

Track Classification: Workload management and Workflows