AN INTEGRATED FRAMEWORK FOR VO-ORIENTED AUTHORIZATION, POLICY-BASED MANAGEMENT AND ACCOUNTING

V. Ciaschini, A. Ferraro, A. Ghiselli, G. Rubini, INFN-CNAF, Bologna, Italy
A. Guarise, G. Patania, R. M. Piro, INFN-TO, Torino, Italy
A. Caltroni, INFN-PD, Padova, Italy

Abstract

One of the most interesting challenges of ’Grid computing’ is how to administer resources allocation and data access, in order to obtain optimized computing performance and secure data access. To reach this goal, a entity has appeared, the Virtual Organization (VO), which represents a distributed community of users, accessing a distributed computing environment. This concept has affected all the proposed models for the administration of authentication, authorization policies and accounting, and the users’s VO membership has already become an attribute of the user certificate traveling in the Grid.

This paper describes the architecture of an integrated framework, based on the Virtual Organization Membership Service (VOMS) [1] [2], Grid Policy Box (G-PBox) [3] [4] and Distributed Grid Accounting System (DGAS) [5] [6], providing respectively authentication, policy-based authorization and accounting. It shows how a VO can build groups of users, assign roles and associate policies and quotas to each group and role in a dynamic way, and implement the agreements with the resource owners. Then we descibe how these integrated systems can collaborate in a Grid (gLite/LCG) [7] [8] and how they are used by the Workload Management System (WMS) [9] operating in EGEE [10] is described.

This integrated framework of a VO-based approach to authorization, policy management and accounting aims an efficient use of the Grid.

VO specific use-cases will be described.

INTRODUCTION

The Grid Computing paradigm

The Grid computing paradigm has introduced the Virtual Organization (VO) concept, which comprises a set of individuals and/or institutions having direct access to computers, software, data, and other resources for collaborative problem solving or other purposes. The sharing of resources is regulated by a context for Grid operations that allow discovering, accessing and monitoring, regardless of their physical location. This set of services acts as an intermediary between the physical resources and applications, it is called Grid Middleware.

In this paper we consider the gLite middleware developed by the EGEE project.

The EGEE middleware services

The EGEE middleware follows a service oriented architecture which allows a reliable interoperability among Grid services and an easier compliance with upcoming standards - such as Open Grid Services Architecture (OGSA) [11] - that are also based on these principles. Generally most services are managed by a VO and there is no requirement of having independent service instances per VO; for performance and scalability reasons service instances will in most cases serve multiple VOs. EGEE middleware focuses on four main service categories as shown in Figure 1.

Information and monitoring services: provide the crucial mechanism to publish and consume information data and to use it for the purpose of monitoring and maintenance of the Grid infrastructure.

Data management services: provide the three main service groups related to data and file access and storage: Catalog Services, Storage Elements (SEs), and Data Management. Closely related to the data services are the security-related services.

Security services: encompass the Authentication, Authorization and Auditing services which enable the identification of entities, access to services and resources and provide information for post-mortem analysis of security related events.

Job management services: the main services related to job management/execution are the Computing Element (CE), the Workload Management, Accounting, Job Provenance, and Package Manager services. These services communicate with each other as the job request progresses through the system, so that a consistent view of the status of the job is maintained.

Figure 1 shows the scope of the framework described in this paper regarding the authorization, authorization and accounting issues in a VO-oriented context.

A user that wants to use Grid services first has to authenticate itself by obtaining a certificate from a Certification Authority (CA), then he can connect to a User Interface (UI) to invoke a proxy certificate, needed to authenticate the user to other nodes. VOMS that improved the flexibility of the authorization process, introduced an Attribute Certificate (AC) extension to the users certificate, containing some information regarding the users roles and permissions granted by the VOs. Based on these roles/capabilities the

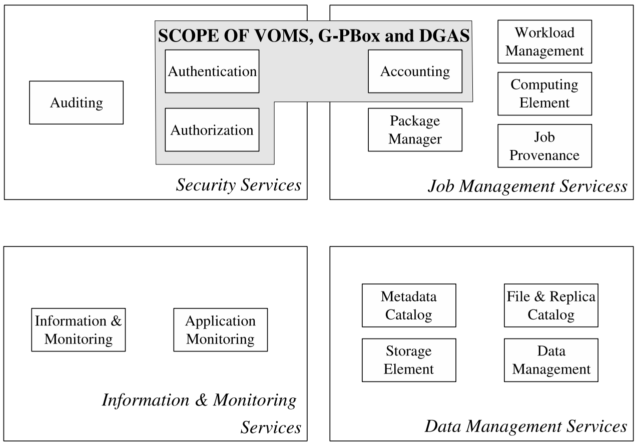

Figure 1: Scope of VOMS, G-PBox and DGAS among the EGEE Grid middleware services.

authorization is granted by the CEs and SEs, the gridmap-file [12] maps a user to a local account.

Job operations are managed by the Resource Broker (RB), which is part of the WMS. If a user needs to run a job he has to create a Job Description Language (JDL) file and has to submit it to the RB that will dispatch the job to the appropriate CE. The RB also allows users to get information about the job status and about the job output. Nevertheless a user can bypass the RB's job scheduling decision because the JDL allows to specify the CE's unique ID.

This architecture has a limitation regarding the authorization process, the user roles and capabilities (decided by a VO administrator using the VOMS) do not necessarily guarantee access to the resource selected by the RB because, for example, a local resource administrator might have banned the access to all users for a limited time. In this case there is a conflict between a VO, which decides the users capabilities and roles, and a local site where one ore more administrators manage resources owned by a local organization. In this paper we propose to extend this architecture using a policy framework (G-PBox) integrated with VOMS and an accounting service (DGAS) to have a homogeneous and VO-oriented authorization process.

A NEW INTEGRATED FRAMEWORK

The new VO manager perspective

Hands-on experience of Grid technology in a production environment has resulted in the identification of two well-defined management layers: the user layer and the resource layer. In the usual non-Grid distributed framework, there is only the resource management layer: users are local consumers and their jobs are managed by the local resource owner. In a Grid environment, on the other hand, users operate in a wider context which is beyond the control of local resources. In this perspective a new role emerges: the VO administrator who defines the permissions/rights of the users of the VO on resources not owned by the VO itself. Although the VO administrator doesn't directly control the resources the VO users are accessing, in a VO-oriented environment like the Grid, his role is as critical as the one of the resource administrator. The VO administrator needs a custom set of tools to accomplish her task.

The components involved in the framework

Three important components are involved in the proposed VO-oriented framework:

- VOMS (Attribute authority)
- G-PBox (Policy system)
- DGAS (Accounting system)

VOMS handles the authorization part of the security mechanism allowing a user to provide authorization data as he tries to access a remote resource. The type of data VOMS handles is information about a user's relationship with the virtual organizations he 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 to a remote resource for special processing needs. VOMS features include:

- single login at the beginning of a session
- limited validity of authorization credentials
- backward compatibility with existing non VOMS-aware grid services
- handling of role/capability information for multiple credential for all VOs a user belongs to
- allows access to any of them

The purpose of DGAS is to implement 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 which collect usage metrics from the local batch systems' log files and integrate them with grid-related information about the jobs and the users that submitted them. Account Balancing and Resource Pricing are optional features. Account Balancing may help in balancing demand and supply while Economic Brokering based on resource pricing may help in balancing the incoming workload among Grid resources [13] [14]. Account Balancing is based on the exchange of virtual credits between the User account and the Resource account. Resource pricing is under the responsibility of dedicated Price Authorities (PAs) which may use different pricing algorithms. Accounting information is associated to user and resource accounts and can be stored at user or VO level by dedicated User Home Location Register servers (User HLRs) and at resource level by dedicated Resource HLRs.

G-PBox is a tool for managing policies in a grid environment. A G-PBox controls the policies for the administrative domain of a resource provider, locally storing all policies that concern the resource itself. G-PBoxes form a network which allows for the creation of policies on any administrative domain, the existence of an authoritative mechanism to grant a domain control over other domains, policy distribution (propagation) and synchronization. Policies are described in XACML [15], a high level general purpose language. The actual usability of a category of policies by G-PBox may depend on the availability of external information such as the ones provided by an accounting tool or a monitoring tool. The communication with these external tools is performed through a plug-in mechanism.

The interaction among the components

In a Grid perspective VOMS, DGAS and G-PBox address the typical Authentication-Authorization-Accounting (AAA) issues. VOMS is an attribute authority system, DGAS is an accounting system and G-PBox is a grid policy system.

In a production Grid the VO activity can be characterized by two phases:

- the definition of the groups/roles, policies and the management of DGAS user accounts by the VO administrator
- the interaction between the VO users and the Grid resources

Figure 2 shows the first phase with the VO administrator tasks and the usage of VOMS, GPBox and DGAS tools in order to define VO-wide policies and permissions for the VO's users.

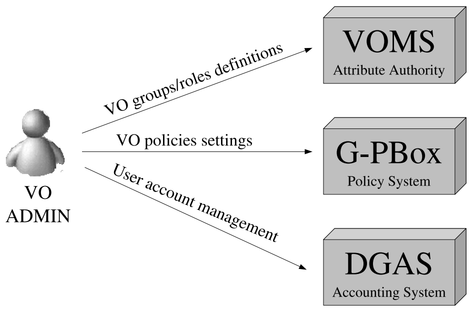

Figure 2: 1st phase - VO administrator tasks.

VOMS and G-PBox together allow building and managing a smart Role-Based-Access-Control (RBAC) policy system, with VOMS providing attributes for groups and roles and G-PBox providing the permission profiles granted to the groups/roles defined by the VOMS. G-PBox and DGAS together allow the enforcement of policies regarding the accounting information for a user or a VO in its entirety. VOMS, G-PBox and DGAS communicate with each other using secure channels based on Globus GSI [16] in order to guarantee data integrity and privacy wile sharing sensitive data.

Figure 3 shows the information flow among the three components when a user submits a job. The first step is the proxy certificate creation (1),(2), followed by the job submission(3) to the Resource Broker (RB), then the G-PBox plug-in in the RB Policy Enforcement Point (PEP) queries(4) the VO G-PBox about any policy concerning the user. These policies have been previously defined by the administrator of the user's VO or set by a site administrator and then propagated to the VO's G-PBox.

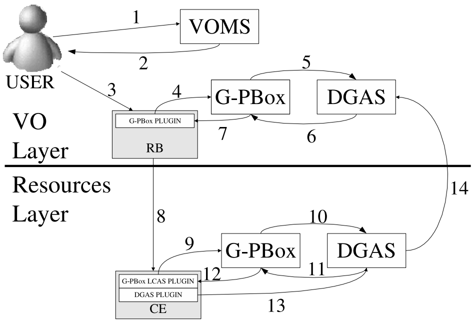

Figure 3: 2st phase - User job submission.

In the case of accounting policies, the VO's G-PBox queries the VO's DGAS server for the required accounting information(5),(6). The RB receives the answer from the VO G-PBox (7) and submits the job to the proper CE(8). On the resource layer a similar CE/G-PBox/DGAS process happens (9,10,11,12). After job execution the job's resource usage information is stored by DGAS (13,14).

Resource Broker use cases

One of the first use cases we analysed was how to apply policies to the matchmaking done by the Resource Broker (RB). The first such request we got was to have an RB capable of splitting resources in a set of classes, each with its own priority, and then assigning jobs to resources based on such priority and the user's VOMS credentials. Needless to say, this job/resource match had to be dynamic, e.g. the credentials needed to access a specific class of resources had to be changeable without affecting in any way the configuration of the resources or of the broker.

The chosen solution is to require a resource to publish a tag describing their class in the information system, and then define policies associating a specific group/role combination to a class of resources. The PEP associated to the RB needs then only to contact the G-PBox passing the following parameters: the action (job-submission), the credentials of the user and a list of suitable resources, each with its associated tag. It will obtain as a result a set of allow/deny answers for each resource describing whether the user is allowed to submit a job or not.

Although this implementation of a PEP aimed at a very specific policy, it can also be used to enforce other types of policies, such as blacklists. An extension to new types of policies will just require the PEP to process additional tags, showing the flexibility of this approach.

Computing element use case

Another PEP we implemented was a plug-in for the Computing Element (CE), whose job was policy-based mapping of Grid users to local accounts.

Its implemented as an LCMAPS [17] plug-in, which contacts the site's G-PBox, sends it the credentials of the user and obtains a local account or pool account as a result, or a deny if the user is not allowed to submit jobs to the host.

Unfortunately, due to limitations of the current CE architecture some policies, while already supported by G-PBox, cannot be implemented by this plug-in, like for example fair resource sharing among users, because they would require significant modifications of the CE.

CONCLUSIONS

An efficient use of world wide Grids by distributed user communities requires specific VO oriented tools allowing coordinated, role/group based user management and resource access management granted by specific policies and accounting. The integration of these services, VO membership management, policy management and accounting, can build a Grid production framework where Grid users (VOs) and resource owners interact according to dynamic agreements for accessing and providing resources and services. The first experience of the definition of policies related to different groups of a VO, enforced by a Grid Resouce Broker and checked by the CEs, suggests 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. This approach is independent of specific Grid implementations and can be integrated with any service aiming to enforce policies in a distributed system where users and resource owners want to be able to agree on different service levels, important for eventually establishing a business-based Grid model.

REFERENCES

[1] 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.

[2] VOMS at INFN Authorization Working Group, `http://grid-auth.infn.it/`

[3] 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.

[4] The G-PBox Home Page at INFN, `http://infnforge.cnaf.infn.it/gpbox/`

[5] R.M. Piro, A. Guarise, and A. Werbrouck. An Economy-based Accounting Infrastructure for the DataGrid. In Proceedings of the 4th International Workshop on Grid Computing (GRID2003), Phoenix, Arizona, November 17, 2003.

[6] The Distributed Grid Accounting System, `http://www.to.infn.it/grid/accounting/`

[7] Lightweight Middleware for Grid Computing, `http://glite.web.cern.ch/glite/`

[8] The Large Hadron Collider (LHC) Computing Grid, `http://lcg.web.cern.ch/LCG/index.html`

[9] The gLite Workload Management System, `http://glite.web.cern.ch/glite/wms/`

[10] EGEE web site, `http://www.eu-egee.org`

[11] The Open Grid Service Architecture workink group, `http://forge.gridforum.org/projects/ogsa-wg`

[12] The Globus alliance, `http://www.globus.org`

[13] A. Guarise, R. M. Piro, A. Werbrouck. Simulation of Price-sensitive Resource Brokering and the Hybrid Pricing Model with DGAS-Sim. In Proceedings of the 13th International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE 2004), track on Emerging Technologies for Next Generation Grid (ETNGRID 2004), Modena, Italy, June 14-16, 2004.

[14] A. Guarise, R. M. Piro, A. Werbrouck. Price-sensitive Resource Brokering with the Hybrid Pricing Model and Widely Overlapping Price Domains. Accepted for publication in a special issue of Concurrency and Computation: Practice and Experience (Wiley Publishers). Available advance of print at: `http://www3.interscience.wiley.com/cgi-bin/abstract/112142574/ABSTRACT` , February 2006.

[15] OASIS eXtensible Access Markup Control Language, `http://www.oasis-open.org/committees/+tc_home.php?wg_abbrev=xacml`

[16] I. Foster et al. "A Security Architecture for Computational Grids". In Proceeding of the 5th ACM Conference on Computers and Security, pp. 83-91, ACM Press, 1998.

[17] A local credential mapping services, `http://www.dutchgrid.nl/DataGrid/wp4/lcmaps/`