Using the VOM portal to manage policy within Globus Toolkit, Community Authorisation Service & ICENI resources

Asif Saleem Marko Krznarić Jeremy Cohen Steven Newhouse
John Darlington

London e-Science Centre, Imperial College London, South Kensington Campus, London SW7 2AZ, UK
Email: iceni@imperial.ac.uk

Abstract

The emergence of computational and data grids has led to resources within a single organisation being exposed to other users within a 'virtual organisation' (VO) that encompasses a dynamic distributed infrastructure. Due to this dynamic nature of VOs, there is a need for an infrastructure to facilitate the management of the constituent users and resources. We have been developing an easy to use and secure management infrastructure - the Virtual Organisation Management (VOM) Portal. We present how using the VOM portal, we are able to manage policies within Globus Toolkit, Community Authorisation Service (CAS) and Imperial College e-Science Networked Infrastructure (ICENI) middleware.

1 Introduction

The emergence of 'Computational Grids' have made provision of high performance and distributed computing power, accessible to the scientific community. These systems have made physically distributed computational, storage, software and networking resources integration possible. These resources can be owned by different physical organisations which are cooperating to build computational communities named 'virtual organisations' (VO) [5]. In VOs, the availability of users and resources is highly dynamic and difficult to predict. In addition, some sort of VO-wide access control, usage and related management policies need to be defined and enforced [13]. This is why an integrated infrastructure to manage these VOs is needed.

VOM [11] provides such an infrastructure through a portal for remote VO management, web/grid services to download and upload information into the VOM database, and client tools to interact with the services through Grid Security Infrastructure (GSI) authenticated network connections. Within this paper we describe the use of the VOM Portal as an interface to control three Grid infrastructures:

- GT2 - Globus Toolkit 2 deployed on the UK e-Science Grid
- CAS (Community Authorisation Server) within GT3
- ICENI (Imperial College e-Science Networked Infrastructure)

We use VOM with the Globus Toolkit to provide resource usage logging, this is necessary not only for accounting but also to find out utilisation of resource capacity in a typical grid environment. Also, automating grid-map file management - used for resource access control within Globus Toolkit - is important to support scalabilty within the VO.

Globus Toolkit v3 (GT3) provides command line clients and a Java API for the Community Authorisation Service (CAS), but unfortunately no graphical user interface (GUI). The VOM portal solves this issue and helps both administrators and users of CAS enabled VOs in their daily tasks.

The Imperial College e-Science Networked Infrastructure (ICENI) [6] is a Grid middleware that allows users to construct applications through a graphical composition tool utilising distributed component repositories. In ICENI various administrative functions - for instance role management - can be administered through their respective XML based configuration files or graphical user interfaces. Providing a web interface could further simplify such administration tasks and many instances running on different resources can be managed remotely without the need to install any ICENI clients on the user's desktop.

The rest of this paper includes sections containing further details on VOM, how it is used to manage Globus Toolkit, Community Authorisation Service and other ICENI components and finally details of the work being done currently and it's future directions.

2 Virtual Organisation Management (VOM) Portal

VOM provides user registration using grid certificates, resource access control through grid-map file management (a grid-map file maps a user's grid identity to the local grid environment - thereby controlling access to Globus) and resource usage accounting and reporting functionalities.

Within VOM, we have incorporated the latest recommendation of a minimal Usage Record (UR) from the UR-WG of GGF [1] and provided a prototype implementation of the Resource Usage Service (RUS) Grid Service being standardised by the RUS-WG within GGF.

The VOM Portal can be used standalone for user and resource enrollment into a VO, it has no dependency on Globus Toolkit, ICENI or CAS. However, to fully exploit its capabilities we can plug in clients for Globus Toolkit, ICENI or CAS which can make use of the secure authentication and authorisation infrastructure provided by VOM.

2.1 User registration

Enrolment into a VO, a collaboration such as an e-Science project that has participants and resources from many real organisations, is split into two phases: authentication and authorisation. Authentication, proof of your identity, is encapsulated within a Globus compatible X.509 public key certificate. One source of such certificates is the UK e-Science Certification Authority being run by the UK Grid Support Centre [2]. Authorisation to join a VO is down to the policy of that VO. The VOM portal provides a secure web-based user registration functionality. Users register with the VO by using their grid certificate, embedded within a standard desktop web browser. This mechanism is used to prove their identity during all interactions with the portal. Once the user is registered, it is upto the administrator of that particular VO to approve or reject the user's registration request based on the information provided.

2.2 User roles and their responsibilities

The management of a VO is done by assigning roles to registered users. Whenever users log in to the portal they get access to a restricted set of functionalities based on the role assigned to them by the VO administrator. This is done by first authenticating and then authorising users using their digital certificates.

First users have to register with the VO, once their request is approved by the VO manager, it is forwarded to the managers of the resources. Finally, users can view the resources they have been approved to access and accounting information about their resource usage.

The resource manager's responsibility is to approve user's access to the resources they manage by assigning account names to them. He/She also needs to install clients for resource usage logging and grid-map file management on their resources.

A VO Manager is responsible for enrolling users and resources (along with assigning managers to them) into the VO. He/She also allocates users to the resources and views the overall resource usage of the VO.

3 VOM & Globus Toolkit

3.1 Resource access control

The VOM portal also provides the facility to automate the work flow in creating accounts on distributed resources. Each resource needs to install a Java based client, which connects to the web service hosted on the VOM Server, to update the resource's grid-map file.

Once the VO manager has approved a user's registration, local resource managers are notified of the request. It is upto a local resource manager to approve or reject the account creation request on that particular resource. Various account creation strategies [8] can be employed to map the grid identity to a local account. The local resource manager can either decide to create a local user account, or map to a pool of existing accounts, or use account templates [9] [12]. After the creation of this account, the local username is entered into VOM for inclusion in the next update of the grid-map file.

This way grid-map files for all the resources can be managed centrally from a portal. Similarly, a client can connect to multiple VOs and update the grid-map file accordingly.

3.2 Resource usage accounting and reporting

VOM provides facilities for resource usage logging, which can be uploaded into the central database hosted at the VOM Server. Users, resource ad-

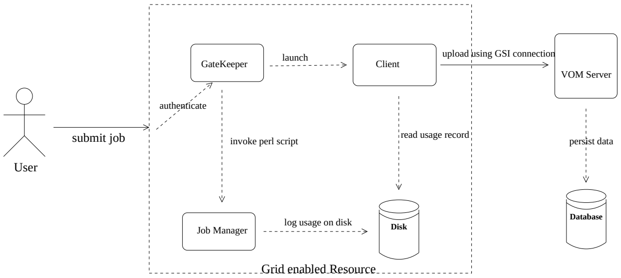


Figure 1: Resource Usage Service Client

ministrators and VO managers can view their usage records restricted based on their access privileges.

GGF Usage Record WG has specified a minimal set of parameters that constitute a usage record. The 22 parameters include job id, project id, CPU usage, memory usage, disk usage among others. VOM uses this recommended set of parameters to store and retrieve usage records.

The RUS client (Figure 1) running on a resource connects to the RUS grid service to submit the usage record, each time a job is submitted on that particular resource. A log of all the jobs (in XML format) submitted on a particular resource can also be retrieved by the client. A user can view usage records in tabular (Figure 3) and graphical format (Figure 2) through the web interface.

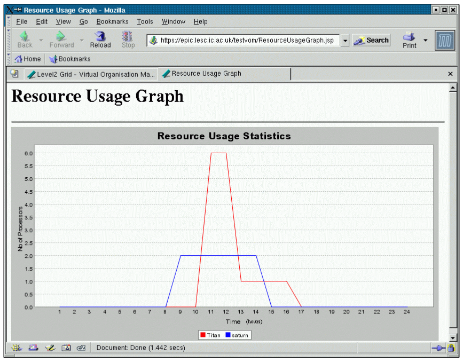


Figure 2: Graphical display of user's resource usage

4 VOM & Community Authorisation Service

Community Authorisation Service (CAS), [10, 4, 3], is an authorisation architecture proposed by the Globus Team to manage access to the resources that constitute a VO. CAS allows resource owners to specify course-grained access control policies in terms of communities/VOs as a whole, thus being spared of day-to-day administration tasks - the resource administrator does not need to be involved in, say, enrolling new users, changing privileges, etc. The fine-grained access control policy management is delegated to the community/VO itself - community representatives with sufficient privileges can easily add new users, grant permissions on some or all of the community's resources, etc. The CAS model improves scalability properties comparing with the standard Globus model, while allowing access to resources within the VO.

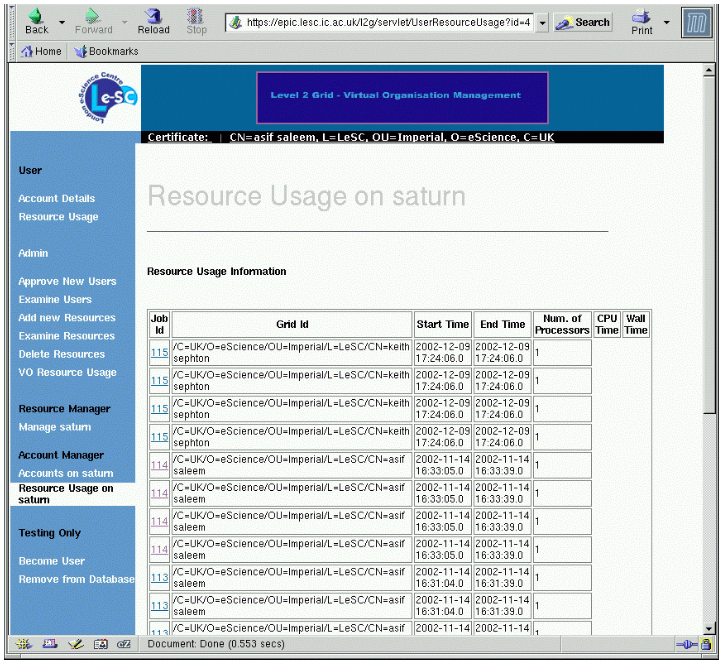
4.1 Employing CAS and administering a VO

A VO representative (VO admin) acquires a GSI (X.509) credential, and using it, employs a single CAS server for the VO. The GSI credential will represent the VO community as a whole (DN value of the credential will be present in the grid-map file, a file which maps a GSI credential to a user account on a VO's resource).

Each of the resource providers grants privileges to the VO as a whole, using standard mechanisms - grid-map file, disk quotas, filesystem permissions, etc. The amount of work required from resource providers is minimal - there is only one user account for the VO and a single modification of the grid-map file.

The VO admin (or his trusted delegates) uses CAS to manage the VO's trust relationships (e.g. adding new users and objects) and to grant fine-grained access control to the VO's resources.

GT3 provides command-line clients for all CAS operations (e.g. to enrol and remove users, namespaces, objects and service types; to maintain permissions, to maintain user groups, object groups and action groups). Furthermore, GT3 provides a Java API for CAS, but unfortunately no GUI. The VOM portal is ideal for the management of a CAS enabled VO. Its user-friendly web-based interface makes fine-grained tasks of VO administrators much simpler and straightforward.



Certificate: | CN=asif saleem, L=LeSC, OU=Imperial, O=eScience, C=UK

Resource Usage on saturn

Resource Usage Information

Job Id	Grid Id	Start Time	End Time	Num. of Processors	CPU Time	Wall Time
115	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=keith sephton	2002-12-09 17:24:06.0	2002-12-09 17:24:06.0	1		
115	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=keith sephton	2002-12-09 17:24:06.0	2002-12-09 17:24:06.0	1		
115	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=keith sephton	2002-12-09 17:24:06.0	2002-12-09 17:24:06.0	1		
115	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=keith sephton	2002-12-09 17:24:06.0	2002-12-09 17:24:06.0	1		
114	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=asif saleem	2002-11-14 16:33:05.0	2002-11-14 16:33:39.0	1		
114	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=asif saleem	2002-11-14 16:33:05.0	2002-11-14 16:33:39.0	1		
114	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=asif saleem	2002-11-14 16:33:05.0	2002-11-14 16:33:39.0	1		
114	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=asif saleem	2002-11-14 16:33:05.0	2002-11-14 16:33:39.0	1		
113	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=asif saleem	2002-11-14 16:31:04.0	2002-11-14 16:31:39.0	1		
113	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=asif saleem	2002-11-14 16:31:04.0	2002-11-14 16:31:39.0	1		
113	/C=UK/O=eScience/OU=Imperial/L=LeSC/CN=asif	2002-11-14	2002-11-14	1		

Figure 3: Tabular display of user's resource usage

4.2 Using CAS

When a user wants to access a resource served by the CAS, he/she does it using restricted credentials of the CAS server, rather than his/her own individual GSI credential. The user first makes a request to the CAS server using his/her individual proxy. Provided with appropriate privileges, the CAS issues the user a restricted proxy with an embedded policy giving the user the right to perform the requested actions.

Using the restricted CAS proxy, the user then performs any Globus enabled operation, say GridFTP. The resource then applies its local policy (granted to the VO as the whole) and further restricts that access based on the policy in the CAS credential itself. This way, the user privileges are equal to the intersection of the privileges granted to the user by the CAS and those granted to the VO as a whole by the resource provider.

5 VOM & ICENI

The Imperial College e-Science Networked Infrastructure (ICENI) is a Grid middleware that allows users to construct applications through a graphical composition tool utilising distributed component repositories. The ICENI model consists of private domains and public computational communities (Figure 4, [7]). Domain and identity managers control the resources that are published from a private domain into a public community. When an organisation publishes a resource into their private domain, the domain manager discovers the resource and delegates access control to the identity manager. Each resource has an associated XML-based access control policy allowing resource access to be defined at role, group, organisation or individual user level. Access to resources at role, group, organisation and individual level can be constrained by time, day and date providing flexibility when administering the system.

Advanced role-based access control features include role modification lists and role mappings. Role modification lists allow temporary modification to role membership without the requirement to add users to a main list of role members. Role mappings allow users from trusted external organisations to be mapped on to local roles. This helps simplify the setup of access permissions for external users. Role and group information in ICENI is stored in a simple XML-based format and can be administered through the role management GUI (Figure 5) that further simplifies administration tasks.

Given the crossover in domains of the Globus Toolkit, Community Authorisation Service and ICENI, a common means of user administration is desirable. The VOM portal provides a user-friendly web-based interface designed specifically for VO management and is therefore ideal as a centralised

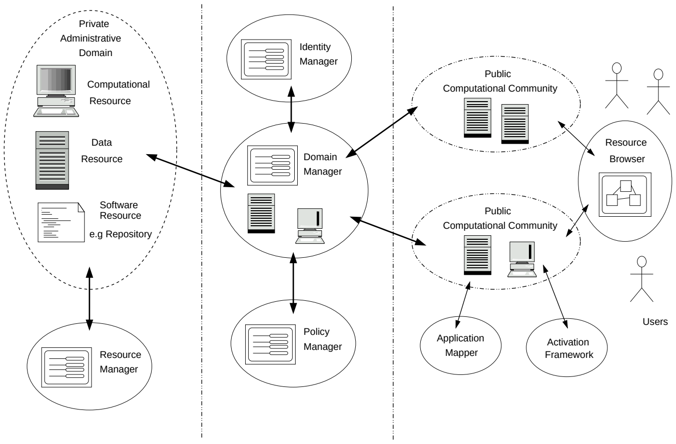


Figure 4: ICENI Architecture

means of administering these domains. The ICENI role management framework is based on X.509 certificates and provides an interface exposing a variety of methods to alter and dynamically update the membership of roles and groups. VOM utilises this interface to enable comprehensive access to ICENI's administration features via the VOM interface. The ability to apply updates to ICENI dynamically means that administrators can remotely connect to an ICENI domain through the VOM user interface and make changes that will take effect immediately. These changes are also updated in the XML configuration file held on persistent storage, ensuring that they persist in the event that a domain needs to be restarted.

6 Future Work

6.1 VO deploment issues

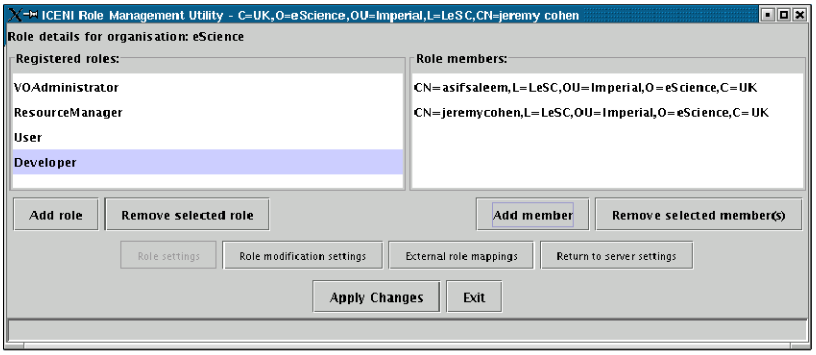
There are interesting open issues regarding the deployment pattern of the VOM Portal. For instance, should there be a single VOM Portal for the whole physical Grid infrastructure (e.g. e-Science Grid) or should each VO be defined at community or project level having its own instance of the VOM Portal. In the UK, there are already projects and communities that have a strong internal culture e.g., RealityGrid, e-Minerals etc.

One possibility is to have the grid infrastructure such as the UK e-Science Grid treated as the SuperVO with each e-Science community or project being a VO within the SuperVO.

These issues require further investigation and feedback from real-life experiences before we can arrive at some sort of definitive agreement.

6.2 Expressing & enforcing policy by making it formal/explicit

Currently we are investigating the use of WS-Policy, WS-PolicyAssertion and other web services standards along with formal policy languages like Ponder and Akenti to let stakeholders (e.g. users, resource managers and administrators) explicitly specify the service level agreements (SLA). This way users would be able to know what is the mini-


ICENI Role Management Utility - C=UK,O=eScience,OU=Imperial,L=LeSC,CN=jeremy cohen

Role details for organisation: eScience

Registered roles:

VOAdministrator
ResourceManager
User
Developer

Role members:

CN=asifsaleem,L=LeSC,OU=Imperial,O=eScience,C=UK
CN=jeremycohen,L=LeSC,OU=Imperial,O=eScience,C=UK

Figure 5: ICENI Role Management Application

mum quality of service they are supposed to provide and/or receive.

6.3 Web services based Grids compatibilty

Many efforts (like WS-GAF, WSRF, .NET Grid) to build interoperable grids using existing web standards are emerging. We aim to provide a pure web services based implementation for interoperabilty with such efforts.

7 Conclusion

VOM provides a centralised management interface for managing a VO and is already being used in UK e-Science Grid. We are using it for resource access control and usage accounting for the Globus Toolkit. It provides an easy-to-use web interface for specifying community level access control policies for Community Authorisation Service, as well as role-based identity management in ICENI.

8 Acknowledgements

The authors want to thank members of the UK Grid Engineering Task Force for testing and evaluating the software. The work has been carried out as part of the OSCAR-G project at the London e-Science Centre supported by the DTI, Compusys and Intel (THBB/C/008/00028). The CAS activities have been supported by the Joint Information Systems Committee (JISC) AAA Programme (`http://www.jisc.ac.uk/index.cfm?name=programme_aaa`).

References

[1] Global Grid Forum. `http://www.ggf.org/L_WG/wg.htm`.

[2] Grid Support Centre. `http://www.grid-support.ac.uk/`.

[3] CAS GT3 notes. `http://www.globus.org/security/CAS/GT3/`.

[4] S. Cannon, S. Chan, D. Olson, C. Tull, V. Welch, and L. Pearlman. Using CAS to Manage Role-Based VO Sub-Groups. *Computing in High-Energy and Nuclear Physics (CHEP 03) La Jolla, California*, March 2003.

[5] I. Foster, C. Kesselman, and S. Tuecke. The Anatomy of the Grid: Enabling Scalable Virtual Organisations. *International Journal of Supercomputing Applications*, 2001.

[6] N. Furmento, W. Lee, A. Mayer, S. Newhouse, and J. Darlington. ICENI: An Open Grid Service Architecture Implemented with Jini. In *SuperComputing 2002, Baltimore, USA*, 2002.

[7] N. Furmento, A. Mayer, S. McGough, S. Newhouse, T. Field, and J. Darlington. ICENI: Optimisation of Component Applications within a Grid Environment. *Journal of Parallel Computing*, 28(12):1753–1772, 2002.

[8] Thomas J. Hacker and Brian D. Athey. A Methodology for Account Management in Grid Computing Environments. In Craig A. Lee, editor, *Proceedings of Grid Computing - GRID 2001, Second International Workshop, Denver, CO, USA, November 12, 2001*, volume 2242 of *Lecture Notes in Computer Science*, pages 133–144. Springer, 2001.

[9] Laura F. McGinnis, William Thigpen, and Thomas J. Hacker. Accounting and Accountability for Distributed and Grid Systems. In *2nd IEEE International Symposium on Cluster Computing and the Grid (CCGrid 2002), 22-24 May 2002, Berlin, Germany*, pages 284–285. IEEE Computer Society, 2002.

[10] L. Pearlman, C. Kesselman, V. Welch, I. Foster, and S. Tuecke. The Community Authorization Service: Status and Future. *Computing in High-Energy and Nuclear Physics (CHEP 03) La Jolla, California*, March 2003.

[11] A. Saleem, M. Krznaric, S. Newhouse, and J. Darlington. ICENI Virtual Organisation Management. In *UK e-Science All Hands Meeting, p. 117–120, Nottingham, UK*, 2003.

[12] William Thigpen, Thomas J. Hacker, Brian D. Athey, and Laura F. McGinnis. Distributed Accounting on the Grid. In *Proceedings of the 6th Joint Conference on Information Science, March 8-13, 2002, Research Triangle Park, North Carolina, USA*, pages 1147–1150. JCIS/Association for Intelligent Machinery, 2002.

[13] Glen Wasson and Marty Humphrey. Policy and Enforcement in Virtual Organizations. In *4th International Workshop on Grid Computing (Grid2003) Phoenix, AZ.*, 2003.