

Authorization, Accounting and User Account Management in GRID Environment

Michal Jankowski, Pawel Wolniewicz, Norbert Meyer
Poznan Supercomputing and Networking Center

Logging and accounting (features crucial from security and economy points of view) are possible on a single computer system, but currently it is almost impossible to gather accounting for a whole GRID environment. Logging and accounting in any system is complicated and limited without operating system support and personal user accounts. GRID is potentially a system that consists of lots of dynamic Virtual Organizations with hundreds or even thousands of users. The VOs belong to different administrative domains with different security policies, so that solutions with centrally managed accounts are not appropriate. Also, there is no single authorization decision make point. In order to enable logging and accounting features, existing solutions (e.g. as Globus Toolkit GSI) require having user account on each GRID node he (potentially) needs to access.

This solution however, produces too big administrative burden in case of wide, complex and dynamic environment. Moreover, it doesn't combine (dynamic) policies of organizations- resource owners and consumers. So, there is a need for a tool that allow distributed user management with minimum administrative work, combining policies from different sources and enabling logging and accounting features. PSNC has introduced the Virtual User System (VUS), which meets the above requirements.

VUS is an extension of the system that runs users' jobs (e.g. queuing system, Globus Gatekeeper, etc.) and allows running jobs without having a user account on a node. This allows minimizing overhead related to creating and maintaining additional user accounts. On the contrary to other solutions, VUS assures an accurate security level achieved by user authorization and possibility of charging the user with costs of resource usage. Additionally, it respects local policy of sites and makes it possible for the local administrator to differentiate between local and remote users.

The first implementation of VUS was an extension to queuing systems (e.g. LSF) and it was successfully exploited 3 years ago in the Polish national cluster, which connected several HPC centers in Poland. The current implementation is GRAM 'callout', a mechanism introduced in Globus Toolkit 3.2.

VUS extends the GT Gatekeeper and GridFTP services by the following features:

- Flexible and configurable, fine-grained authorization with minimum administrative overhead. Authorization is done by querying plugins
- Virtual user accounts. There is a set on such accounts on each node, they are bound to users only for some time - there is no need to maintain an account on each node for each user
- Accounting. Once we know who and when used a virtual account, it is possible to charge him/her with costs of used resources

- Virtual Organization Information System plugin allows easy combining local and remote security policies.

VUS is used in various configurations in several national projects: Clusterix (National Cluster of Linux Systems), SGIgrid (done in cooperation with Silicon Graphics) and international projects like GridLab (5 FP of EU) and CoreGrid (6 FP of EU).