Contribution ID: **93** Type: **Sessions contributions**

Improved Resilience and Usability for Science Gateway Infrastructures via Integrated Virtual Organizations

Wednesday, 21 May 2014 14:20 (20 minutes)

The workflow-enabled MoSGrid Science Gateway is especially tailored to perform advanced molecular simulations in a user-friendly way. It employs a distributed science gateway infrastructure applicable for science gateways in general. Key focus is the high usability by creating an intuitive virtual environment. Since the underlying distributed computing infrastructure (DCI) including job, workflow and data management is complex, it becomes a constant challenge to ensure high availability. The goal of our work is to improve the resilience and usability of the MoSGrid science gateway. This was achieved regarding the security by easing the registration of users and lowering the complexity of their authentication. Without the following solution, users had to apply for a membership in a Virtual Organization (VO) and the application was manually handled via a VO manager. In our solution, a user can register via an intuitive process and after his account is unlocked he automatically becomes a member of the MoSGrid VO. The distinguished names (DNs) of these are mapped to the respective cluster-specific accounts. To enable this a series of modules was created to allow the extraction of user information, make it available via secure download, and finally use it to configure the DCI user database. The efforts made it possible to depreciate a service, removing a potential source of error and simplifying the registration procedure.

URL(s) for further info

http://link.springer.com/article/10.1007%2Fs10723-012-9247-y
http://onlinelibrary.wiley.com/doi/10.1002/cpe.3116/abstract
https://mosgrid.de

Wider impact and conclusions

Science gateway infrastructures are complex by nature, especially the security infrastructure. Ensuring high availability and user experience is a big challenge on different levels and infrastructure layers. Our approach applies user information already available in the science gateway to form the MoSGrid virtual organization. Based on this an account to cluster login mapping is created. Together with SAML assertions, which are used for authentication for the underlying DCIs, the authentication and authorization in MoSGrid is simplified. Previously a separate server for managing the virtual organization had to be maintained and has now been made obsolete. On the one hand, the infrastructure becomes simpler and thus less error prone, since a service less has to be maintained. On the other hand, the registration is simplified for the users, resulting in a lower hurdle of use which ensures broader usage in the chemical community and hence a better sustainability.

Description of work

For generating the mapping of MoSGrid VO members to their specific DCI logins, the user IDs are extracted from the science gateway database and stored in a list. The IDs are used to identify the users'SAML (Security Assertion Markup Language) assertions residing on the gateway. The SAML assertions are used to access the underlying middlewares performing the job, workflow, and data management. The DNs are extracted from the SAML assertions, duplicates are removed, and finally stored. To keep track, the unique Dns, user IDs, and the status are maintained in a flat file database. This prevents user IDs from being used twice to avoid the possibility of users accessing data of previously deleted users with the same ID. The algorithm for ensuring that every entry in the database has the correct status, works as follows: For each entry in the database the DN and status are extracted. If the DN is not present in list of current users, then the entry is invalidated. The algorithm for ensuring that current users are present in the database processes the list of current user DNs line by line. If such a DN has an invalid status in the database it is changed to valid. If the DN does not exist at all, a new valid entry is created. Using the database a generic mapping of user IDs to user DNs is subsequently created. To make the resulting file containing the user mapping information available for secure download, we created a WebApp and configured it to be accessible by users, who are specifically granted the access to the WebApp. On the cluster side a module is installed and periodically run. The module securely downloads the mapping file and specifically adjusts it for the cluster using the cluster name and user suffix. The MoSGrid Science Gateway integrates the middleware layer UNICORE for job and data management. The UNICORE user database is automatically ingested with the new user mappings and, thus, the user IDs become instantly active.

Primary author: Mr GRUNZKE, Richard (Technische Universität Dresden)

Co-authors: Dr HOFFMANN, Alexander (Ludwig-Maximilians-Universität München); Dr KRÜGER, Jens (University of Tübingen); Mr DE LA GARZA, Luis (University of Tübingen); Dr GESING, Sandra (University of Notre Dame); Prof. HERRES-PAWLIS, Sonja (Ludwig-Maximilians-Universität München)

Presenter: Mr GRUNZKE, Richard (Technische Universität Dresden)

Session Classification: Authentication & Authorisation

Track Classification: Integrated AAI services (Track Leaders: P. Solagna, A. Bonvin, J. Kewley)