Data Management And Security In Dynamic Grid-Based Virtual Organizations

Marcin Admaski, Michal Kulczewski, Krzysztof Kurowski, Jarek Nabrzyski
Poznan Supercomputing and Networking Center
Poland

In many business sectors and research areas in general, the ability to securely access diverse data sources in a collaborative multi-institutional environment, called often netowrked Virtual Organization (VO), is becoming an essential requirement for optimizing the design and development phase of the product lifecycle or accelerating the conducted research. Dynamic and secure transparent data access as well as integration of heterogeneous data sources is a key issue in many collaboration environments today. With the increasing pressure of reducing costs and time-to-market in industry and research, end-users have turned their focus to secure data access and dynamic collaboration access control to provide the answer for this requirement. In order to offer a framework that facilitates the coordination and cooperation between virtually partnering research laboratories or companies we have successfully adopted OGSA-DAI middleware framework together with important security enhancements. OGSA-DAI has been exploited as a generic high-level grid middleware offering frequently used capabilities such as data federation and distributed query processing. It abstracts away also concerns as database driver technology, data formatting techniques, data delivery and transfer mechanisms. Unfortunately, OGSA-DAI provides relatively simple and static mechanisms that must be extended with more flexible security solutions. Usually, an access user request is authorized if a certain data resource has an entry in its grid map file or access control list for the (authenticated) global identity presented with the request. Then, user identity is mapped to a corresponding local user identity and finer authorization depends on the local database or data resource. This approach is shown to be too restrictive and static to support dynamic scenarios in VOs in collaborative use of various data resources. One of the common problems in VOs is the lack of a definition of internal (authorization), external (authentication) dependencies for data access. The next challenge is that such cross-organizational policies are typically beyond the normal expressive power of security assertions used to represent policies in any of the individual organizations participating in the VO. Moreover, an additional frequent requirement is that each organizational security domain within the VO should retain full control over who, when and how can access data resources.
Therefore, in order to fulfill mentioned requirements, we have integrated OGSA-DAI services and underlying heterogonous data resources with Gridge Authorization Service (GAS) which acts as a trusted centralized logical point for defining and enforcing VO data access policies. Due to the fact that GAS is considered as independent security component of specific technologies used at lower layers it should be fully useable in different VO environments based on OGSA-DAI as well as Globus or other typical grid middleware toolkits. In this paper we present different scenarios and authorization models for dynamic data access, management and control in VOs. We also discuss preliminary results we have obtained in many experiments performed in a Pan-European testbed to proof the concept of real needs for fine-grained access control VO policy management.