Policy Management in Grids

Marty A. Humphrey, University of Virginia

1. Overview

A main goal of Grid Computing is to facilitate the creation of Virtual Organizations (VOs); however, to date, not enough attention and research has been placed on the policies by which successful collaborations and VOs operate. "Policies" in this context refers to the preferences, rules, goals, conditions, obligations, and acceptable procedures by which an entity shares information, shares physical resources, or engages services. Productive collaborative research among scientists results from a matching (perhaps via negotiation) of policies of the individual researchers involved, the policies of the physical organizations to which the researchers belong, and the policies of the VO itself. While out-of-band policy negotiations (e.g., phone calls) have been successful in the past, this approach will fail as collaborators increasing rely on and trust Grid software components and tools to accelerate and automate the collaboration. Simply, software components cannot currently negotiate to an agreement because there is a lack of acceptable policy languages, human participants cannot easily express their policies, software components do not know where to find user policies, VOs do not generally make their policies explicit, and there do not exist robust tools to perform automated policy conflict resolution. Unless these problems are solved, collaborators should be and will be reluctant to engage Grid-level collaborative tools for fear of discovering either in real-time or after-the-fact that their intentions with regard to information sharing, resource consumption, data integrity and confidentiality, etc., have been violated and subject to potentially damaging ramifications.

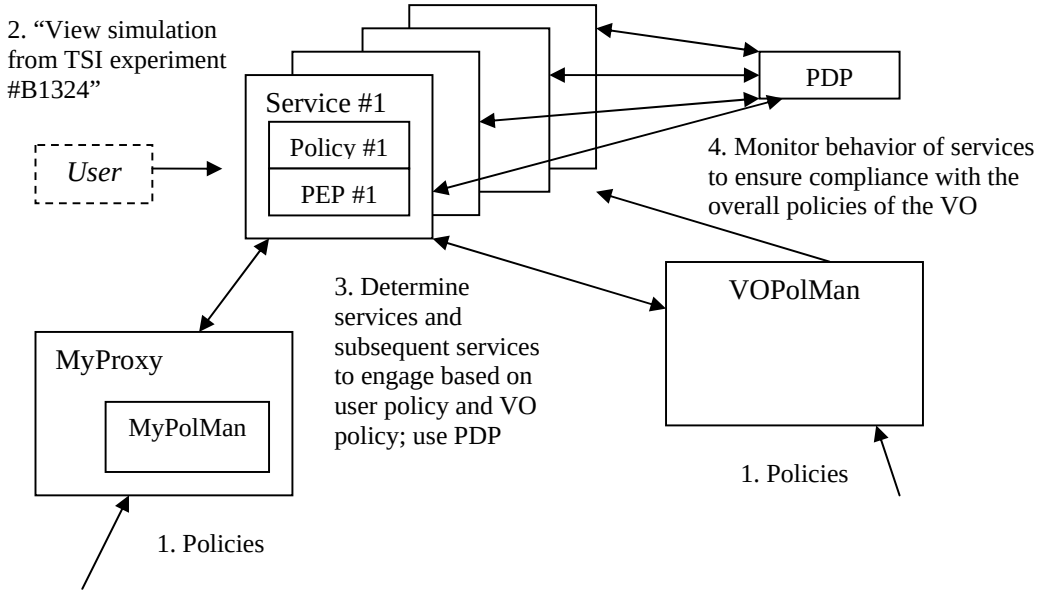

Figure 1: Grid Policy Management Architecture

To meet these needs, this project contributes tools, recommendations, and protocols for policy management in Grids to support the collaborative process. As shown in Figure 1, MyPolMan is an add-in tool suite to MyProxy, a widely-available on-line Grid credential manager, that creates the ability for a Grid user to centralize (where appropriate) and manage his/her policies. Contributed tools in the MyPolMan suite include mechanisms to securely store these policies,

perform policy evaluation, have relying (software) parties securely retrieve these policies, and record policy usage dates/times for auditing purposes. The policies of the VO as a whole are recorded and managed in the VOPolMan tool suite. MyPolMan and VOPolMan share many of the same mechanisms (e.g., it is anticipated that this project will leverage the emerging policy languages WS-Policy, WS-SecurityPolicy, and XACML); however, the scope and implications of policies and policy conflicts require separate approaches. For example, VOPolMan also contains a monitoring infrastructure to determine if the overall goals and policies of the VO are being met over time. All services and tools produced in this project are supportive of emerging Web Services standards and are consistent with the Open Grid Services Architecture (OGSA), thus facilitating core interoperability and applicability with the emerging suite of OGSA-compliant services.

2. Current Status

We have recently implemented a policy-aware Grid data movement system, utilizing our own GridFTP implementation on the Microsoft .NET Framework. As shown in Figure 2, the resource provider is currently able to interact (via a GUI) with its associated policy manager ("MyPolMan #1") to constrain policy (for example, to limit the amount of a local disk that is available for Grid use). The Grid user is able to specify her policies via a GUI (to "MyPolMan #2), which is then utilized by the policy-aware Data client application. In our example use-case, the user wishes to upload a file into the Grid that is a particular size, and the policy-aware Data client guides the user to a server box that allows files of this size. (In the figure, the "right" legacy GridFTP client is engaged to transfer the job).

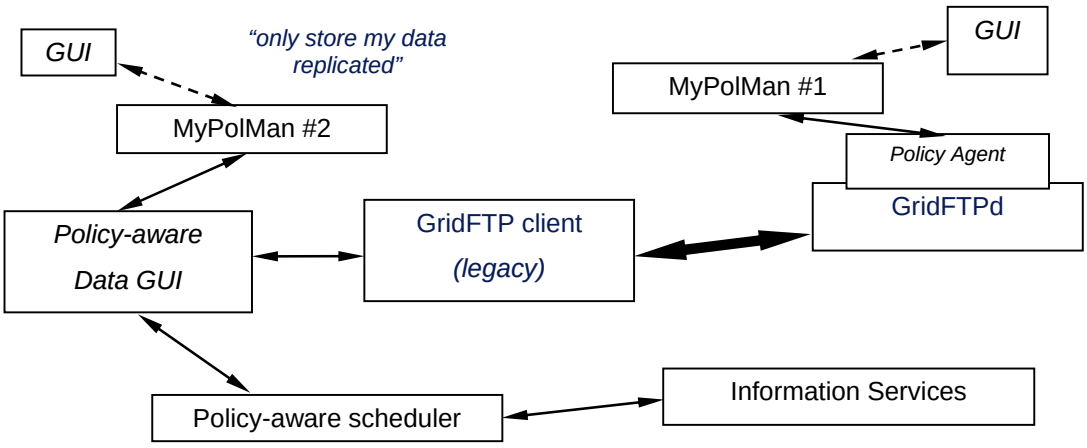

Figure 2: Policy-Aware Grid Data Movement

We are currently working to incorporate policy into the network as well. That is, we want to expand our use-case to include the policies of the networking fabric. For example, we want to give the user the ability to select the path that provides the appropriate quality of service for the data movement (e.g., through GMPLS). We recognize that the selection of path should be done in two phases: in the first phase, the policies of the network providers are retrieved so that the reasonable choice can be made. In the second phase, the network paths are configured (e.g., RSVP-TE) at run-time in order to obtain this behavior from the network. We believe the first phase is directly supported by our current work, while the second phase is a more significant challenge.