

Policy Based Governance For Virtual Computing Federation

PRASHANT C. KEDIYAL, MUNINDAR P. SINGH

North Carolina State University

Virtual computing supports the prospect of different organizations pooling their individual resources yet retaining control over them to ensure that their respective missions are not compromised. Imagine a not-too-distant future when the educational and research computing resources of the North Carolina universities and community colleges are federated. The federations could arise at multiple levels with colleges, departments, laboratories within a university retaining autonomy over the resources purchased or maintained through program funds. For virtual computing to expand to cross-organizational settings, however, requires policy-based governance. We define governance as dealing with processes by which autonomous stakeholders may administer themselves and their resources.

Say NCSU would like to offer access to students at UNC and Duke provided the students in question are PhD candidates in their respective universities, the resources they request are otherwise under-utilized, their use doesn't violate licensing or security policies, and they have not been blacklisted for any such infraction in the current academic year. The necessary policies combine support for reactive and proactive behaviors and decisions that involve both authorizations and obligations. To state such policies, we need a model that captures (1) the roles of individuals in organizations (e.g., PhD candidate at Duke), (2) business relationships among organizations (e.g., between Duke and NCSU), (3) measures of resource state (e.g., load), (4) further policy checks (e.g., apparent illegal file sharing), and (5) user properties (e.g., blacklists).

Our approach enables us to naturally handle scenarios such as the above. First, we propose a rich model that can represent independent administrative domains and cross-organizational interactions. Second, we develop an approach to specify and enact a variety of policies that incorporate the stakeholders' qualifications, their organizational relationships, their ongoing conversations as well as properties of the resources and capabilities involved. Third, we develop an architecture that supports proactive policies, and show how to realize this architecture on top of conventional policy engines and enterprise service bus infrastructure.

Existing approaches by and large do not address the challenges of governance. They include policy management techniques that support important functions such as authorization. However, they lack the vocabulary and conceptual model with which to express policies at a level that is meaningful to end users and other stakeholders. The Community Authorization Service (CAS) presumes that a resource provider would give up its autonomy to the community. In our approach, by contrast, an organization may participate in a variety of business relationships, which may limit its autonomy but not eliminate it. The VO Membership Service (VOMS) has a limited vocabulary that consists of roles, group, and capabilities [Alfieri et al. 2005], but lacks modeling the organizational relationships and ongoing interactions, which are a component of our vocabulary. Further, we support proactive policies by which a party may act on its own initiative. Such policies can be built on common resource properties, such as those supported by the Web Services Resource Framework (WSRF).

Today such policies are expressed only informally and much of governance is carried out manually. For example, the TeraGrid project provides several forms that a user or group of users may fill out to submit a proposal for using the TeraGrid resources. A committee reviews such requests and decides who is permitted. Manual governance of that nature is expensive and slow, taking place at the time-scale of weeks. Thus it cannot accommodate emerging situations. By contrast, our approach enables a larger variety of governance scenarios to be automated.

Additional Key Words and Phrases: XACML, Policy, Governance, Virtual Computing

Authors' addresses: Box 8206, Dept of Computer Science, NC State University, Raleigh, NC, 27695, USA