proc. of the 5th International Conference on Enterprise Information Systems - ICEIS2003, Angers, France, 23-26 April 2003.

POLICIES COMPOSITION THROUGH GRAPHICAL COMPONENTS

Vitor Roque
Polytechnic Institute of Guarda, ESTG, Guarda – Portugal
Email: vitor.roque@ipg.pt

José Luís Oliveira
University of Aveiro, DET, Aveiro – Portugal
Email: jlo@det.ua.pt

Rui P. Lopes
Polytechnic Institute of Bragança, ESTiG, Bragança – Portugal
Email: rlopes@ipb.pt

Keywords: Policy based management, Policies specification, Network Management.

Abstract: Policy based management have gained a crescent importance in the two last years. New demands on internetworking, on services specification, on QoS achievement and generically on network management functionality, have driven this paradigm to a very important level. The main idea is to provide services that allow specifying management and operational rules in the same way people do business. Despite the main focus of this technology has been associated with network management solutions, its generality allows to extend these principles to any business process inside an organization. In this paper we discuss the main proposals in the field, namely the IETF/DMTF model, and we present a proposal that allows the specification of policy rules through a user-friendly and component-oriented graphical interface.

1 INTRODUCTION

Network management has become in the last years a matter of great importance due the increased dependence of enterprises on their networked applications. This dependence has made the availability and performance of network services more critical than ever.

The configuration area of network management is probably the most important area in network management and affects directly or indirectly other areas, also very important, like security, performance, accounting and fault. Usually network configuration is an interactive task between the network administrator and the managed network equipments. If we consider that, due the crescent complexity of equipments and their management, new technologies, new network services and so on, the network administration occupy more and more time of user managers it is essential to find new solutions for network management.

On this context it is desirable that a network management system will be provided with the ability to automatically manage the network configuration based upon high-level rules, more or less in the same way business-oriented requests are issued. For example, a management system should be capable, for a specific management situation, to offer facilities to reconfigure the whole system without the network administrator have to worry about the configuration details of network equipment.

Policy-Based Management (PBM) has emerged during the last years as the right paradigm to deal with this type of requirements (Sloman, 1994). The main idea of PBM is the definition of high level procedures – policies – that will rule the behaviour of the network regardless the intricate lower level equipment details. The main purpose of the PBM systems is the storage, management and the transformation of policies into configuration instructions that can be applied to the network equipment. Although the focus has been primary put

on configuration management, all other areas of network management, such as security, performance, accounting and fault, are suitable for the application of policies

This paper discusses the IETF and the DMTF approaches for PBM, and proposes a solution to representing graphically management policies.

2 NETWORK MANAGEMENT AND POLICIES

Along the past years several network management models have been proposed, adopted, failed, redefined, tested, augmented (…). This rich and continuous work around the theme has been motivated by the increasing need for managing networks, systems, services and applications in an integrated and simple way. While the network complexity grows up new requirements were made to the management entities – for instance, better handling of internetworking processes to deal well with quality of service and security constraints. Although traditional management models are to tightly to the lower level instrumentation procedures, and the construction of high level management rules have been outside normalization comities until recently. In this context new proposals have been presented such as COPS (Durham et al., 2000) and SNMP for Configuration (MacFaden et al., 2002), inside the IETF, and CIM (CIM-Core, 2002) and PCIM (Moore et al., 2001) from the DMTF (in fact PCIM is a result from both organizations).

The activities on PBM standardization have been done mostly by two working groups of IETF: the Resource Allocation Protocol Working Group (Rap, 2002) and the Policy Framework Working Group (Policy, 2002).

The policy framework architecture is composed of four functional entities: the Policy Management Tool (Policy Console), the Policy Repository, the Policy Decision Point or Policy Server (PDP) and the Policy Enforcement Points (PEP). The model describes the key components but it does not prescribe any implementation details such as distribution, platform or language. As a consequence the Policy Console is the less defined component and it depends greatly on the functionality and design options taken by developers.

The PDP is the entity responsible for checking when and how policies can be applied.

The mean of policy in this context in the simplest sense: it is one or more rules that describe the action(s) to be taken when specific condition(s) exist. It can be expressed semantically as:

if (policyCondition) then (policyAction)

On the other side, the PEP is the point where the policy decisions are enforced when the rule conditions evaluate to “true”.

The Policy Repository is the site where all policy information is stored. The information stored here describes authorized users, applications, computers and services (objects and attributes) and their relationships. The repository is also accessed in the rule validation process to detect conflicts.

A policy protocol is used to transfer policy information among PDPs and between PDPs and PEPs. As the PDPs involved in the decision process may be located in different organizations, we can differentiate between intra-organizational and inter-organizational policy transfer protocols. COPS has been used mainly for intra-organizational policy transfer, while RSVP has been proposed to be used for inter-organizational policy transfer (INTAP, 2001).

This policy model has been also pushed by the DMTF that has been working closed with the IETF in this area. Within the CIM context, the organization has also proposed an extension schema that deals with policy modeling. The Policy Core Information Model (Moore et al., 2001), PCIM, extends the CIM with classes to represent policy information.

3 A GRAPHICAL APPROACH FOR POLICIES DEFINITION

The Policy Framework WG defines policy as an aggregation of policy rules (Westerinen et al., 2001). Each policy rule is made up of a set of conditions and a corresponding set of actions. The policy framework architecture defined by this WG describes the key components, but it does not prescribe any implementation details such as distribution, platform or specification language.

In policy management, the network administrator needs a tool to define the behaviour that he wants the system own. This definition of the behaviour must be done in an independent fashion from the network equipments and the syntax must enable the definition of a wide set of events. In this context the use of a generic specification language permits the network administrator to represents the policy independently from the management system that must have to enforce it. The main problem is precisely in the way how to translate behaviours or high-level policies to a generic language due factors like comprehensibility, integration, security and heterogeneity (Goh, 1998).

A main goal of policy languages has been the definition of a generic and widely used language that can be used in a universal way in all areas of network management. However, several "network policy specific languages" have been developed. The languages developed are used to represent varying types of network policies such as routing, access control and QoS. Some of the major network policy languages are currently PFDL, RPSL/SPSL, Ponder, SRL and XML (Stone and Xie, 2001). However the definition of a generic widely use language seems difficult to achieve due the actual technology limitations.

The Extensible Markup Language (XML) allows describing structured information by defining specific tags (XML, 1998). This tag arrangement builds a document that can be used to exchange information independently of the platform, programming language or application objective. These characteristics make it ideal for representing policies. In fact, a pioneer work has been done in this association by the Organization for the Advancement of Structured Information Standards (OASIS, 2002). The XACML is a specification issued by the organization for expressing policies in XML formalism for information access over the Internet.

We have been using XML for the definition of high level management operations (Lopes and Oliveira, 2002) and yet for the provisioning of management information persistence in typically volatiles SNMP agents (Lopes and Oliveira, 2001). Associated with this work we have created a component-based graphical interface that allows defining operations, expressions or rules using pre-defined Java Beans that can be dynamically attached to the user interface (Figure 1).

The same solution can easy be extended to the definition of roles, conditions, actions, rules and policies – we are currently working on the definition of a set of base components that characterizes the way these concepts are defined.

Another achievement from this work is the usage of a unique specification language (XML) that can be stored both in the PDP side, or policy repository, and in the PEP side, if this entity accepts directly this specification formalism (Lopes and Oliveira, 2002).

4 CONCLUSIONS AND FUTURE WORK

Policy-Based Management means managing or configuring network elements based upon a set of business rules or business objectives.

While traditional configuration management enables a device-by-device configuration of network elements, increased size (more devices to configure) and complexity (devices are of different types, from different vendors, with different technologies and

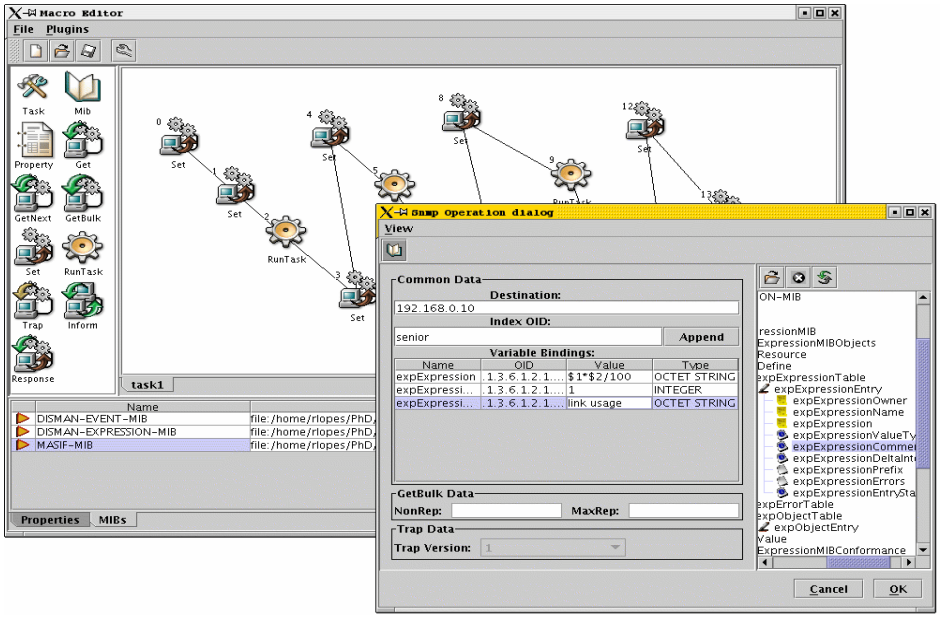

Figure 1: A composition framework for the definition of management policies. The example is based on the definition of tasks for the configuration of remote SNMP agents.

perform far more operations) are turning the configuration into a more difficult task. The main goal of Policy-Based Management is to go beyond these difficulties.

To achieve this goal, the definition of policies is a subject of a great importance in this context. Within this paper we made some considerations about what a policy language must implement for be usable in PBM systems. Concepts like user, policy, role, role hierarchy, permission, constraint, history and application and their interactions were discussed.

Although the general idea of using policies for managing network is powerful and appealing, policy management products and generalized implementations and usage are still far from the expected scenario. Improving policy languages with graphical and user-friendly interfaces can help to change this slow evolution.

In this paper we have presented a solution for the definition of policies in a graphical oriented way. Despite, the work is still under development it is based in an already existing platform that has been used successfully for the definition of SNMP management operations.

5 REFERENCES

CIM-Core, 2002. Common Information Model - Core Model v2.6, DMTF.

Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R. and Sastry, A., 2000. The COPS (Common Open Policy Service), IETF, RFC2748, January.

Goh, C., 1998. Policy Management Requirements. HP OpenView University Association (HP-OVUA) Plenary Workshop, ENST de Bretagne, Rennes, France,

INTAP, 2001. Survey on Policy-Based Networking, Interoperability Technology Association for Information Processing (INTAP).

Lopes, R. and Oliveira, J., 2001. A new mechanism for distributed managers persistence. In *ICEIS 2001, 3rd International Conference on Enterprise Information Systems*, Setúbal, Portugal,

Lopes, R. and Oliveira, J., 2002. A Multi-protocol architecture for SNMP entities. In *IPOM 2002, IEEE Workshop on IP Operations and Management*, Dallas, USA,

MacFaden, M., Partain, D., Saperia, J. and Tackabury, W., 2002. Configuring Networks and Devices With SNMP, IETF SNMPCONF Working Group, draft-ietf-snmpconf-bcp-10.txt.

Moore, B., Ellesson, E., Strassner, J. and Westerinen, A., 2001. Policy Core Information Model Specification v1, IETF, RFC3060, February.

OASIS, 2002. OASIS eXtensible Access Control Markup Language (XACML), Organization for the Advancement of Structured Information Standards, Committee Specification 1.0, October.

Policy, 2002. Policy Framework (policy) WG, IETF, http://www.ietf.org/html.charters/policy-charter.html.

Rap, 2002. Resource Allocation Protocol (rap) WG, IETF, http://www.ietf.org/html.charters/rap-charter.html

Sloman, M., 1994. Policy Driven Management for Distributed Systems. *Journal of Management Information Systems 2(4): 333-360*.

Stone, G. and Xie, G., 2001. Network Policy Languages: a survey and a new approach. *IEEE Network 15(1)*.

Westerinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Huynh, A., Carlson, M., Perry, J. and Waldbusser, S., 2001. Terminology for Policy-Based Management, IETF, RFC3198, November 2001.

XML, 1998. Extensible Markup Language (XML) 1.0, XML World Wide Web Consortium,, W3C REC-xml-19980210, February.