Policy Management Requirements

Cheh Goh
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-98-64
April, 1998

E-mail: cng@hplb.hpl.hp.com

system management, policy-based, management requirements

The use of policy in system management is increasingly being recognised as a very important part of a more advanced approach to making IT administration less daunting. However, despite the many excellent papers that have emerged in the last few years proposing ways of doing management with policy, the requirements of this approach have not been well documented. This paper attempts to spell out what the ideal policy-based management packages for IT systems should provide to an organisation, and how this will enable the IT manager to cope with the various aspects in the availability, performance and security issues in system and service support.

Internal Accession Date Only

Policy Management Requirements

Cheh Goh, cng@hplb.hpl.hp.com

Internet Business Management Department,
Hewlett Packard Laboratories,
Stoke Gifford, Bristol BS12 6QZ
United Kingdom

Abstract: The use of policy in system management is increasingly being recognised as a very important part of a more advanced approach to making IT administration less daunting. However, despite the many excellent papers that have emerged in the last few years proposing ways of doing management with policy, the requirements of this approach have not been well documented. This paper attempts to spell out what the ideal policy-based management packages for IT system should provide to an organisation, and how this will enable the IT manager to cope with the various aspects in the availability, performance and security issues in system and service support.

Keywords: system management, policy-based, management requirements.

1 Introduction

Network and system management has evolved over the years to such an extend that more and more people are beginning to be able to raise to a "higher level of abstraction" when they discuss this topic. One of the consequences of having a higher level view of the system as a whole is to be able to talk about system management in a global sense. Almost inevitably, this leads to the use of policy and high level goals to describe the desirable behaviour of an IT system which will support the business process of an enterprise.

Many papers have emerged in the last few years with the aim of understanding ways of using policy to help system management. Many of these papers concentrate on the mechanics of describing, or enforcing, different policies. What emerges to be very important is the requirements in managing the policies themselves, and how the various parties connected to the IT system would be able to deal with these managed policies. This paper aims to address this point by stating the "ideal case", with the hope that one day in the future, all the requirements may be met and the job of the IT manager would become that of a strategist, rather than a "fire fighter".

In this paper, some definition policy and its evolution life cycle will first be given, followed by separate sections clarifying the policy management requirements according to different people in an organisation. We will conclude by an assessment of the feasibility of achieving the goal of a perfect policy management system.

2 Preliminaries

2.1 Definitions

Policy, goal, and objective are usually mentioned together, and are often interchanged in discussions. For the purpose of this paper, we use the definitions given in [Goh97]:

- *objective*: a description of what is to be achieved at a high level in measurable terms.
- *implementable*: low level mechanism for achieving specific measurable results.

- *policy*: a description of the constraints imposed upon the means to achieving an *objective* or a *sub-goal*. When a policy is sufficiently refined, the constraints become executable as one or more *implementables*.

In addition, we also define the following for convenience:

- *goal* and *sub-goal*: an independent and measurable part of an objective which is thus divided for ease of management. The lowest level of a sub-goal can be executed as an *implementable*.

In the above definition, the context of operation of a system is included as part of the associated policies, because the context in which an objective is to be achieved is considered to be none other than a set of additional constraints.

2.2 Policy in an Organisation

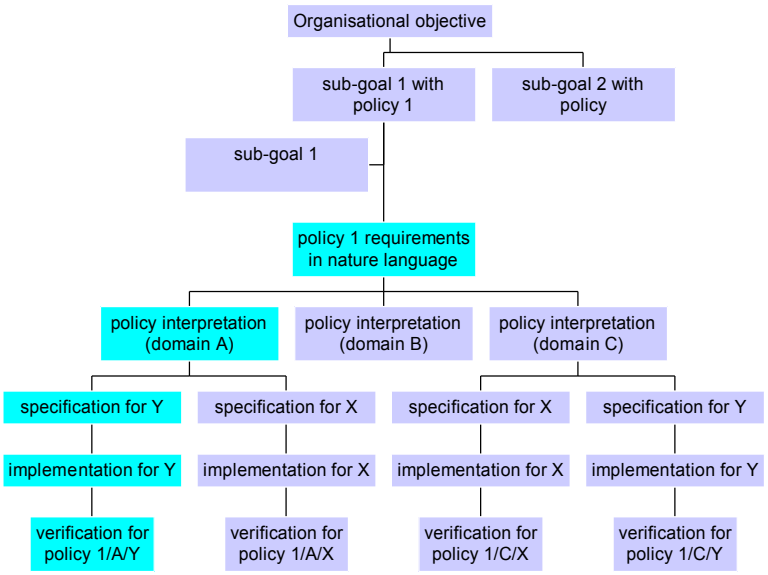

Figure 1 Policy and its implementation structure

All organisations have their business objectives. These objectives may have their accompanying policies, or may be broken down into sub-goals and have policies associated with them. In all cases, sub-goals get handed down the organisational hierarchy and at certain point, its associated policy must be interpreted in a way specific to a particular domain of the organisation. Within that domain, a policy must be further interpreted and refined until it can be enforced. This is the point when specification of device-level functions becomes possible. Management protocol must then be employed to configure the physical devices in the real world as part of policy enforcement. This generic transformation process from a high level policy to low level implementable through refinement as depicted in Figure 1 is very well known and has been amply discussed in the past such as in [Wies95, Heiler96]. The dark colour boxes constitute an instance of the path of realisation and enforcement of policy in a very specific context: a device of type **Y** in domain **A**.
The example indicates that existing high level policies are mostly written in natural language and only after interpretation and refinement would the policies appear as configuration-like information.

2.3 Policy Evolution Life-cycle

Policy Evolution Life-cycle (PEL) is the process that starts from the initial description of a top-level policy through to the low level enforcement using system configuration and audit checks. This process necessarily involves the transformation of unimplementable high level policy statements—usually in natural language—into device specific configuration for specific domain area. Because continuous changes are needed to meet the requirements of organisational operation, as well as the failure to execute some functions in the system (because all objects are subject to failure), this life-cycle must be managed.
The evolution of a policy can be separated into five key stages:

- Establishment of organisational requirements.
- Interpretation according to relevance to domain.
- Refinement to arrive at functional specification.
- Mapping for configuration in the real world.
- Monitoring and audit analysis as a way to verify policy enforcement.

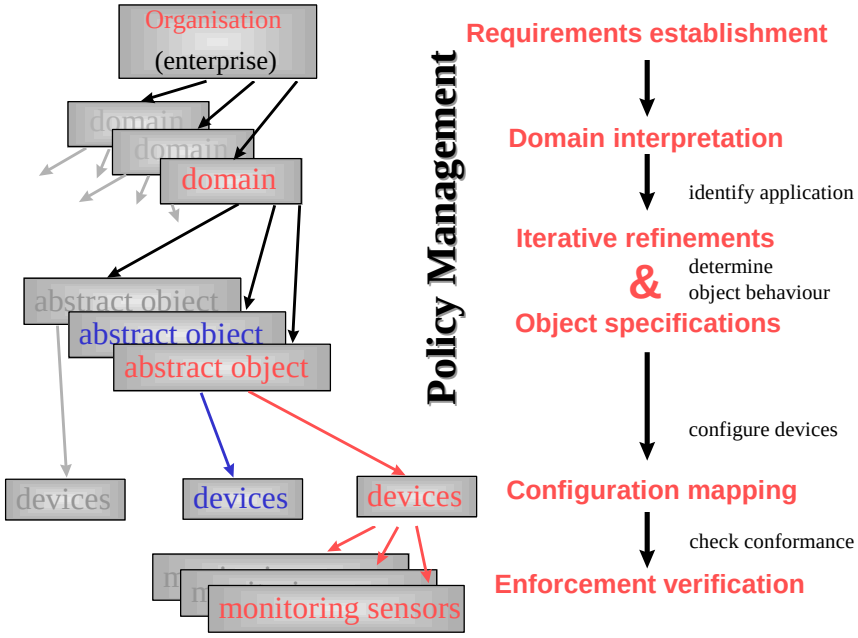

Figure 2 An abstract view of policy evolution life-cycle

The overall picture of the PEL according to these stages is depicted in Figure 2. This high level view represents a way of drawing the boundaries in the progress of an evolving policy. The concept of *specificity* can be observed in the picture, in that organisational policies become clearer because of the constraints imposed, first by the domain, then by the specific objects in that domain, and finally the actual devices being managed.

2.4 Policy Management

As can be seen, the use of policy for supporting an enterprise's business is rather involved. This contrasts with the policy-based management packages offered by some system management vendors, in that these packages are mostly rule-based and are mainly for low level configuration control. While such an approach is simple and effective for low level needs, the capability of this approach to exist in a PEL in a more integrated manner has not been demonstrated. In order for integration to happen, the management of the policies themselves is needed.

In can be argued that policy management itself does not offer real value. This, however, is true for all management related areas. The importance of policy management, however, can be glimpsed if we can take a step back to look at information technology as a whole. IT has no value unless it can effectively support the business of an organisation. In turn, IT management supports the networked IT systems, and policies are used to support the management systems. Likewise, policy management can be viewed as the last stage of the "support value chain", because policy management system can be applied to itself to manage itself.

3 Policy Management Requirements

The policy life cycle described above has many requirements, not only for enabling the management of policy, but also to make it useful for everyone who needs to deal with the policies. The requirements related to different policy users, and may be separated into two broad categories. The first is the *general* requirements, which are common to everybody in the enterprise. The other category is *specific* requirements for people with particular roles only. We make the assumption here that the system manager is responsible for communicating policies to users, and is ultimately responsible for policy enforcement.

3.1 General Requirements

In addition to the normal requirements of availability, performance and security, we need:

- **Comprehensible description language**. A policy description language which can both represent a collection of rules and be understood by policy users is essential. A user customer needs to specify policy in an integrated way that spans the PEL, and yet, it should be relatively easy to extract the semantics of the policy description.
- **Browsing from anywhere**. Whoever is affected by the policies should be able to browse the related information. The extent to which policy can be browsed will depend on the privileges of the person browsing. Clearly an auditor will have full access while a guest to the organisation will be limited in the ability to view the policies related to her role only. (This UI functionality may be combined with the next one.) Full browsing from a single point of access is also essential.
- **Accessing explanations**. Not only should one be able to look at the policy that affects oneself, it is also important to have access to the cumulative reason for the setting of policy. The purposes are twofold. On the one hand the policy setter will be able to remember the reason behind establishing a policy. This reason can easily be lost due to forgetfulness or change of administrator. On the other hand, this is a purely social factor that encourages people to conform to the policy in the organisation; people are more willing to do something when they know the reason for doing it. In some environment, the person responsible for the policy should also be contactable so that suggestions for change can be made.

3.2 Specific Requirements

In this category, the needs of the following four types of users are outlined:

- Policy setters
- Auditors
- System administrators
- End-users

When there is overlap of requirements in different categories, the requirements will not be repeated.

3.2.1 Policy Setter's Requirements

There are three different sub-categories of policy setter.

3.2.1.1 Top-level policy originator

At the very top, the corporate setter determines the *principles* of operation as policy. The requirements are:

- The ability to express the principles with "normal" daily language because it is not essential to be very specific and should not be technically orientated.
- The ability to browse the immediately next level (not low level) interpretations.

- The ability to check the consistency and integrity of low level policy interpretations.

3.2.1.2 Domain-level policy writer

The domain manager who inherits corporate policies from the head office and must make sense of them in the area over which he is responsible. The requirements are:

- The ability to retrieve the latest version of the company's policies, add information that is relevant to his domain to create more specific policies or create exceptions, and doing so while keeping notes on the reasons.
- The ability to navigate through the policy tree to understand potential interaction between his domain and other domains.
- The ability to detect policy conflicts within and external to his domain and get help to resolve these conflicts. This leads to the need of a *meta-policy*, which guides the negotiation of one's domain policy in the face of a foreign policy.
- Inspection of deployment needs and deployment results.

3.2.1.3 System specialist policy writer

The system specialist will receive from the domain manager domain level policy which is to be converted into enforcement information. The requirements are:

- The ability to easily retrieve the latest version of the domain's policies and add necessary refinement to them.
- Wizard tools that help determine the appropriate functions to meet the policies needs, and the mechanisms to implement the functions.
- Catalogue of available resource including software and hardware packages that could support the mechanisms required. These packages are expected to have the right API that can link up their configurator with the lowest level of policy at this point.
- Feedback to the domain policy writer and the top-level policy originator to make extension, adaptation, and reconsideration. This is the result of:
  - new technology: how new processes or equipment can render policy ineffective, new machine achieving different performance to allow new policy interpretation.
  - experience of enforcement: discovery of policy violation previously not thought of
  - changing orthogonal organisational requirements: new user role and mobility, new legislation, physical rearrangement.
- Feedback requirement, similar to the task of policy enforcement, is also relevant to the system administrator. See section 3.2.3.

3.2.2 Auditor's Requirements

There are two main requirements for the auditor: tractability with amenability for being traced, and verifiability. A secondary requirement is the highlighting of special cases.

- **Easy system discovery**. In addition to providing the general ability to browse and to see the reasons for the way policies evolved according to their specific contexts, the auditor must be able to examine the evolution of the policies, and see that they are tractable.
- **Effective consistency and enforcement check**. It might not be possible to conclusively prove that a static configuration made to the system definitely conforms to a given policy, but the auditor must have access to all details in the policy evolution to become satisfied that the policies at all levels are adequately consistent. The verification process includes the ability to confirm accurate static configurations, accurate mechanism for dynamic response to events, and adequate audit-trail analysis to demonstrate non-violation.

- **Ease of noticing special cases**. Special cases such as exceptions are potential weak points. They must be highlighted for easy inspection to ensure correctness of policy interpretations.

3.2.3 System Administrator's Requirements

The system administrator's normal tasks are to keep applications alive so that users can get on with their job. The administrator has to do so within the policy, so there is a cross-over of responsibility between her and the specialist policy writer. System administrator's requirements are:

- **Ease of communication to system users**. Most system policies can only be enforced if the people within the system know, understand and willingly accept them!
- **Ease of pre-setting system to respond to events**. This includes, but not limited to, compiling policies into rules or ACL, configuring devices and setting "trip-wire" or "threshold" in systems as mapping to policies. Ideally it should allow the administrator to use standard management protocols and software tools directly from the same environment, and link the events to appropriate actions.
- **Tools to test enforcement.** Testing tools to verify that when something triggers the policy, the system will respond according to the policies.
- **Ease to set up sensors, loggers and event handlers.**. The system is most probably distributed, so ease of configuration to create the audit log is vital. It should also be easy to set up analyses of the collected information for enforcement verification.
- **Instant guideline for responding to policy violation**. This is particularly vital when the violation is deliberate or hostile.
- **Effective feedback mechanism**. This will facilitate reports of policy holes, enforcement problems and improvements.

3.2.4 End User's Requirements

System end users are the ones most affected by policies. Their needs are many:

- Be informed about the policies, and be persuaded by the associated reasons for adhering to them.
- Ease of access to relevant policies—usually in the form of *guidelines*—when the need arises in the course of doing their job.
- Unintrusive enforcement that will least affect their work and behaviour. No obstructive enforcement is every acceptable or useful!
- Helpful guides to overcome frustration due to unintentional violation of policy.
- Ease of providing feedback to policy writers regarding the reasonableness of policy and improvement of its enforcement.

4 Discussion

What we have set forth in the last section is the closest to date to the ideal list of requirements for managing policy. Regardless of whether more requirements will emerge in the future, it is sufficiently formidable to try to deal with these alone. The following is a discussion of the challenges that emerge from this list.

4.1 Comprehensibility

To begin with, it is important to note that policy management is, more than other system management issues, an intensely human task. The policy setter at the top level is usually the executive officer who is not well acquainted with symbols and abstract representations. Likewise, the system end-users are unlikely to have much technical savvy. To create a management system that can be used by and

capable of meeting the needs of integrating these two types of policy users requires a fresh look at the language and presentation problem.
A policy management system must cater for different categories of users not only in words but also, if possible, in graphical view or in schematics. The integration of the user requirements in each category with a view that is appropriate to that category based on a common source of policy is a very challenging topic.

4.2 Integration

A policy management package can only be useful when it is integrated into the information technology management system in which the managed policies apply. As mentioned above, the business of an enterprise must be considered from the outset before arriving at policy management. Consequently, business information should be integrated into the management system. This is a step deeper than the general consideration of integrating IT management and business process only. The approach to such deep integration is not a well understood as yet.

4.3 Heterogeneity

As in all system management problems, heterogeneity is a challenge that will always haunt the administrator. In addition to the problem of having to deal with diverse hardware and associated software applications, policy management must take into account the general aspect that the policy is applied to. Are we talking about system availability, system performance or system security? Is it possible to have a policy management system that fulfils the needs of the grand unification, or should there be different policy manager for each consideration? These are questions that still await answers.

5 Summary

In this paper, we first elaborated upon some definitions related to policy and its management. Following that we presented policy management requirements according to the four different major categories of policy users. It is easy to see from the requirements the various challenges that present to anyone attempting to create a solution that will manage the policies for an IT system. However, it is hoped that this challenge will inspire creative work to be carried out in a way that enables IT management to become a less arduous task in the future.

References

[GOH97] Goh, C., *A Generic Approach to Policy Description in System Management*, Proceedings of the 8th IFIP/IEEE International Workshop on Distributed Systems Operations & Management, DSOM ’97, Sydney, Australia, October 1997, pp1-12.

[Wies95] Wies, R.,*Using a Classification of Management Policies for Policy Specification and Policy Transformation,* Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management, Santa Barbara, CA, USA, May 1995.

[Heiler96] Heiler,K,, Wies, R., *Policy Driven Configuration Management of Network Devices*, Proceedings of the IFIP/IEEE Network Operations & Management Symposium, Kyoto, Japan, April 1996, pp 674-689.