

Network Working Group
Internet Draft
Intended status: Informational
Expires: December 5, 2015

G. Karagiannis
J. Strassner
Huawei Technologies
Q. Sun
China Telecom
Luis M. Contreras
Telefonica
P. Yegani
Juniper Networks
J.Bi
Tsinghua University
June 5, 2015

Problem Statement for Simplified Use of Policy Abstractions (SUPA)
draft-karagiannis-supa-problem-statement-07

Abstract

The increase in complexity of modern networks makes it challenging to deploy new services and to keep networks up to date whilst maintaining stability and availability for critical business services. This is a major challenge that network operators (service providers, SME, etc) face today. The operators aim of streamlining both operations and the deployment of new services, is being met by increasingly relying on (1) software abstractions to simplify the design and configuration of monitoring and control operations and (2) the use of programmatic control over the configuration and operation of such networks.

In this context, providing network operators with a generic policy-based management model that can be used to express policies on top of arbitrary configuration data models is essential.

In particular, SUPA addresses the needs of operators and application developers to use a generic policy-based management model for defining and representing multiple types of policy rules.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
1.1	Motivation	3
2.	Terminology	4
3.	Use Case: Distributed Data Centers (DDCs)	5
4.	Requirements	6
5.	Security Considerations	6
6.	IANA Considerations	6
7.	Acknowledgements	6
8.	References	7
8.1	Normative References	7
8.2	Informative References	7
	Authors' Addresses	7

1. Introduction

Network operators are faced with networks of increasing size and complexity while trying to improve their quality and availability, as more and more business services depend on them. Software abstractions to simplify the design and configuration of monitoring and control operations and the use of programmatic control, often called software-defined, are considered by many network operators as an essential tool toward the management of that complexity.

Providing means to network operators to (1) express policies on top of arbitrary configuration data models and (2) represent multiple types of policy rules, enable significant improvements in configuration agility, error detection and uptime for operators. This document describes the problems that need to be addressed in order to equip service providers with the means, such as a generic policy-based management model used to represent multiple types of policy rules to quickly and dynamically manage their offering of network services.

1.1 Motivation

The rapid growth in the variety and importance of traffic flowing over increasingly complex enterprise and service provider network makes the task of network operations and management applications and of deploying new services much more difficult.

This is a significant challenge that network operators (service providers, SME, etc) face today.

Several mechanisms can be used to deal with this challenge. The main ones are: (1) the use of software abstractions to simplify the design and configuration of monitoring and control operations and (2) the use of programmatic control over the configuration and operation of such networks. By combining these mechanisms can (1) provide additional and significant benefits in design and deployment agility and (2) be used to define a generic policy-based management model.

In particular, the power of policy management is its applicability to many different types of systems. Many different types of actors can be identified that can use a policy management system, including applications, end-users, developers, network administrators and operators. Each of these actors, typically, has different skills and uses different concepts and terminologies. For example, an operator may want to express that only Platinum and Gold users can use streaming and interactive multimedia applications. As a second example, an operator may want to define a more concrete policy rule that looks at the number of dropped packets. If, for example, this number exceeds a certain threshold value, then the applied queuing, dropping and scheduling algorithms could be changed in order to reduce the number of dropped packets.

Both examples can be referred to as "policy rules", but they take very different forms, since they are at very different levels of abstraction and likely authored by different actors. The first example described a very abstract policy rule, and did not contain any technology-specific terms, while the second example included a more concrete policy rule and likely used technical terms of a general (e.g., IP address range, port numbers) as well as vendor-specific nature (e.g., specific algorithms implemented in a particular device). Furthermore, these two policy rules could affect each other. For example, Gold and Platinum users might need different device configurations to give the proper QoS markings to their streaming multimedia traffic. This is very difficult to do if a common policy framework does not exist.

It needs to be mentioned that there are ongoing policy modeling efforts in IETF. However, all these policy modeling models can be characterized as being technology specific. This means that the IETF needs to reinvent the wheel in different colors (i.e., policy models that apply for a specific technology) several times.

SUPA will address these challenges by:

- (1) developing an information model fragment for defining standardized policy rules at different levels of abstraction,
- (2) specifying how to map this information fragment into corresponding YANG [RFC6020] and [RFC6991], data models to define interoperable implementations that can exchange and modify generic policies using protocols such as NETCONF/RESTCONF on the interface north of the controller (or other similar management entity) and south of the service manager.

Specifically, three information model fragments are envisioned:

- (a) a generic policy information model (GPIM) that defines concepts needed by policy management independent of the form and content of the policy
- (b) a more specific information model that refines the generic information model to specify how to build policy rules of the event-condition-action (ECA) paradigm
- (c) a more specific information model that refines the generic information model to specify how to build policy rules that declaratively specify what goals to achieve (but not how to achieve those goals); this is often called "intent-based" policy

2. Terminology

Some of definitions are based on [RaBell] and/or [Stras02].

Network Service: the composition of network functions as defined by its functional and behavioral specification. A network service is characterized by performance, dependability, and security specifications. Furthermore, a network service is delivered by network service endpoints, which may be aggregations of multiple lower-layer technology specific endpoints.

Network Element: a physical or virtual entity that implements one or more network function(s). NEs can interact with local or remote network controllers in order to exchange information, such as configuration information and status.

Service specific abstraction: an abstract view of the service topology, associated with a specific network service type, e.g., inter-datacenter communication services

Policy: a definite goal, course, or method of action to guide and determine present and future decisions. Policies are implemented or executed within a particular context.

SUPA policy: a means to monitor and control the changing and/or maintaining of the state of one or more managed entities.

Policy-based management: the usage of policy rules to manage one or more entities.

Information Model: a representation of managed objects and their relationships that is independent of data repository, language, and protocol.

Data Model: a representation of managed objects and their relationships that is dependent on data repository, language, and/or protocol (typically all three).

Policy Rule: A container that uses metadata to define how the content is interpreted, and hence, how the behavior that it governs is defined separates the content of the policy from its representation provides a convenient control point for OAMP operations.

Policy condition: a representation of the necessary state and/or prerequisites that define whether a policy rule's actions should be performed.

Policy action: defines what is to be done to enforce a policy rule when its conditions are met.

Event Condition Action policy: reactive behavior of a system that correlates a set of events, a set of conditions, and a set of actions. Conditions are evaluated on the occurrence of an event and which determine whether the policy is applicable or not for that particular situation. Furthermore, the actions are only executed only if the conditions are met.

Goal (Intent) policy rule (also called a declarative policy rule, or an intent-based policy rule): a declarative statement that defines what the policy should do, but not how to implement the policy.

Model Mapping: a translation from one type of model to another type of model. Model mapping changes the representation and/or level of abstraction used to another representation and/or level of abstraction. The most common form of model mapping is from an information model to a data model; another important form is from a vendor-neutral data model to a vendor-specific data model.

3. Use Case: Distributed Data Centers (DDCs)

Large scale Distributed Data Centers (DDCs) can provide various services and usually consist of many internal and external links where various VPNs are built upon. The Service provisioning and network connectivity configurations could be complex and dynamic, for which manual configuration is not onerous and error-prone. The SUPA generic policy management models can be used to support the dynamic and automated resource usage and simplify and automate the

service/network deployment/configuration of various VPN scenarios in the DDC environment. A more detailed description of this use case is provided in [ID.draft-cheng-sup-a-ddc-use-cases].

4. Requirements

In order to satisfy the challenges mentioned in Section 1.1 and the goal of the DDC use case briefly described in section 3, the following requirements need to be addressed:

- o) Specify a generic and non-technology specific policy information model.
- o) Specify a more specific information model that defines how to build policy rules of the event-condition-action (ECA) paradigm.
- o) Specify a more specific information model that defines how to build policy rules that declaratively specify what goals (what intents) to achieve using the Goal (Intent) policy paradigm.
- o) Specify how to map the above mentioned information models into corresponding YANG standardized data models to define interoperable implementations that can exchange and modify generic policies using protocols such as NETCONF/RESTCONF on the interface north of the controller (or other similar management entity) and south of the service manager.

5. Security Considerations

Security is a key aspect of any protocol that allows state installation and extracting detailed configuration states of network elements. This places additional security requirements on SUPA (e.g., authorization, and authentication of network services) that needs further investigation. Moreover, policy interpretation can lead to corner cases and side effects that should be carefully examined, e.g., in case policy rules are conflicting with each other.

6. IANA Considerations

This document has no actions for IANA.

7. Acknowledgements

The authors of this draft would like to thank the following persons for the provided valuable feedback and contributions: Diego Lopez, Spencer Dawkins, Jun Bi, Xing Li, Chongfeng Xie, Benoit Claise, Ian Farrer, Marc Blancet, Zhen Cao, Hosnieh Rafiee, Mehmet Ersue, Simon Perreault, Fernando Gont, Jose Saldana, Tom Taylor, Kostas Pentikousis, Juergen Schoenwaelder, John Strassner, Eric Voit, Scott O. Bradner, Marco Liebsch, Scott Cadzow, Marie-Jose Montpetit.

Tina Tsou, Will Liu and Jean-Francois Tremblay contributed to an early version of this draft.

8. References

8.1. Normative References

8.2. Informative References

[ID.draft-cheng-supadddc-use-cases] Y. Cheng, JF. Tremblay, J. Bi, L. M. Contreras, "Use Case for Distributed Data Center in SUPA", IETF Internet draft (Work in progress), draft-cheng-supadddc-use-cases-07, May 8, 2015

[RFC6020] M. Bjorklund, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, October 2010.

[RFC6991] J. Schoenwaelder, "Common YANG Data Types", RFC 6991, July 2013.

[RaBel1] Raphael Romeikat, Bernhard Bauer, "Formal Specification of DomainSpecific ECA Policy Models", in Proc. 2011 Fifth IEEE International Conference on Theoretical Aspects of Software Engineering, 2011

[Stras02] John Strassner, "DEN-ng: Achieving Business-Driven Network Management" in Proc. IEEE Network Operations and Management Symposium (NOMS), 2002.

Authors' Addresses

Georgios Karagiannis
Huawei Technologies
Hansaallee 205,
40549 Dusseldorf,
Germany
Email: Georgios.Karagiannis@huawei.com

Qiong Sun
China Telecom
No.118 Xizhimennei street, Xicheng District
Beijing 100035
P.R. China
Email: sunqiong@ctbri.com.cn

Luis M. Contreras
Telefonica I+D
Ronda de la Comunicacion, Sur-3 building, 3rd floor
Madrid 28050
Spain
Email: luismiguel.contrerasmurillo@telefonica.com
URI: <http://people.tid.es/LuisM.Contreras/>

Parviz Yegani
JUNIPER NETWORKS
1133 Innovation Way
Sunnyvale, CA 94089
Email: pyegani@juniper.net

John Strassner
Huawei Technologies
2330 Central Expressway
Santa Clara, CA 95138 USA
Email: john.sc.strassner@huawei.com

Jun Bi
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China
EMail: junbi@tsinghua.edu.cn