Network Working Group
Request for Comments: 3198
Category: Informational

A. Westerinen
J. Schnizlein
Cisco Systems
J. Strassner
Intelliden Corporation
M. Scherling
xCert
B. Quinn
Celox Networks
S. Herzog
PolicyConsulting
A. Huynh
Lucent Technologies
M. Carlson
Sun Microsystems
J. Perry
Network Appliance
S. Waldbusser
November 2001

Terminology for Policy-Based Management

Status of this Memo

Copyright Notice

Abstract

This document is a glossary of policy-related terms. It provides abbreviations, explanations, and recommendations for use of these terms. The document takes the approach and format of RFC 2828, which defines an Internet Security Glossary. The intent is to improve the comprehensibility and consistency of writing that deals with network policy, particularly Internet Standards documents (ISDs).

1. Introduction

This document provides abbreviations, definitions, and explanations of terms related to network policy. All definitions are provided in Section 3, with the terms listed in alphabetical order.

The intent is to improve the comprehensibility and consistency of Internet Standards documents (ISDs) -- i.e., RFCs, Internet-Drafts, and other material produced as part of the Internet Standards Process [RFC2026]. Benefits across the ISDs are well-stated in the Introduction to RFC 2828 [RFC2828]:

- "Clear, Concise, and Easily Understood Documentation" - Requires that the set of terms and definitions be consistent, self-supporting and uniform across all ISDs.

- Technical Excellence - Where all ISDs use terminology accurately, precisely, and unambiguously.

- Prior Implementation and Testing - Requires that terms are used in their plainest form, that private and "made-up" terms are avoided in ISDs, and that new definitions are not created that conflict with established ones.

- "Openness, Fairness, and Timeliness" - Where ISDs avoid terms that are proprietary or otherwise favor a particular vendor, or that create a bias toward a particular technology or mechanism.

Common and/or controversial policy terms are defined. These terms are directly related and specific to network policy.

Wherever possible, this document takes definitions from existing ISDs. It should be noted that:

- Expired Internet-Drafts are not referenced, nor are their terminology and definitions used in this document.

- Multiple definitions may exist across the ISDs. Each definition is listed, with its source.

2. Explanation of Paragraph Markings

Section 3 marks terms and definitions as follows:

- Capitalization: Only terms that are proper nouns are capitalized.

- "P" identifies basic policy-related terms.

- "T" identifies various techniques to create or convey policy-related information in a network. For example, COPS and an "Information Model" are two techniques for communicating and describing policy-related data. SNMP and MIBs are another.

- "A" identifies specific Work Groups and general "areas of use" of policy. For example, AAA and QoS are two "areas of use" where policy concepts are extremely important to their function and operation.

3. Terms

Note: In providing policy definitions, other "technology specific" terms (for example, related to Differentiated Services) may be used and referenced. These non-policy terms will not be defined in this document, and the reader is requested to go to the referenced ISD for additional detail.

$ AAA
See "Authentication, Authorization, Accounting".

$ abstraction levels
See "policy abstraction".

$ action
See "policy action".

$ Authentication, Authorization, Accounting (AAA)
(A) AAA deals with control, authentication, authorization and accounting of systems and environments based on policies set by the administrators and users of the systems. The use of policy may be implicit - as defined by RADIUS [RFC2138]. In RADIUS, a network access server sends dial-user credentials to an AAA server, and receives authentication that the user is

who he/she claims, along with a set of attribute-value pairs authorizing various service features. Policy is implied in both the authentication, which can be restricted by time of day, number of sessions, calling number, etc., and the attribute-values authorized.

$ CIM
See "Common Information Model".

$ Common Information Model (CIM)
(T) An object-oriented information model published by the DMTF (Distributed Management Task Force) [DMTF]. It consists of a Specification detailing the abstract modeling constructs and principles of the Information Model, and a textual language definition to represent the Model. CIM's schemas are defined as a set of files, written in the language of the Specification, with graphical renderings using UML [UML]. Sets of classes and associations represent CIM's Core and

systems, devices, users, software distribution, the physical environment, networks and policy (in the Common Models). (See also "information model".)

$ Common Open Policy Service (COPS)
(T) A simple query and response TCP-based protocol that can be used to exchange policy information between a Policy Decision Point (PDP) and its clients (Policy Enforcement Points, PEPs) [RFC2748]. The COPS protocol is used to provide for the outsourcing of policy decisions for RSVP [RFC2749]. Another usage is for the provisioning of policy [RFC3084]. (See also "Policy Decision Point" and "Policy Enforcement Point".)

$ condition
See "policy condition".

$ configuration
(P) "Configuration" can be defined from two perspectives:
- The set of parameters in network elements and other systems that determine their function and operation. Some parameters are static, such as packet queue assignment and can be predefined and downloaded to a network element. Others are more dynamic, such as the actions taken by a network device upon the occurrence of some event. The distinction between static (predefined) "configuration" and the dynamic state of network elements blurs as setting parameters becomes more responsive, and signaling controls greater degrees of a network device's behavior.

- A static setup of a network element, done before shipment to a customer and which cannot be modified by the customer.

The first is the accepted usage in the Internet community.

$ COPS
See "Common Open Policy Service".

$ data model
(T) A mapping of the contents of an information model into a form that is specific to a particular type of data store or repository. A "data model" is basically the rendering of an information model according to a specific set of mechanisms for representing, organizing, storing and handling data. It has three parts [DecSupp]:
- A collection of data structures such as lists, tables, relations, etc.
- A collection of operations that can be applied to the structures such as retrieval, update, summation, etc.
- A collection of integrity rules that define the legal states (set of values) or changes of state (operations on values).

(See also "information model".)

$ DEN
See "Directory Enabled Networks".

$ Differentiated Services (DS)

the Traffic Class octet [RFC2474].
(A) "Differentiated Services" is also an "area of use" for QoS policies. It requires policy to define the correspondence between codepoints in the packet's DS-field and individual per-hop behaviors (to achieve a specified per-domain behavior). In addition, policy can be used to specify the routing of packets based on various classification criteria. (See also "Quality of Service" and "filter".)

$ diffserv
See "Differentiated Services".

$ Directory Enabled Networks (DEN)
(T) A data model that is the LDAP mapping of CIM (the Common Information Model). Its goals are to enable the deployment and use of policy by starting with common service and user concepts (defined in the information model), specifying their

mapping/storage in an LDAP-based repository, and using these concepts in vendor/device-independent policy rules [DMTF]. (See also "Common Information Model" and "data model".)

$ domain
(P) A collection of elements and services, administered in a coordinated fashion. (See also "policy domain".)

$ DS
See "Differentiated Services".

$ filter
(T) A set of terms and/or criteria used for the purpose of separating or categorizing. This is accomplished via single- or multi-field matching of traffic header and/or payload data. "Filters" are often manipulated and used in network operation and policy. For example, packet filters specify the criteria for matching a pattern (for example, IP or 802 criteria) to distinguish separable classes of traffic.

$ goal
See "policy goal".

$ information model
(T) An abstraction and representation of the entities in a managed environment, their properties, attributes and operations, and the way that they relate to each other. It is independent of any specific repository, software usage, protocol, or platform.

$ Management Information Base (MIB)
(T) A collection of information that can be accessed via the Simple Network Management Protocol. Management information is defined in MIB modules using the rules contained in SNMP's Structure of Management Information (SMI) specifications [RFC2570]. Management information is an abstract concept, and

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.