Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 6, 2009

S. Chisholm
Nortel
R. Gerhards
Adiscon GmbH

November 2, 2008

Alarms in SYSLOG
draft-ietf-opsawg-syslog-alarm-01.txt

Status of this Memo

Copyright Notice

Abstract

This document describes how to send alarm information in syslog. It includes the mapping of ITU perceived severities onto syslog message fields.

Table of Contents

1. Introduction

In addition to sending out alarm information asynchronously via protocols such as SNMP or Netconf, many implementations also log alarms via syslog. This memo defines a set of SD-PARAM to support logging and defines a mapping of syslog severity to the severity of the alarm.

1.1. terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

Alarm related terminology is defined in [RFC3877].

2. Severity Mapping

The Alarm MIB RFC3877 [RFC3877] defines ITU perceived severities which are useful to be able to relate to the syslog message fields, particularly in the case where alarms are being logged. This memo describes the representation of ITU perceived severities in appropriate syslog fields described in [Syslog]. Syslog offers both a so-called SEVERITY as well as STRUCTURED-DATA. Due to constraints in syslog, there is no one-to-one mapping possible for SEVERITY. A STRUCTURED-DATA element is defined to allow inclusion of the unmodified ITU perceived severity.

Syslog supports severity values different from ITU perceived severities. These are defined in section 6.2.1 of [Syslog]. The mapping shown in table 1 below SHOULD be used to map ITU perceived severities to syslog severities.

ITU Perceived Severity	syslog SEVERITY (Name)
Critical	1 (Alert)
Major	2 (Critical)
Minor	3 (Error)
Warning	4 (Warning)
Indeterminate	5 (Notice)
Cleared	5 (Notice)

Table 1. ITUPerceivedSeverity to syslog SEVERITY mapping.

3. Alarm STRUCTURED-DATA Elements

STRUCTURED-DATA allows to include any structured information into a syslog message. The following are defined to support structuring alarm information.

- Resource Under Alarm
- Probable Cause
- Event Type
- Perceived Severity
- Trend Indication
- Resource Mapping

Support of the alarm SD-ID is optional, but once supported some of the SD-PARARMS are mandatory.

3.1. alarmedResource

If the alarm SD-ID is supported, the alarmResource SD-PARAM MUST be supported. This item uniquely identifies the resource under alarm within the scope of a network element.

3.2. probableCause

If the alarm SD-ID is supported, the probableCause SD-PARAM MUST be supported. This parameter is the mnemonic associated with the IANAItuProbableCause object defined within [RFC3877] and any subsequent extensions defined by IANA. For example, IANAItuProbableCause defines a transmission failure to a probable cause of 'transmissionError (10)'. The value of the parameter in this case would be 'transmissionError'"

3.3. perceivedSeverity

If the alarm SD-ID is supported, the perceivedSeverity SD-PARAM MUST be supported. Similar to the definition of perceived severity in [X.736] and [RFC3877], this object can take the following values:

- cleared
- indeterminate

- critical
- major
- minor
- warning

See section 2 for the relationship between this severity and syslog severity.

3.4. eventType

If the alarm SD-ID is supported, the eventType SD-PARAM SHOULD be supported. This parameter is the mnemonic associated with the IANAItuEventType object defined within [RFC3877] and any subsequent extensions defined by IANA. For example, IANAItuEventType defines a environmental alarm to a event type of 'environmentalAlarm (6)'. The value of the parameter in this case would be 'environmentalAlarm'"

3.5. trendIndication

If the alarm SD-ID is supported, the trendIndication SD-PARAM SHOULD be supported. Similar to the definition of perceived severity in [X.733] and [RFC3877], this object can take the following values:

- moreSevere
- noChange
- lessSevere

3.6. resourceMapping

If the alarm SD-ID is supported, the resourceMapping SD-PARAM SHOULD be supported. This item uniquely identifies the resource under alarm within the scope of a network element. This must be the same value as alarmActiveResourceId [RFC3877] for this alarm or follow similar semantics if the Alarm MIB is not supported.

4. Security Considerations

In addition to general syslog security considerations discussed in [Syslog], the information contained with alarms may provide hackers with helpful information about parts of the system currently experiencing stress as well as general information about the system such as inventory.

Users should not have access to information in alarms that their normal access permissions would not permit if the information was accessed in another manner.

5. IANA Considerations

IANA is requested to register the SD-IDs and PARAM-NAMEs shown below:

SD-ID	PARAM-NAME	
alarm		OPTIONAL
	alarmedResource	MANDATORY
	probableCause	MANDATORY
	perceivedSeverity	MANDATORY
	eventType	OPTIONAL
	trendIndication	OPTIONAL
	resourceMapping	OPTIONAL

6. Acknowledgments

Thanks to members of the Syslog and OPSAWG work group who contributed to this specification.

7. References

7.1. Normative References

[RFC2119] Bradner, s., "Key words for RFCs to Indicate Requirements Levels", RFC 2119, March 1997.

[RFC3877] Chisholm, S. and D. Romascanu, "Alarm Management Information Base (MIB)", RFC 3877, September 2004.

[Syslog] Gerhards, Rainer., "The syslog Protocol", ID draft-ietf-syslog-protocol-19.txt, November 2006.

7.2. Informative References

[X.733] ITU-T, ""Information Technology - Open Systems Interconnection - System Management: Alarm Reporting Function"", ITU-T X.733, 1992.

[X.736] ITU-T, ""Information Technology - Open Systems Interconnection - System Management: Security Alarm Reporting Function"", ITU-T X.736, 1992.

Authors' Addresses

Sharon Chisholm
Nortel
3500 Carling Ave
Nepean, Ontario K2H 8E9
Canada

Email: schishol@nortel.com

Rainer Gerhards
Adiscon GmbH
Mozartstrasse 21
Grossrinderfeld, BW 97950
Germany

Email: rgerhards@adiscon.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).