

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: December 21, 2008

S. Chisholm  
Nortel  
R. Gerhards  
Adiscon GmbH  
June 19, 2008

Alarms in SYSLOG  
draft-ietf-opsawg-syslog-alarm-00.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on December 21, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Internet-Draft

Alarms in SYSLOG

June 2008

## 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">3</a>
<a href="#">1.1.</a>	terminology . . . . .	<a href="#">3</a>
<a href="#">1.2.</a>	Severity Mapping . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Alarm STRUCTURED-DATA Elements . . . . .	<a href="#">4</a>
<a href="#">2.1.</a>	alarmedResource . . . . .	<a href="#">4</a>
<a href="#">2.2.</a>	probableCause . . . . .	<a href="#">4</a>
<a href="#">2.3.</a>	perceivedSeverity . . . . .	<a href="#">4</a>
<a href="#">2.4.</a>	eventType . . . . .	<a href="#">5</a>
<a href="#">2.5.</a>	trendIndication . . . . .	<a href="#">5</a>
<a href="#">2.6.</a>	resourceMapping . . . . .	<a href="#">5</a>
<a href="#">3.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">4.</a>	IANA Considerations . . . . .	<a href="#">7</a>
<a href="#">5.</a>	Acknowledgments . . . . .	<a href="#">8</a>
<a href="#">6.</a>	References . . . . .	<a href="#">9</a>
<a href="#">6.1.</a>	Normative References . . . . .	<a href="#">9</a>
<a href="#">6.2.</a>	Informative References . . . . .	<a href="#">9</a>
	Authors' Addresses . . . . .	<a href="#">10</a>
	Intellectual Property and Copyright Statements . . . . .	<a href="#">11</a>

## 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](#)].

### 1.2. 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.

## [2.](#) 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.

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

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

### [2.1.](#) 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.

### [2.2.](#) 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'"

### [2.3.](#) 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:

- o cleared
- o indeterminate

- o critical
- o major
- o minor
- o warning

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

### [2.4.](#) 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 an environmental alarm to an event type of 'environmentalAlarm (6)'. The value of the parameter in this case would be 'environmentalAlarm'"

### [2.5.](#) 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:

- o moreSevere
- o noChange
- o lessSevere

## 2.6. 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.

## 3. 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.

#### [4.](#) 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



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

## [6.](#) References

### [6.1.](#) 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.

### [6.2.](#) 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.

Internet-Draft

Alarms in SYSLOG

June 2008

Authors' Addresses

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

Email: [schishol@nortel.com](mailto:schishol@nortel.com)

Rainer Gerhards  
Adiscon GmbH  
Mozartstrasse 21  
Grossrinderfeld, BW 97950  
Germany

Email: [rgerhards@adiscon.com](mailto:rgerhards@adiscon.com)

Internet-Draft

Alarms in SYSLOG

June 2008

### Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

### Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this

specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at [ietf-ipr@ietf.org](mailto:ietf-ipr@ietf.org).

#### Acknowledgment

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