Network Working Group
Request for Comments: 5674
Category: Standards Track

S. Chisholm
Nortel
R. Gerhards
Adiscon GmbH

October 2009

Alarms in Syslog

Abstract

This document describes how to send alarm information in syslog. It includes the mapping of ITU perceived severities onto syslog message fields. It also includes a number of alarm-specific SD-PARAM definitions from X.733 and the IETF Alarm MIB.

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Table of Contents

1. Introduction

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

The Alarm MIB [RFC3877] includes mandatory alarm fields from X.733 [X.733] as well as information from X.736 [X.736]. In additional, the Alarm MIB introduces its own alarm fields. This memo reuses terminology and fields from the Alarm MIB.

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].

Alarm-related terminology is defined in [RFC3877].

SD-ID, SD-PARAM, and other syslog-related terms are defined in [RFC5424].

2. Severity Mapping

The Alarm MIB [RFC3877] defines ITU perceived severities; it is useful to be able to relate these 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, which are described in [RFC5424]. 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 in this document 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 [RFC5424]. 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 the inclusion of any structured information into a syslog message. The following are defined in this document to support the structuring of alarm information.

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

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

3.1. resource

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

3.2. probableCause

If the "alarm" SD-ID is included, the "probableCause" SD-PARAM MUST be included. 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 included, the "perceivedSeverity" SD-PARAM MUST be included. 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 included, the "eventType" SD-PARAM SHOULD be included. 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'.

3.5. trendIndication

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

- moreSevere
- noChange
- lessSevere

3.6. resourceURI

If the "alarm" SD-ID is included, the "resourceURI" SD-PARAM SHOULD be included. This item uniquely identifies the resource under alarm.

The value of this field MUST conform to the URI definition in [RFC3986] and its updates. In the case of an SNMP resource, the syntax in [RFC4088] MUST be used and "resourceURI" must point to the same resource as alarmActiveResourceId [RFC3877] for this alarm.

Both the "resource" and the "resourceURI" parameters point at the resource experiencing the alarm, but the "resourceURI" has syntactic constraint requiring it to be a URI. This makes it easy to correlate this syslog alarm with any alarms that are received via other protocols, such as SNMP, or to use SNMP or other protocols to get additional information about this resource.

4. Examples

Example 1 - Mandatory Alarm Information

```
<165>1 2003-10-11T22:14:15.003Z mymachine.example.com
evntslog - ID47 [exampleSDID@32473 iut="3" eventSource=
"Application" eventID="1011"][alarm resource="su root"
probableCause="unauthorizedAccessAttempt"
perceivedSeverity="major"]
BOMAn application event log entry...
```

In this example, extended from [RFC5424], the VERSION is 1 and the Facility has the value of 4. The severity is 2. The message was created on 11 October 2003 at 10:14:15pm UTC, 3 milliseconds into the next second. The message originated from a host that identifies itself as "mymachine.example.com". The APP-NAME is "evntslog" and the PROCID is unknown. The MSGID is "ID47". We have included both the structured data from the original example, a single element with the value "[exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"]", and a new element with the alarm information defined in this memo. The alarm SD-ID contains the mandatory SD-PARAMS of resource, probableCause, and preceivedSeverity. The MSG itself is "An application event log entry..." The BOM at the beginning of the MSG indicates UTF-8 encoding.

Example 2 - Additional Alarm Information

```
<165>1 2004-11-10T20:15:15.003Z mymachine.example.com
evntslog - ID48 [alarm resource="interface 42"
probableCause="unauthorizedAccessAttempt"
perceivedSeverity="major"
eventType="communicationsAlarm"
resourceURI="snmp://example.com//1.3.6.1.2.1.2.2.1.1.42"]
```

In this example, we include two optional alarm fields: eventType and resourceURI.

5. Security Considerations

In addition to the general syslog security considerations discussed in [RFC5424], 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 were accessed in another manner.

There is no standardized access control model for syslog, and hence the ability to filter alarms based on a notion of a receiver identity is, at best, implementation specific.

6. IANA Considerations

IANA registered the syslog Structured Data ID values and PARAM-NAMEs shown below:

SD-ID	PARAM-NAME	
alarm		OPTIONAL
	resource	MANDATORY
	probableCause	MANDATORY
	perceivedSeverity	MANDATORY
	eventType	OPTIONAL
	trendIndication	OPTIONAL
	resourceURI	OPTIONAL

7. Acknowledgments

Thanks to members of the Syslog and OPSAWG work group who contributed to this specification. We'd also like to thank Juergen Schoenwaelder, Dave Harrington, Wes Hardaker, and Randy Presuhn for their reviews.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

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

[RFC3986] Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[RFC4088] Black, D., McCloghrie, K., and J. Schoenwaelder, "Uniform Resource Identifier (URI) Scheme for the Simple Network Management Protocol (SNMP)", RFC 4088, June 2005.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, March 2009.

8.2. 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