Network Working Group
Request for Comments: 5427
Category: Standards Track

G. Keeni
Cyber Solutions Inc.

March 2009

Textual Conventions for Syslog Management

Status of This Memo

Copyright Notice

Abstract

This MIB module defines textual conventions to represent Facility and Severity information commonly used in syslog messages. The intent is that these textual conventions will be imported and used in MIB modules that would otherwise define their own representations.

Table of Contents

1. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

2. Background

Operating systems, processes, and applications, collectively termed "Facilities" in the following, generate messages indicating their own status or the occurrence of events. These messages have come to be known as syslog messages. A syslog message in general will contain among other things a code representing the Facility that generated the message and a code representing the Severity of the message. The Facility and the Severity codes are commonly used to categorize and select received syslog messages for processing and display. The Facility codes have been useful in qualifying the originator of the content of the messages but in some cases they are not specific enough to explicitly identify the originator. Implementations of the syslog protocol [RFC5424] that contain structured data elements (SDEs) should use these SDEs to clarify the entity that originated the content of the message.

This document defines a set of textual conventions (TCs) that can be used to represent Facility and Severity codes commonly used in syslog messages.

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 RFC 2119 [RFC2119].

3. The Syslog Textual Conventions MIB

```
SYSLOG-TC-MIB DEFINITIONS ::= BEGIN

IMPORTS
    MODULE-IDENTITY, mib-2
              FROM SNMPv2-SMI        -- [RFC2578]
    TEXTUAL-CONVENTION
              FROM SNMPv2-TC;        -- [RFC2579]

syslogTCMIB  MODULE-IDENTITY
    LAST-UPDATED "200903300000Z"     --  30 March 2009
    ORGANIZATION "IETF Syslog Working Group"
    CONTACT-INFO
    "                       Glenn Mansfield Keeni
                   Postal: Cyber Solutions Inc.
                           6-6-3, Minami Yoshinari
                           Aoba-ku, Sendai, Japan 989-3204.
                      Tel: +81-22-303-4012
                      Fax: +81-22-303-4015
                    EMail: glenn@cysols.com

      Support Group EMail: syslog@ietf.org
      "

    DESCRIPTION
        "The MIB module containing textual conventions for syslog
         messages.

         Copyright (c) 2009 IETF Trust and the persons
         identified as authors of the code.  All rights reserved.

         Redistribution and use in source and binary forms, with or
         without modification, are permitted provided that the
         following conditions are met:

         - Redistributions of source code must retain the above
           copyright notice, this list of conditions and the
           following disclaimer.

         - Redistributions in binary form must reproduce the above
           copyright notice, this list of conditions and the
           following disclaimer in the documentation and/or other
           materials provided with the distribution.
```

```
            - Neither the name of Internet Society, IETF or IETF
              Trust, nor the names of specific contributors, may be
              used to endorse or promote products derived from this
              software without specific prior written permission.

            THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
            CONTRIBUTORS 'AS IS' AND ANY EXPRESS OR IMPLIED
            WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
            WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
            PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE COPYRIGHT
            OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
            INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
            (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
            GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR
            BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
            LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
            (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
            OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
            POSSIBILITY OF SUCH DAMAGE.

            This version of this MIB module is part of RFC 5427;
            see the RFC itself for full legal notices.
           "

        REVISION "200903300000Z"     --  30 March 2009
        DESCRIPTION
            "The initial version, published as RFC 5427."

        ::= { mib-2 173 }

    -- ------------------------------------------------------------
    -- Textual Conventions
    -- ------------------------------------------------------------

    SyslogFacility  ::=  TEXTUAL-CONVENTION
        STATUS  current
        DESCRIPTION
            "This textual convention enumerates the Facilities that
             originate syslog messages.

             The Facilities of syslog messages are numerically coded
             with decimal values.  For interoperability and backwards-
             compatibility reasons, this document specifies a
             normative mapping between a label, which represents a
             Facility, and the corresponding numeric value.  This label
             could be used in, for example, SNMP Manager user
             interfaces.
```

```
            The label itself is often semantically meaningless
            because it is impractical to attempt to enumerate all
            possible Facilities, and many daemons and processes do
            not have an explicitly assigned Facility code or label.
            For example, there is no Facility label corresponding to
            an HTTP service.  An HTTP service implementation might log
            messages as coming from, for example, 'local7' or 'uucp'.
            This is typical current practice, and originators, relays,
            and collectors can be configured to properly handle this
            situation.  For improved accuracy, an application can also
            include an APP-NAME structured data element.

            Note that operating system mechanisms for configuring
            syslog, such as syslog.conf, have not yet been standardized
            and might use different sets of Facility labels and/or
            mapping between Facility labels and Facility codes than the
            MIB.

            In particular, the labels corresponding to Facility codes 4,
            10, 13, and 14, and the code corresponding to the Facility
            label 'cron' are known to vary across different operating
            systems.  To distinguish between the labels corresponding
            to Facility codes 9 and 15, a label of 'cron2' is assigned
            to the Facility code 15.  This list is not intended to be
            exhaustive; other differences might exist, and new
            differences might be introduced in the future.

            The mapping specified here MUST be used in a MIB network
            management interface, even though a particular syslog
            implementation might use a different mapping in a
            different network management interface.
          "
        REFERENCE "The Syslog Protocol (RFC5424): Table 1"
        SYNTAX  INTEGER
             {

               kern            (0), -- kernel messages
               user            (1), -- user-level messages
               mail            (2), -- mail system messages
               daemon          (3), -- system daemons' messages
               auth            (4), -- authorization messages
               syslog          (5), -- messages generated internally by
                                    -- syslogd
               lpr             (6), -- line printer subsystem messages
               news            (7), -- network news subsystem messages
               uucp            (8), -- UUCP subsystem messages
               cron            (9), -- clock daemon messages
               authpriv        (10),-- security/authorization messages
```

```
              ftp             (11),-- ftp daemon messages
              ntp             (12),-- NTP subsystem messages
              audit           (13),-- audit messages
              console         (14),-- console messages
              cron2           (15),-- clock daemon messages
              local0          (16),
              local1          (17),
              local2          (18),
              local3          (19),
              local4          (20),
              local5          (21),
              local6          (22),
              local7          (23)
            }

   SyslogSeverity  ::=  TEXTUAL-CONVENTION
       STATUS  current
       DESCRIPTION
           "This textual convention enumerates the Severity levels
            of syslog messages.

            The Severity levels of syslog messages are numerically
            coded with decimal values.  For interoperability and
            backwards-compatibility reasons, this document specifies
            a normative mapping between a label, which represents a
            Severity level, and the corresponding numeric value.
            This label could be used in, for example, SNMP Manager
            user interfaces.

            The label itself is often semantically meaningless
            because it is impractical to attempt to strictly define
            the criteria for each Severity level, and the criteria
            that is used by syslog originators is, and has
            historically been, implementation-dependent.

            Note that operating system mechanisms for configuring
            syslog, such as syslog.conf, have not yet been standardized
            and might use different sets of Severity labels and/or
            mapping between Severity labels and Severity codes than the
            MIB.

            For example, the foobar application might log messages as
            'crit' based on some subjective criteria.  Yet the operator
            can configure syslog to forward these messages, even though
            the criteria for 'crit' may differ from one originator to
            another.  This is typical current practice, and originators,
            relays, and collectors can be configured to properly handle
            this situation.
```

```
        "
    REFERENCE "The Syslog Protocol (RFC5424): Table 2"
    SYNTAX  INTEGER
         {
           emerg          (0),  -- emergency; system is unusable
           alert          (1),  -- action must be taken immediately
           crit           (2),  -- critical condition
           err            (3),  -- error condition
           warning        (4),  -- warning condition
           notice         (5),  -- normal but significant condition
           info           (6),  -- informational message
           debug          (7)   -- debug-level messages

         }

END
```

4. Security Considerations

This module does not define any management objects. Instead, it defines a set of textual conventions which may be used by other MIB modules to define management objects. Meaningful security considerations can only be written in the MIB modules that define management objects. This document has therefore no impact on the security of the Internet. Since objects defined using the TCs defined in this document may introduce security issues, the user of these TCs should read the security considerations section of [RFC5424].

5. IANA Considerations

The MIB modules in this document use the following IANA-assigned OBJECT IDENTIFIER values recorded in the SMI Numbers registry:

Descriptor	OBJECT IDENTIFIER value
syslogTCMIB	{ mib-2 173 }

6. References

6.1. Normative References

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

[RFC2578] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

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

6.2. Informative References

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

7. Acknowledgments

This document is a product of the Syslog Working Group. The author would like to thank Chris Lonvick, David Harrington, Juergen Schoenwaelder, and Pasi Eronen for their comments and suggestions.

Author’s Address

Glenn Mansfield Keeni
Cyber Solutions Inc.
6-6-3 Minami Yoshinari
Aoba-ku, Sendai 989-3204
Japan

Phone: +81-22-303-4012
EMail: glenn@cysols.com