Network Working Group J. Schoenwaelder
Internet-Draft Jacobs University Bremen
Intended status: Standards Track A. Clemm
Expires: August 14, 2009 A. Karmakar
Cisco Systems
February 10, 2009

Definitions of Managed Objects for Mapping SYSLOG Messages to Simple Network Management Protocol (SNMP) Notifications
draft-ietf-opsawg-syslog-msg-mib-00.txt

Status of this Memo

This Internet-Draft will expire on August 14, 2009.

Copyright Notice

Abstract

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in the Internet community. In particular, it defines a mapping of SYSLOG messages to Simple Network Management Protocol (SNMP) notifications.

Table of Contents

1. Introduction

SNMP [RFC3410] [RFC3411] and SYSLOG [I-D.ietf-syslog-protocol] are two widely used protocols to communicate event notifications. Although co-existence of several management protocols in one operational environment is possible, certain environments require that all event notifications are collected by a single system daemon such as a SYSLOG collector or an SNMP notification receiver via a single management protocol. In such environments, it is necessary to translate event notifications between management protocols.

This document defines an SNMP MIB module to represent SYSLOG messages and to send SYSLOG messages as SNMP notifications to SNMP notification receivers.

2. 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] .

3. Conventions

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].

4. Overview

SYSLOG messages are converted by a SYSLOG to SNMP converter. Such a converter acts as a SYSLOG receiver [I-D.ietf-syslog-protocol] and implements a MIB module according to the SNMP architecture [RFC3411]. The converter might be tightly coupled to an SNMP agent or it might interface with an SNMP agent via a subagent protocol.

After initialization, the converter will listen for SYSLOG messages.

On receiving a message, the message will be parsed to extract information as described in the MIB module. A conceptual table is populated with information extracted from the SYSLOG message and finally a notification may be generated.

The MIB module is organized into a group of scalars and two tables. The syslogMsgControl group contains two scalars controlling the maximum size of SYSLOG messages recorded in the tables and whether SNMP notifications are generated for SYSLOG messages.

```
--syslogMsgObjects(1)
  |
  +--syslogMsgControl(1)
     |
     +-- Unsigned32 syslogMsgTableMaxSize(1)
     +-- TruthValue syslogMsgEnableNotifications(2)
```

The syslogMsgTable contains one entry for each recorded SYSLOG message. The basic fields of SYSLOG messages are represented in different columns of the conceptual table.

```
--syslogMsgObjects(1)
  |
  +--syslogMsgTable(2)
     |
     +--syslogMsgEntry(1) [syslogMsgIndex]
        |
        +-- Unsigned32              syslogMsgIndex(1)
        +-- SyslogFacility          syslogMsgFacility(2)
        +-- SyslogSeverity          syslogMsgSeverity(3)
        +-- Unsigned32              syslogMsgVersion(4)
        +-- DateAndTimeMicroSeconds syslogMsgTimeStamp(5)
        +-- DisplayString           syslogMsgHostName(6)
        +-- DisplayString           syslogMsgAppName(7)
        +-- DisplayString           syslogMsgProcID(8)
        +-- DisplayString           syslogMsgMsgID(9)
        +-- OctetString             syslogMsgMsg(10)
        +-- Bits                    syslogMsgFlags(11)
```

The syslogMsgSDTable contains one entry for each structured data element parameter contained in a SYSLOG message. Since structured data elements are optional, the relationship between the syslogMsgTable and the syslogMsgSDTable is 1:0..*.

```
   --syslogMsgObjects(1)
     |
     +--syslogMsgSDTable(3)
        |
        +--syslogMsgSDEntry(1) [syslogMsgIndex,
           |                    syslogMsgSDElementName,
           |                    syslogMsgSDParamName,
           |                    syslogMsgSDParamIndex]
           |
           +-- DisplayString   syslogMsgSDElementName(1)
           +-- DisplayString   syslogMsgSDParamName(2)
           +-- Unsigned32      syslogMsgSDParamIndex(3)
           +-- SnmpAdminString syslogMsgSDParamValue(4)
```

5. Relationship to Other MIB Modules

The NOTIFICATION-LOG-MIB [RFC3014] provides a generic mechanism for logging SNMP notifications in order to deal with lost SNMP notifications, e.g., due to transient communication problems. Applications can poll the notification log to verify that they have not missed important SNMP notifications.

The MIB module defined in this memo provides a mechanism for logging SYSLOG notifications. This additional SYSLOG notification log is provided because (a) SYSLOG messages might not lead to SNMP notification (this is configurable) and (b) SNMP notifications might not carry all information associated with a SYSLOG notification.

The following MIB module IMPORTS objects from SNMPv2-SMI [RFC2578], SNMPv2-TC [RFC2579], SNMPv2-CONF [RFC2580], SNMP-FRAMEWORK-MIB [RFC3411], and SYSLOG-TC-MIB [I-D.ietf-syslog-tc-mib].

6. Definitions

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

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE, NOTIFICATION-TYPE, Unsigned32, mib-2
        FROM SNMPv2-SMI
    TEXTUAL-CONVENTION, DisplayString, TruthValue
        FROM SNMPv2-TC
    OBJECT-GROUP, NOTIFICATION-GROUP, MODULE-COMPLIANCE
        FROM SNMPv2-CONF
    SnmpAdminString
        FROM SNMP-FRAMEWORK-MIB
    SyslogFacility, SyslogSeverity
```

```
        FROM SYSLOG-TC-MIB;

syslogMsgMib MODULE-IDENTITY
    LAST-UPDATED "200902100800Z"
    ORGANIZATION "IETF OPSAWG Working Group"
    CONTACT-INFO
        "Juergen Schoenwaelder
         <j.schoenwaelder@jacobs-university.de>
         Jacobs University Bremen
         Campus Ring 1
         28757 Bremen
         Germany

         Alexander Clemm
         <alex@cisco.com>
         Cisco Systems
         170 West Tasman Drive
         San Jose, CA 95134-1706
         USA

         Anirban Karmakar
         <akarmaka@cisco.com>
         Cisco Systems
         170 West Tasman Drive
         San Jose, CA 95134-1706
         USA"
    DESCRIPTION
        "This MIB module represent SYSLOG messages as SNMP objects.

         Copyright (c) 2009 IETF Trust and the persons identified as
         the document authors.  All rights reserved. This version of
         this MIB module is part of RFC XXXX; see the RFC itself for
         full legal notices."
    REVISION "200902100800Z"
    DESCRIPTION
        "Initial version issued as part of RFC XXXX."
-- RFC Ed.: replace XXXX with actual RFC number & remove this note
    ::= { mib-2 XXX }
-- RFC Ed.: replace XXX with IANA-assigned number & remove this note

-- textual convention definitions

DateAndTimeMicroSeconds ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "2d-1d-1d,1d:1d:1d.3d,1a1d:1d"
    STATUS       current
    DESCRIPTION
       "A date-time specification. This type is similar to the
        DateAndTime type defined in the SNMPv2-TC except that
```

```
        the subsecond granulation is microseconds instead of
        deciseconds.

        field  octets  contents                  range
        -----  ------  --------                  -----
          1      1-2   year*                     0..65536
          2       3    month                     1..12
          3       4    day                       1..31
          4       5    hour                      0..23
          5       6    minutes                   0..59
          6       7    seconds                   0..60
                       (use 60 for leap-second)
          7     8-10   microseconds              0..999999
          8      11    direction from UTC        '+' / '-'
          9      12    hours from UTC*           0..13
         10      13    minutes from UTC          0..59

        * Notes:
        - the value of year is in network-byte order
        - the value of microseconds is in network-byte order
        - daylight saving time in New Zealand is +13

        For example, Tuesday May 26, 1992 at 1:30:15 PM EDT would be
        displayed as:

                        1992-5-26,13:30:15.0,-4:0

        Note that if only local time is known, then timezone
        information (fields 11-13) is not present."
    SYNTAX      OCTET STRING (SIZE (10 | 13))

-- object definitions

syslogMsgNotifications OBJECT IDENTIFIER ::= { syslogMsgMib 0 }
syslogMsgObjects       OBJECT IDENTIFIER ::= { syslogMsgMib 1 }
syslogMsgConformance   OBJECT IDENTIFIER ::= { syslogMsgMib 2 }

syslogMsgControl       OBJECT IDENTIFIER ::= { syslogMsgObjects 1 }

syslogMsgTableMaxSize OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "The maximum number of syslog messages that may be held in
        syslogMsgTable.  A particular setting does not guarantee that
        there is sufficient memory available for the maximum number
        of table entries indicated by this object. A value of 0 means
```

```
        no limit.

        If an application reduces the limit while there are syslog
        messages in the syslogMsgTable, the syslog messages that are
        in the syslogMsgTable for the longest time MUST be discarded
        to bring the table down to the new limit.

        The value of this object should be kept in nonvolatile
        memory."
    DEFVAL      { 0 }
    ::= { syslogMsgControl 1 }

syslogMsgEnableNotifications OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Indicates whether syslogMsgNotification notifications are
        generated.

        The value of this object should be kept in nonvolatile
        memory."
    DEFVAL      { false }
    ::= { syslogMsgControl 2 }

syslogMsgTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SyslogMsgEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "A table containing recent syslog messages. The size of the
        table is controlled by the syslogMsgTableMaxSize object."
    ::= { syslogMsgObjects 2 }

syslogMsgEntry OBJECT-TYPE
    SYNTAX      SyslogMsgEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "An entry of the syslogMsgTable."
    INDEX { syslogMsgIndex }
    ::= { syslogMsgTable 1 }

SyslogMsgEntry ::= SEQUENCE {
    syslogMsgIndex      Unsigned32,
    syslogMsgFacility   SyslogFacility,
    syslogMsgSeverity   SyslogSeverity,
    syslogMsgVersion    Unsigned32,
```

```
    syslogMsgTimeStamp  DateAndTimeMicroSeconds,
    syslogMsgHostName   DisplayString,
    syslogMsgAppName    DisplayString,
    syslogMsgProcID     DisplayString,
    syslogMsgMsgID      DisplayString,
    syslogMsg           OCTET STRING,
    syslogMsgFlags      BITS
}

syslogMsgIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "A monotonically increasing number used to identify entries in
        the syslogMsgTable. When syslogMsgIndex reaches the maximum
        value the value wraps back to 1."
    ::= { syslogMsgEntry 1 }

syslogMsgFacility OBJECT-TYPE
    SYNTAX      SyslogFacility
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The facility of the syslog message."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.1)
        RFCZZZZ: Textual Conventions for Syslog Management"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    -- RFC Ed.: replace ZZZZ with SYSLOG TC RFC number, remove this note
    ::= { syslogMsgEntry 2 }

syslogMsgSeverity OBJECT-TYPE
    SYNTAX      SyslogSeverity
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The severity of the syslog message"
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.1)
        RFCZZZZ: Textual Conventions for Syslog Management"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    -- RFC Ed.: replace ZZZZ with SYSLOG TC RFC number, remove this note
    ::= { syslogMsgEntry 3 }

syslogMsgVersion OBJECT-TYPE
    SYNTAX      Unsigned32 (0..999)
    MAX-ACCESS  read-only
```

```
    STATUS      current
    DESCRIPTION
       "The version of the syslog message. A value of 0 indicates
        that the version is unknown."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.2)"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    ::= { syslogMsgEntry 4 }

syslogMsgTimeStamp OBJECT-TYPE
    SYNTAX      DateAndTimeMicroSeconds
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The timestamp of the syslog message. The special value
        '000000000000000000000'H is returned if the timestamp
        is unknown."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.3)"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    ::= { syslogMsgEntry 5 }

syslogMsgHostName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (0..255))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The host name of the syslog message. A zero-length string
        indicates an unknown host name."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.4)"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    ::= { syslogMsgEntry 6 }

syslogMsgAppName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (0..48))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The app-name of the syslog message. A zero-length string
        indicates an unknown app-name."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.5)"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    ::= { syslogMsgEntry 7 }

syslogMsgProcID OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (0..128))
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The procid of the syslog message. A zero-length string
        indicates an unknown procid."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.6)"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    ::= { syslogMsgEntry 8 }

syslogMsgMsgID OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The msgid of the syslog message. A zero-length string
        indicates an unknown msgid."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.2.7)"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    ::= { syslogMsgEntry 9 }

syslogMsgMsg OBJECT-TYPE
    SYNTAX      OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The message part of the syslog message. The syntax does not
        impose a size restriction. Implementations of this MIB module
        may truncate the message part of the syslog message such that
        it fits into the size constraints imposed by the
        implementation environment. If the message has been truncated
        by the SYSLOG to SNMP converter, the truncated bit in the
        syslogMsgFlags must be set to 1.

        If the first octets contain the value 'EFBBBF'h, then the rest
        of the message is a UTF-8 string. Since syslog messages may be
        truncated at arbitrary octet boundaries during forwarding, the
        message may contain invalid UTF-8 encodings at the end."
    REFERENCE
       "RFCYYYY: The syslog Protocol (section 6.4)"
    -- RFC Ed.: replace YYYY with SYSLOG RFC number & remove this note
    ::= { syslogMsgEntry 10 }

syslogMsgFlags OBJECT-TYPE
    SYNTAX      BITS { truncated(0), sdparams(1) }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
       "The bits contained in this object convey meta information
        about the syslog message. The meaning of the bits is as
        follows:

        truncated -  This bit is set if the converter had to
                     truncate the syslogMsgMsg to comply with
                     implementation and/or SNMP message size
                     constraints.

        sdparams  -  This bit is set if the syslog messages
                     contained structured data element parameters
                     and serves as an indicator whether there is
                     data in the syslogMsgSDTable for this syslog
                     message.

        For syslog messages without structured data element parameters
        that were not truncated by the converter, none of the bits is
        set."
    ::= { syslogMsgEntry 11 }

syslogMsgSDTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SyslogMsgSDEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "A table containing structured data elements of syslog
        messages."
    ::= { syslogMsgObjects 3 }

syslogMsgSDEntry OBJECT-TYPE
    SYNTAX      SyslogMsgSDEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "An entry of the syslogMsgSDTable."
    INDEX { syslogMsgIndex, syslogMsgSDElementName,
            syslogMsgSDParamName, syslogMsgSDParamIndex }
    ::= { syslogMsgSDTable 1 }

SyslogMsgSDEntry ::= SEQUENCE {
    syslogMsgSDElementName DisplayString,
    syslogMsgSDParamName   DisplayString,
    syslogMsgSDParamIndex  Unsigned32,
    syslogMsgSDParamValue  SnmpAdminString
}

syslogMsgSDElementName OBJECT-TYPE
```

```
    SYNTAX      DisplayString (SIZE (1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "The name of a structured data element."
    ::= { syslogMsgSDEntry 1 }

syslogMsgSDParamName OBJECT-TYPE
    SYNTAX      DisplayString (SIZE (1..32))
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "The name of a parameter of the structured data element."
    ::= { syslogMsgSDEntry 2 }

syslogMsgSDParamIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "This objects indexes the instance of a structured data element
        that occurs multiple times in a structured data element,
        starting from 1. For parameters that only occure once, the
        value of this object is 1."
    ::= { syslogMsgSDEntry 3 }

syslogMsgSDParamValue OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "The value of the parameter of a syslog message identified by
        the index of this table."
    ::= { syslogMsgSDEntry 4 }

-- notification definitions

syslogMsgNotification NOTIFICATION-TYPE
    OBJECTS     { syslogMsgFacility, syslogMsgSeverity,
                  syslogMsgVersion, syslogMsgTimeStamp,
                  syslogMsgHostName, syslogMsgAppName,
                  syslogMsgProcID, syslogMsgMsgID,
                  syslogMsgMsg, syslogMsgFlags }
    STATUS      current
    DESCRIPTION
       "The syslogMsgNotification is generated when a new syslog
        message is generated and the value of
        syslogMsgGenerateNotifications is true.
```

```
        Implementations may add syslogMsgSDParamValue objects as long
        as the resulting notification fits into the size constraints
        imposed by the implementation environment and the notification
        message size constraints imposed by maxMessageSize [RFC3412]
        and SNMP transport mappings."
    ::= { syslogMsgNotifications 1 }

-- conformance statements

syslogMsgGroups      OBJECT IDENTIFIER ::= { syslogMsgConformance 1 }
syslogMsgCompliances OBJECT IDENTIFIER ::= { syslogMsgConformance 2 }

syslogMsgFullCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
       "The compliance statement for implementations of the
        SYSLOG-MSG-MIB."
    MODULE      -- this module
    MANDATORY-GROUPS {
        syslogMsgGroup,
        syslogMsgSDGroup,
        syslogMsgControlGroup,
        syslogMsgNotificationGroup
    }
    ::= { syslogMsgCompliances 1 }

syslogMsgReadOnlyCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
       "The compliance statement for implementations of the
        SYSLOG-MSG-MIB that do not support read-write access."
    MODULE      -- this module
    MANDATORY-GROUPS {
        syslogMsgGroup,
        syslogMsgSDGroup,
        syslogMsgControlGroup,
        syslogMsgNotificationGroup
    }
    OBJECT syslogMsgTableMaxSize
       MIN-ACCESS  read-only
       DESCRIPTION
          "Write access is not required."
    OBJECT syslogMsgEnableNotifications
       MIN-ACCESS  read-only
       DESCRIPTION
          "Write access is not required."
    ::= { syslogMsgCompliances 2 }
```

```
syslogMsgNotificationCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
       "The compliance statement for implementations of the
        SYSLOG-MSG-MIB that do only generate notifications and not
        provide a table to allow read access to syslog message
        details."
    MODULE      -- this module
    MANDATORY-GROUPS {
        syslogMsgGroup,
        syslogMsgSDGroup,
        syslogMsgNotificationGroup
    }
    OBJECT      syslogMsgFacility
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
        "Read access is not required."
    OBJECT      syslogMsgSeverity
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgVersion
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgTimeStamp
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgHostName
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgAppName
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgProcID
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgMsgID
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgMsg
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
```

```
       "Read access is not required."
    OBJECT      syslogMsgFlags
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    OBJECT      syslogMsgSDParamValue
    MIN-ACCESS  accessible-for-notify
    DESCRIPTION
       "Read access is not required."
    ::= { syslogMsgCompliances 3 }

syslogMsgNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
        syslogMsgNotification
    }
    STATUS      current
    DESCRIPTION
       "The notifications emitted by this MIB module."
    ::= { syslogMsgGroups 1 }

syslogMsgGroup OBJECT-GROUP
    OBJECTS {
        -- syslogMsgIndex,
        syslogMsgFacility,
        syslogMsgSeverity,
        syslogMsgVersion,
        syslogMsgTimeStamp,
        syslogMsgHostName,
        syslogMsgAppName,
        syslogMsgProcID,
        syslogMsgMsgID,
        syslogMsgMsg,
        syslogMsgFlags
    }
    STATUS      current
    DESCRIPTION
       "A collection of objects representing a syslog message
        excluding structured data elements."
    ::= { syslogMsgGroups 2 }

syslogMsgSDGroup OBJECT-GROUP
    OBJECTS {
        -- syslogMsgSDElementName,
        -- syslogMsgSDParamName,
        -- syslogMsgSDParamIndex,
        syslogMsgSDParamValue
    }
    STATUS      current
```

```
    DESCRIPTION
       "A collection of objects representing the structured data
        elements of a syslog message."
    ::= { syslogMsgGroups 3 }

syslogMsgControlGroup OBJECT-GROUP
    OBJECTS {
        syslogMsgTableMaxSize,
        syslogMsgEnableNotifications
    }
    STATUS      current
    DESCRIPTION
       "A collection of control objects to control the size of the
        syslogMsgTable and to enable / disable notifications."
    ::= { syslogMsgGroups 4 }

END
```

7. Usage Example

The following example shows a valid syslog message including structured data. The otherwise-unprintable Unicode BOM is represented as "BOM" in the example.

```
  <165>1 2003-10-11T22:14:15.003Z mymachine.example.com
  evntslog - ID47 [exampleSDID@0 iut="3" eventSource="Application"
  eventID="1011"] BOMAn application event log entry...
```

This syslog message leads to the following entries in the syslogMsgTable and the syslogMsgSDTable (note that string indexes are written as strings for readability reasons):

```
  syslogMsgIndex.1 = 1
  syslogMsgFacility.1 = 20
  syslogMsgSeverity.1 = 5
  syslogMsgVersion.1 = 1
  syslogMsgTimeStamp.1 = 2003-10-11 22:14:15.003+00:00
  syslogMsgHostName.1 = "mymachine.example.com"
  syslogMsgAppName.1 = "evntslog"
  syslogMsgProcID.1 = "-"
  syslogMsgMsgID.1 = "ID47"
  syslogMsgMsg.1 = "BOMAn application event log entry..."
  syslogMsgSDParamValue.1."exampleSDID@0"."iut".1
      = "3"
  syslogMsgSDParamValue.1."exampleSDID@0"."eventSource".1
      = "Application"
  syslogMsgSDParamValue.1."exampleSDID@0"."eventID".1
```

```
         = "1011"
```

8. IANA Considerations

The IANA is requested to assign a value for "XXX" under the 'mib-2' subtree and to record the assignment in the SMI Numbers registry. When the assignment has been made, the RFC Editor is asked to replace "XXX" (here and in the MIB module) with the assigned value.

9. Security Considerations

There are a number of management objects defined in this MIB module with a MAX-ACCESS clause of read-write and/or read-create. Such objects may be considered sensitive or vulnerable in some network environments. The support for SET operations in a non-secure environment without proper protection can have a negative effect on network operations. These are the tables and objects and their sensitivity/vulnerability:

- syslogMsgTableMaxSize: This object controls how many entries are kept in the syslogMsgTable. Unauthorized modifications may either cause increased memory consumption or turn off the capability to retrieve notifications using GET class operations. This be used to hide traces of an attack.
- syslogMsgEnableNotifications: This object enables notifications. Unauthorized modifications to disable notification generation can be used to hide an attack. Unauthorized modifications to enable notification generation may be used as part of a denial of service attack against a network management system if for exampe the syslog server accepts unauthorized syslog messages.

Some of the readable objects in this MIB module (i.e., objects with a MAX-ACCESS other than not-accessible) may be considered sensitive or vulnerable in some network environments. It is thus important to control even GET and/or NOTIFY access to these objects and possibly to even encrypt the values of these objects when sending them over the network via SNMP. These are the tables and objects and their sensitivity/vulnerability:

- syslogMsgTableMaxSize, syslogMsgEnableNotifications: These objects provide information whether SYSLOG messages are forwarded as SNMP notifications and how many messages will be maintained in the syslogMsgTable. This information might be exploited by an attacker in order to plan actions with the goal of hiding attack activities.

- syslogMsgFacility, syslogMsgSeverity, syslogMsgVersion, syslogMsgTimeStamp, syslogMsgHostName, syslogMsgAppName, syslogMsgProcID, syslogMsgMsgID, syslogMsgMsg, syslogMsgFlags, syslogMsgSDParamValue: These objects carry the content of syslog messags and the syslog message oriented security considerations of [I-D.ietf-syslog-protocol] apply. In particular, an attacker who gains access to SYSLOG messages via SNMP may use the knowledge gained from SYSLOG messages to compromise a machine or do other damage.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

10. Acknowledgments

The authors wish to thank Rainer Gerhards, Wes Hardacker, David Harrington, Juergen Quittek, and all other people who commented on various versions of this proposal.

11. References

11.1. Normative References

[I-D.ietf-syslog-protocol]
Gerhards, R., "The syslog Protocol", Internet Draft (work in progress), September 2007.

[I-D.ietf-syslog-tc-mib]
Keeni, G., "Textual Conventions for Syslog Management", Internet Draft (work in progress), May 2008.

[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)", RFC 2578, STD 58, April 1999.

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

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

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

11.2. Informative References

[RFC3014] Kavasseri, R., Ed., "Notification Log MIB", RFC 3014, November 2002.

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

Authors' Addresses

Juergen Schoenwaelder
Jacobs University Bremen
Campus Ring 1
28725 Bremen
Germany

Email: j.schoenwaelder@jacobs-university.de

Alexander Clemm
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Email: alex@cisco.com

Anirban Karmakar
Cisco Systems
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Email: akarmaka@cisco.com