NETMOD WG
Internet-Draft
Intended status: Informational
Expires: May 10, 2015

Clyde Wildes
Cisco Systems
Agrahara Kiran Koushik
Brocade Communication Systems

Nov 10, 2014

SYSLOG YANG model
draft-ietf-netmod-syslog-model-00

Abstract

This document describes a data model for Syslog protocol which is used to convey event notification messages.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Operating systems, processes and applications generate messages indicating their own status or the occurence of events. These messages are useful for managing and/or debugging the network and its services. The BSD Syslog protocol is a widely adopted protocol that is used for transmission and processing of the messages.

Since each process, application and operating system was written somewhat independently, there is little uniformity to the content of Syslog messages. For this reason, no assumption is made upon the formatting or contents of the messages. The protocol is simply designed to transport these event messages. No acknowledgement of the receipt is made.

Essentially, a Syslog process receives messages (from the kernel, processes, applications or other Syslog processes) and processes those. The processing involves logging to a local file, displaying on console, user terminal, and/or relaying to syslog processes on other machines. The processing is determined by the "facility" that originated the message and the "severity" assigned to the message by the facility.

We are using definitions of Syslog protocol from [RFC3164] in this draft.

1.1. Definitions and Acronyms

IP: Internet Protocol

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

UDP: User Datagram Protocol

VRF: Virtual Routing and Forwarding

2. Problem Statement

This document defines a YANG [RFC6020] configuration data model that may be used to monitor and control one or more syslog processes running on a system. YANG models can be used with network management agents such as NETCONF [RFC6241] to install, manipulate, and delete the configuration of network devices.

This module makes use of the YANG "feature" construct which allows implementations to support only those Syslog features that lie within their capabilities.

3. Design of the SYSLOG Model

The syslog model was designed by comparing various syslog features implemented by various vendors' in different implementations.

This draft addresses the common leafs between all vendors and creates a common model, which can be augmented with proprietary features, if necessary. The base model is designed to be very simple for maximum flexibility.

Syslog consists of message producers, a group level suppression filter, and message distributors. The following digram shows syslog messages flowing from a message producer, through the group level suppression filter, and if passed by the group filter to message distributors where further suppression filtering can take place.

```
   Message Producers
    +-------------+  +-------------+  +-------------+  +-------------+
    |  Various    |  |     OS      |  |             |  |   Remote    |
    | Components  |  |   Kernel    |  | Line Cards  |  |   Servers   |
    +-------------+  +-------------+  +-------------+  +-------------+

    +-------------+  +-------------+  +-------------+  +-------------+
    |    SNMP     |  |  Interface  |  |   Standby   |  |   Syslog    |
    |   Events    |  |   Events    |  |  Supervisor |  |   Itself    |
    +-------------+  +-------------+  +-------------+  +-------------+

    |                                                                |
    +----------------------------------------------------------------+
                 |
                 |
                 v

   Group Level Suppression
    +------------------------------+
    | Filter by message facility   |
    | and message severity         |
    +------------------------------+
                 |
                 |
                 |
           +-----+---------+----------------+-----------------+
           |               |                |                 |
           v               v                v                 v

   Message Distributors
    +-------------+  +-------------+  +-------------+  +-------------+
    |             |  |             |  |    User     |  |   Remote    |
    |   Console   |  | Log File(s) |  |  Terminals  |  |   Servers   |
    +-------------+  +-------------+  +-------------+  +-------------+
```

The leaves in the base syslog model correspond to the group level suppression filter and each message distributor:

- console
- log file(s)
- user terminals
- remote server(s).

Optional features are used to specified fields that are not present in all vendor configurations.

3.1. SYSLOG Module

```
module: ietf-syslog
   +--rw syslog
      +--rw global-logging-action {global-logging-action}?
      |  +--rw (logging-level-scope)?
      |  |  +--:(logging-facility-all)
      |  |  |  +--rw (logging-severity-scope)?
      |  |  |     +--:(logging-severity-all)
      |  |  |     |  +--rw all?                                 empty
      |  |  |     +--:(logging-severity)
      |  |  |        +--rw severity?
syslogtypes:Severity
      |  |  +--:(logging-facility-none)
      |  |  |  +--rw none?                                empty
      |  |  +--:(logging-facility)
      |  |     +--rw logging-facilities* [facility]
      |  |        +--rw facility    identityref
      |  |        +--rw (logging-severity-scope)?
      |  |           +--:(logging-severity-all)
      |  |           |  +--rw all?        empty
      |  |           +--:(logging-severity)
      |  |              +--rw severity?   syslogtypes:Severity
      |  +--rw logging-advanced-level-processing {selector-advanced-level-
processing-config}?
      |  |  +--rw (logging-severity-operator)?
      |  |     +--:(default)
      |  |     |  +--rw default?      empty
      |  |     +--:(equals)
      |  |     |  +--rw equals?       empty
      |  |     +--:(not-equals)
      |  |        +--rw not-equals?   empty
      |  +--rw logging-match-processing {selector-match-processing-config}?
      |     +--rw pattern-match?   string
      +--rw console-logging-action
      |  +--rw (logging-level-scope)?
      |  |  +--:(logging-facility-all)
      |  |  |  +--rw (logging-severity-scope)?
      |  |  |     +--:(logging-severity-all)
      |  |  |     |  +--rw all?                                 empty
      |  |  |     +--:(logging-severity)
      |  |  |        +--rw severity?
syslogtypes:Severity
      |  |  +--:(logging-facility-none)
      |  |  |  +--rw none?                                empty
      |  |  +--:(logging-facility)
      |  |     +--rw logging-facilities* [facility]
      |  |        +--rw facility    identityref
      |  |        +--rw (logging-severity-scope)?
      |  |           +--:(logging-severity-all)
      |  |           |  +--rw all?        empty
      |  |           +--:(logging-severity)
      |  |              +--rw severity?   syslogtypes:Severity
      |  +--rw logging-advanced-level-processing {selector-advanced-level-
processing-config}?
      |  |  +--rw (logging-severity-operator)?
      |  |     +--:(default)
      |  |     |  +--rw default?      empty
      |  |     +--:(equals)
      |  |     |  +--rw equals?       empty
      |  |     +--:(not-equals)
      |  |        +--rw not-equals?   empty
      |  +--rw logging-match-processing {selector-match-processing-config}?
      |     +--rw pattern-match?   string
      +--rw file-logging-action
      |  +--rw file-name                            inet:uri
      |  +--rw (logging-level-scope)?
      |  |  +--:(logging-facility-all)
      |  |  |  +--rw (logging-severity-scope)?
      |  |  |     +--:(logging-severity-all)
      |  |  |     |  +--rw all?                                 empty
      |  |  |     +--:(logging-severity)
      |  |  |        +--rw severity?
syslogtypes:Severity
      |  |  +--:(logging-facility-none)
      |  |  |  +--rw none?                                empty
      |  |  +--:(logging-facility)
      |  |     +--rw logging-facilities* [facility]
      |  |        +--rw facility    identityref
      |  |        +--rw (logging-severity-scope)?
      |  |           +--:(logging-severity-all)
      |  |           |  +--rw all?        empty
      |  |           +--:(logging-severity)
      |  |              +--rw severity?   syslogtypes:Severity
      |  +--rw logging-advanced-level-processing {selector-advanced-level-
processing-config}?
      |  |  +--rw (logging-severity-operator)?
      |  |     +--:(default)
      |  |     |  +--rw default?      empty
      |  |     +--:(equals)
      |  |     |  +--rw equals?       empty
      |  |     +--:(not-equals)
      |  |        +--rw not-equals?   empty
      |  +--rw logging-match-processing {selector-match-processing-config}?
      |  |  +--rw pattern-match?   string
      |  +--rw file-logging-structured-data?        boolean {file-logging-
structured-data}?
      |  +--rw file-logging-archive {file-logging-archive-config}?
      |     +--rw file-number?       uint32
      |     +--rw file-size?         uint32
      |     +--rw file-permission?   enumeration
      +--rw remote-logging-action
      |  +--rw remote-logging-destination* [destination]
      |     +--rw destination                          inet:host
      |     +--rw (logging-level-scope)?
      |     |  +--:(logging-facility-all)
      |     |  |  +--rw (logging-severity-scope)?
      |     |  |     +--:(logging-severity-all)
      |     |  |     |  +--rw all?                                 empty
      |     |  |     +--:(logging-severity)
      |     |  |        +--rw severity?
syslogtypes:Severity
      |     |  +--:(logging-facility-none)
      |     |  |  +--rw none?                                empty
      |     |  +--:(logging-facility)
      |     |     +--rw logging-facilities* [facility]
      |     |        +--rw facility    identityref
      |     |        +--rw (logging-severity-scope)?
      |     |           +--:(logging-severity-all)
      |     |           |  +--rw all?        empty
      |     |           +--:(logging-severity)
      |     |              +--rw severity?   syslogtypes:Severity
      |     +--rw logging-advanced-level-processing {selector-advanced-level-
processing-config}?
      |     |  +--rw (logging-severity-operator)?
      |     |     +--:(default)
      |     |     |  +--rw default?      empty
      |     |     +--:(equals)
      |     |     |  +--rw equals?       empty
      |     |     +--:(not-equals)
      |     |        +--rw not-equals?   empty
      |     +--rw logging-match-processing {selector-match-processing-config}?
      |     |  +--rw pattern-match?   string
      |     +--rw destination-facility?                identityref
      |     +--rw source-interface?                    if:interface-ref
      |     +--rw vrf-name?                            string {remote-logging-
use-vrf}?
      |     +--rw syslog-sign! {signed-messages-config}?
      |        +--rw certInitialRepeat?   uint16
      |        +--rw certResendDelay?     uint16
      |        +--rw certResendCount?     uint16
      |        +--rw sigMaxDelay?         uint16
      |        +--rw sigNumberResends?    uint16
      |        +--rw sigResendDelay?      uint16
      |        +--rw sigResendCount?      uint16
      +--rw terminal-logging-action
         +--rw (user-scope)?
            +--:(all-users)
            |  +--rw all-users
            |     +--rw (logging-level-scope)?
            |     |  +--:(logging-facility-all)
            |     |  |  +--rw (logging-severity-scope)?
            |     |  |     +--:(logging-severity-all)
            |     |  |     |  +--rw all?                                empty
            |     |  |     +--:(logging-severity)
            |     |  |        +--rw severity?
syslogtypes:Severity
            |     |  +--:(logging-facility-none)
            |     |  |  +--rw none?                                empty
            |     |  +--:(logging-facility)
            |     |     +--rw logging-facilities* [facility]
            |     |        +--rw facility    identityref
            |     |        +--rw (logging-severity-scope)?
            |     |           +--:(logging-severity-all)
            |     |           |  +--rw all?        empty
            |     |           +--:(logging-severity)
            |     |              +--rw severity?   syslogtypes:Severity
            |     +--rw logging-advanced-level-processing {selector-advanced-
level-processing-config}?
            |     |  +--rw (logging-severity-operator)?
            |     |     +--:(default)
            |     |     |  +--rw default?      empty
            |     |     +--:(equals)
            |     |     |  +--rw equals?       empty
            |     |     +--:(not-equals)
            |     |        +--rw not-equals?   empty
            |     +--rw logging-match-processing {selector-match-processing-
config}?
            |        +--rw pattern-match?   string
            +--:(per-user) {terminal-facility-user-logging-config}?
               +--rw user-name* [uname]
                  +--rw uname                                string
                  +--rw (logging-level-scope)?
                  |  +--:(logging-facility-all)
                  |  |  +--rw (logging-severity-scope)?
                  |  |     +--:(logging-severity-all)
                  |  |     |  +--rw all?                                empty
                  |  |     +--:(logging-severity)
                  |  |        +--rw severity?
syslogtypes:Severity
                  |  +--:(logging-facility-none)
                  |  |  +--rw none?                                empty
                  |  +--:(logging-facility)
                  |     +--rw logging-facilities* [facility]
                  |        +--rw facility    identityref
                  |        +--rw (logging-severity-scope)?
                  |           +--:(logging-severity-all)
                  |           |  +--rw all?        empty
                  |           +--:(logging-severity)
                  |              +--rw severity?   syslogtypes:Severity
                  +--rw logging-advanced-level-processing {selector-advanced-
level-processing-config}?
                  |  +--rw (logging-severity-operator)?
                  |     +--:(default)
                  |     |  +--rw default?      empty
                  |     +--:(equals)
                  |     |  +--rw equals?       empty
                  |     +--:(not-equals)
                  |        +--rw not-equals?   empty
                  +--rw logging-match-processing {selector-match-processing-
config}?
                     +--rw pattern-match?   string
```

4. SYSLOG YANG Models

4.1. SYSLOG-TYPES module

```
module ietf-syslog-types {
  namespace "urn:ietf:params:xml:ns:yang:ietf-syslog-types";
  prefix syslogtypes;

  organization "IETF NETMOD (NETCONF Data Modeling Language) Working
                Group";
  contact
    "WG Web:   <http://tools.ietf.org/wg/netmod/>
     WG List:  <mailto:netmod@ietf.org>

     WG Chair: Juergen Schoenwaelder
               <mailto:j.schoenwaelder@jacobs-university.de>

     WG Chair: Tom Nadeau
               <mailto:tnadeau@brocade.com>

     Editor:   Clyde Wildes
               <mailto:cwildes@cisco.com>

     Editor:   Agrahara Kiran Koushik
               <mailto:kkoushik@brocade.com>";
  description
    "This module contains a collection of YANG type definitions for
     SYSLOG.";

  revision 2014-10-24 {
    description
      "syslog-model-04 Revision";
    reference
      "This model references RFC 5424 - The Syslog Protocol,
       and RFC 5848 - Signed Syslog Messages.";
  }

  typedef Severity {
    type enumeration {
      enum "emergency" {
        value 0;
        description
          "Emergency Level Msg";
      }
      enum "alert" {
        value 1;
        description
          "Alert Level Msg";
      }
      enum "critical" {
        value 2;
        description
          "Critical Level Msg";
      }
      enum "error" {
        value 3;
        description
          "Error Level Msg";
      }
      enum "warning" {
        value 4;
        description
          "Warning Level Msg";
      }
      enum "notice" {
        value 5;
        description
          "Notification Level Msg";
      }
      enum "info" {
        value 6;
        description
          "Informational Level Msg";
      }
      enum "debug" {
        value 7;
        description
          "Debugging Level Msg";
      }
    }
    description
      "The definitions for Syslog message severity.";
  }

  identity syslog-facility {
    description
      "The base identity to represent syslog facilities";
  }

  identity kern {
    base syslog-facility;
    description
      "The facility for kernel messages as defined in RFC 5424.";
  }

  identity user {
    base syslog-facility;
    description
      "The facility for user-level messages as defined in RFC 5424.";
  }

  identity mail {
    base syslog-facility;
    description
      "The facility for the mail system as defined in RFC 5424.";
  }

  identity daemon {
    base syslog-facility;
    description
      "The facility for the system daemons as defined in RFC 5424.";
   }
  identity auth {
    base syslog-facility;
    description
      "The facility for security/authorization messages as defined
       in RFC 5424.";
  }

  identity syslog {
    base syslog-facility;
    description
      "The facility for messages generated internally by syslogd
       facility as defined in RFC 5424.";
  }

  identity lpr {
    base syslog-facility;
    description
      "The facility for the line printer subsystem as defined in
       RFC 5424.";
  }

  identity news {
    base syslog-facility;
    description
      "The facility for the network news subsystem as defined in
       RFC 5424.";
  }

  identity uucp {
    base syslog-facility;
    description
      "The facility for the UUCP subsystem as defined in RFC 5424.";
  }

  identity cron {
    base syslog-facility;
    description
      "The facility for the clock daemon as defined in RFC 5424.";
  }

  identity authpriv {
    base syslog-facility;
    description
      "The facility for privileged security/authorization messages
       as defined in RFC 5424.";
  }

  identity ftp {
    base syslog-facility;
```

```
      description
        "The facility for the FTP daemon as defined in RFC 5424.";
    }
```

```
  identity ntp {
    base syslog-facility;
    description
      "The facility for the NTP subsystem as defined in RFC 5424.";
  }

  identity audit {
    base syslog-facility;
    description
      "The facility for log audit messages as defined in RFC 5424.";
  }

  identity console {
    base syslog-facility;
    description
      "The facility for log alert messages as defined in RFC 5424.";
  }

  identity cron2 {
    base syslog-facility;
    description
      "The facility for the second clock daemon as defined in
       RFC 5424.";
  }

  identity local0 {
    base syslog-facility;
    description
      "The facility for local use 0 messages as defined in
       RFC 5424.";
  }

  identity local1 {
    base syslog-facility;
    description
      "The facility for local use 1 messages as defined in
       RFC 5424.";
  }

  identity local2 {
    base syslog-facility;
    description
      "The facility for local use 2 messages as defined in
       RFC 5424.";
  }

  identity local3 {
    base syslog-facility;
    description
```

```
      "The facility for local use 3 messages as defined in
       RFC 5424.";
  }

  identity local4 {
    base syslog-facility;
    description
      "The facility for local use 4 messages as defined in
       RFC 5424.";
  }
  identity local5 {
    base syslog-facility;
    description
      "The facility for local use 5 messages as defined in
       RFC 5424.";
  }

  identity local6 {
    base syslog-facility;
    description
      "The facility for local use 6 messages as defined in
       RFC 5424.";
  }

  identity local7 {
    base syslog-facility;
    description
      "The facility for local use 7 messages as defined in
       RFC 5424.";
  }
}
```

4.2. SYSLOG module

```
module ietf-syslog {
  namespace "urn:ietf:params:xml:ns:yang:ietf-syslog";
  prefix syslog;

  import ietf-inet-types {
    prefix inet;
  }

  import ietf-interfaces {
    prefix if;
  }

  import ietf-syslog-types {
    prefix syslogtypes;
  }

  organization "IETF NETMOD (NETCONF Data Modeling Language) Working
                Group";
  contact
    "WG Web:   <http://tools.ietf.org/wg/netmod/>
     WG List:  <mailto:netmod@ietf.org>

     WG Chair: Juergen Schoenwaelder
               <mailto:j.schoenwaelder@jacobs-university.de>
     WG Chair: Tom Nadeau
               <mailto:tnadeau@brocade.com>

     Editor:   Clyde Wildes
               <mailto:cwildes@cisco.com>

     Editor:   Agrahara Kiran Koushik
               <mailto:kkoushik@brocade.com>";
```

```
  description
    "This module contains a collection of YANG definitions
     for Syslog configuration.";

  revision 2014-10-24 {
    description
      "syslog-model-04 Revision";
    reference
      "This model references RFC 5424 - The Syslog Protocol,
       and RFC 5848 - Signed Syslog Messages.";
  }

  feature global-logging-action {
    description
      "This feature represents the ability to suppress log
       messages on the global level.";
  }

  feature file-logging-structured-data {
    description
      "This feature represents the ability to log messages
       to a file in structured-data format as per RFC 5424.";
  }

  feature file-logging-archive-config {
    description
      "This feature represents the ability to archive log files.";
  }

  feature remote-logging-use-vrf {
    description
      "This feature allows remote logging of messages to a
       particular VRF.";
  }

  feature terminal-facility-user-logging-config {
    description
      "This feature represents the ability to adjust
       log message settings for individual terminal users.";
  }

  feature selector-advanced-level-processing-config {
    description
      "This feature represents the ability to select messages
       using the additional operators equal to, or not equal to
       when comparing the Syslog message severity.";
  }

  feature selector-match-processing-config {
    description
      "This feature represents the ability to select messages based
       on a Posix 1003.2 regular expression pattern match.";
  }

  feature signed-messages-config {
    description
      "This feature represents the ability to configure signed
       syslog messages according to RFC 5848.";
  }
```

```
  grouping syslog-severity {
    description
      "This grouping defines the Syslog severity which is used to
       filter log messages. Choose one of the following:
         logging-severity-all
         logging-severity <severity>";
    choice logging-severity-scope {
      description
        "This choice describes the option to specify all severities
         or a specific severity.";
      case logging-severity-all {
        description
          "This case specifies all severities.";
        leaf all {
          type empty;
          description
          "This leaf specifies that all severities participate in
           the filtering of Syslog messages.";
        }
      }
      case logging-severity {
        description
          "This case specifies a specific severity to participate
           in the filtering of Syslog messages.";
        leaf severity {
          type syslogtypes:Severity;
          description
            "This leaf specifies the Syslog message severity.";
        }
      }
    }
  }

  grouping syslog-selector {
    description
      "This grouping defines a Syslog selector which is used to
       filter log messages for the given action in which the
       selector appears. Choose one of the following:
         logging-facility-all <severity>
         logging-facility-none
         logging-facility [<facility> <severity>...]
       Additional severity comparison operations are available
       using the logging-advanced-level-processing container. If
       the logging-advanced-level-processing container is not
       present all messages of the specified severity and higher
       are logged according to the given action.";
    choice logging-level-scope {
      description
        "This choice describes the option to specify all
```

```
           facilities, no facilities, or a specific facility.";
        case logging-facility-all {
          description
            "This case specifies all facilities will match when
             comparing the Syslog message facility.";
          uses syslog-severity;
        }
```

```
      case logging-facility-none {
        description
          "This case specifies no facilities will match when
           comparing the Syslog message facility. This is a method
           that can be used to turn an action off.";
        leaf none {
          type empty;
          description
          "This leaf specifies that no facilities participate in the
           filtering of Syslog messages for this action.";
        }
      }
      case logging-facility {
        description
          "This case specifies one or more specified facilities
           will match when comparing the Syslog message facility.";
        list logging-facilities {
          key "facility";
          description
            "This list describes a collection of Syslog facilities
             and severities.";
          leaf facility {
            type identityref {
              base syslogtypes:syslog-facility;
            }
            description
              "The leaf uniquely identifies a Syslog facility.";
          }
          uses syslog-severity;
        }
      }
    }
    container logging-advanced-level-processing {
      if-feature selector-advanced-level-processing-config;
      description
        "This container describes the configuration parameters for
         advanced Syslog selector severity comparison.";
      choice logging-severity-operator {
        description
          "This choice describes the option to specify how the
           severity comparison is performed.";
        case default {
          description
            "All messages of the specified severity and higher are
             logged according to the given action";
          leaf default {
            type empty;
            description
            "This leaf specifies the default behavior.";
           }
         }
```

```
        case equals {
          description
            "All messages of the specified severity are logged
             according to the given action";
          leaf equals {
            type empty;
            description
            "This leaf specifies all messages for the speicified
             severity.";
          }
        }
        case not-equals {
          description
            "All messages that are not of the specified severity are
             logged according to the given action";
          leaf not-equals {
            type empty;
            description
            "This leaf specifies all messages that are not for the
             speicified severity.";
          }
        }
      }
    }
    container logging-match-processing {
      if-feature selector-match-processing-config;
      description
        "This container describes the configuration parameters for
         matching Syslog messages using a regular expression pattern
         match.";
      leaf pattern-match {
        type string;
        description
          "This leaf describes a Posix 1003.2 regular expression
           string that can be used to select a Syslog message for
           logging.";
      }
    }
  }

  container syslog {
    config true;
    description
      "This container describes the configuration parameters for
       Syslog.";
    container global-logging-action {
      if-feature global-logging-action;
      description
        "This container describes the configuration parameters for
```

```
           global logging. Global logging represents the ability to
           perform global log message suppression.";
        uses syslog-selector;
      }
      container console-logging-action {
        description
          "This container describes the configuration parameters for
           console logging.";
        uses syslog-selector;
      }
```

```
    container file-logging-action {
      description
        "This container describes the configuration parameters for
         file logging.";
      leaf file-name {
        type inet:uri;
        mandatory true;
        description
          "This leaf specifies the name of the log file.";
      }
      uses syslog-selector;
      leaf file-logging-structured-data {
        if-feature file-logging-structured-data;
        type boolean;
        description
          "This leaf describes how log messages are written to the
           log file. If set messages will be written in structured-
           data format; if not set messages will be written in
           standard message format.";
      }
      container file-logging-archive {
        if-feature file-logging-archive-config;
        description
          "This container describes the configuration parameters for
           log file archiving.";
        leaf file-number {
          type uint32;
          description
            "This leaf specifies the maximum number of log files
             retained.";
        }
        leaf file-size {
          type uint32;
          description
            "This leaf specifies the maximum log file size.";
        }
        leaf file-permission {
          type enumeration {
             enum world-readable {
               value 1;
               description
                 "This enum specifies that the log files
                  are readable by world.";
             }
             enum no-world-readable {
               value 2;
               description
                 "This enum specifies that the log files
                  are not readable by world.";
             }
          }
          description
            "This leaf describes who can read log files";
        }
      }
    }
    container remote-logging-action {
      description
        "This container describes the configuration parameters for
         remote logging.";
      list remote-logging-destination {
        key "destination";
        description
          "This list describes a collection of remote logging
           destinations.";
        leaf destination {
          type inet:host;
          mandatory true;
          description
            "The leaf uniquely specifies the address of the
             remote host. One of the following must be specified:
             an ipv4 address, an ipv6 address, or a host name.";
        }
        uses syslog-selector;
        leaf destination-facility {
          type identityref {
            base syslogtypes:syslog-facility;
          }
          description
            "This leaf specifies the facility used in messages
             delivered to the remote server.";
        }
        leaf source-interface {
          type if:interface-ref;
          description
            "This leaf sets the source interface for the remote
             Syslog server. Either the interface name or the
             interface IP address can be specified.";
        }
        leaf vrf-name {
          if-feature remote-logging-use-vrf;
          type string;
          description
            "This leaf specifies the name of the virtual routing
             facility (VRF).";
        }
        container syslog-sign {
          if-feature signed-messages-config;
          presence
            "If present, syslog-sign is activated.";
          description
            "This container describes the configuration parameters
             for signed syslog messages as described by RFC 5848.";
          leaf certInitialRepeat {
            type uint16;
            description
            "This leaf specifies the number of times each
             Certificate Block should be sent before the first
             message is sent.";
          }
          leaf certResendDelay {
            type uint16;
            description
              "This leaf specifies the maximum time delay in seconds
               until resending the Certificate Block.";
          }
          leaf certResendCount {
            type uint16;
            description
              "This leaf specifies the maximum number of other
               syslog messages to send until resending the
               Certificate Block.";
          }
```

```
          leaf sigMaxDelay {
            type uint16;
            description
              "This leaf specifies when to generate a new Signature
               Block. If this many seconds have elapsed since the
               message with the first message number of the
               Signature Block was sent, a new Signature Block
               should be generated.";
          }
          leaf sigNumberResends {
            type uint16;
            description
              "This leaf specifies the number of times a Signature
               Block is resent. (It is recommended to select a value
               of greater than 0 in particular when the UDP
               transport [RFC5426] is used.).";
          }
          leaf sigResendDelay {
            type uint16;
            description
              "This leaf specifies when to send the next Signature
               Block transmission based on time. If this many
               seconds have elapsed since the previous sending of
               this Signature Block, resend it.";
          }
          leaf sigResendCount {
            type uint16;
            description
              "This leaf specifies when to send the next Signature
               Block transmission based on a count. If this many
               other syslog messages have been sent since the
               previous sending of this Signature Block, resend it.";
          }
        }
      }
    }
    container terminal-logging-action {
      description
        "This container describes the configuration parameters for
         the terminal logging configuration.";
      choice user-scope {
        description
          "This choice describes the option to specify all users
           or a specific user. The all users case implies that
           messages will be sent to all terminals";
        case all-users {
          description
            "This case specifies all users.";
          container all-users {
            description
              "This container describes the configuration parameters
               for all users.";
            uses syslog-selector;
          }
        }
        case per-user {
          if-feature terminal-facility-user-logging-config;
          description
            "This case specifies a specific user.";
          list user-name {
            key "uname";
            description
              "This list describes a collection of user names.";
            leaf uname {
              type string;
              description
                "This leaf uniquely describes a user name.";
            }
            uses syslog-selector;
          }
        }
      }
    }
  }
}
```

4.3. A SYSLOG Example

```
   Requirement:
   Enable global logging of two facilities:
     kern - severity critical(1)
     auth - severity error(3)

   Enable console logging of syslogs of severity
   critical(1)

   Here is the example syslog configuration xml:
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <edit-config>
       <target>
         <running/>
       </target>
       <config>
         <syslog xmlns="urn:ietf:params:xml:ns:yang:ietf-syslog">
           <global-logging-action>
             <logging-facilities>
               <facility>kern</facility><logging-severity>critical</logging-
severity>
             </logging-facilities>
             <logging-facilities>
               <facility>auth</facility><logging-severity>error</logging-
severity>
             </logging-facilities>
           </global-logging-action>
           <console-logging-action>
             <severity>critical</severity>
           </console-logging-action>
         </syslog>
       </config>
     </edit-config>
   </rpc>

   <?xml version="1.0" encoding="UTF-8"?>
   <rpc-reply message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     <ok/>
   </rpc-reply>
```

5. Implementation Status

[Note to RFC Editor: Please remove this section before publication.]

This section records the status of known implementations of the Syslog YANG model at the time of posting of this Internet-Draft.

Cisco Systems, Inc. has implemented the proposed IETF Syslog model for the Nexus 7000 NXOS OS as a prototype, together with an augmentation model for operating system specific Syslog configuration features.

Five leaves were implemented in the base IETF model and three leaves were implemented in the NXOS specific augmentation model as follows:

Leaf XPATH	Sample NXOS CLI Command(s)
syslog:global-logging-action	logging level cron 2
syslog:console-logging-action	logging console 1
syslog:file-logging-action	logging logfile mylog.log 2 4096
syslog:terminal-logging-action	logging monitor 2
syslog:remote-logging-action	*logging server server.cisco.com 2 facility user use-vrf management *logging source-interface loopback 0
cisco-syslog:logging-timestamp-config	logging timestamp milli-seconds
cisco-syslog:origin-id-cfg	logging origin-id string abcdef
cisco-syslog:module-logging	logging module 1

*The "logging server" and "logging source-interface" commands were combined into one base model leaf.

The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs.

6. Security Considerations

The YANG module defined in this memo is designed to be accessed via the NETCONF protocol [RFC6241] [RFC6241]. The lowest NETCONF layer is the secure transport layer and the mandatory-to-implement secure transport is SSH [RFC6242] [RFC6242]. The NETCONF access control model [RFC6536] [RFC6536] provides the means to restrict access for particular NETCONF users to a pre-configured subset of all available NETCONF protocol operations and content.

There are a number of data nodes defined in the YANG module which are writable/creatable/deletable (i.e., config true, which is the default). These data nodes may be considered sensitive or vulnerable in some network environments. Write operations (e.g., <edit-config>) to these data nodes without proper protection can have a negative effect on network operations.

TBD: List specific Subtrees and data nodes and their sensitivity/vulnerability.

7. IANA Considerations

This document registers a URI in the IETF XML registry [RFC3688] [RFC3688]. Following the format in RFC 3688, the following registration is requested to be made:

URI: urn:ietf:params:xml:ns:yang:syslog

Registrant Contact: The IESG.

XML: N/A, the requested URI is an XML namespace.

This document registers a YANG module in the YANG Module Names registry [RFC6020].

name: syslog namespace: urn:ietf:params:xml:ns:yang:syslog
prefix: syslog reference: RFC XXXX

8. Acknowledgements

The authors wish to thank the following who provided feedback during the writing of this document:

Alexander Clemm <alex@cisco.com>
Jim Gibson <gibson@cisco.com>
Jeffrey Haas <jhaas@pfrc.org>
John Heasley <heas@shrubbery.net>
Giles Heron <giheron@cisco.com>
Lisa Huang <yihuan@cisco.com>
Jeffrey K Lange <jeffrey.K.lange@ge.com>
Chris Lonvick <lonvick@gmail.com>
Juergen Schoenwaelder <j.schoenwaelder@jacobs-university.de>
Peter Van Horne <petervh@cisco.com>
Bert Wijnen <bertietf@bwijnen.net>
Aleksandr Zhdankin <azhdanki@cisco.com>

9. Change log [RFC Editor: Please remove]

10. References

[RFC3164] Lonvick, C., "The BSD syslog Protocol", BCP 81, RFC 3164, August 2001.

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, April 2704.

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

[RFC5426] Okmianski, A., "Transmission of Syslog Messages over UDP", RFC 5426, March 2009

[RFC5848] Kelsey, J., Callas, J., Clemm, A., "Signed Syslog Messages", RFC 5848, May 2010.

[RFC6020] Bjorklund, M., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, November 2010.

[RFC6241] Enns, R., Bjorklund, M., Schoenwaelder, J., and A. Bierman, "Network Configuration Protocol (NETCONF)", RFC 6241, June 2011.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, June 2011.

[RFC6536] Bierman, A., Bjorklund, M., "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, March 2012.

[RFC6536] Bierman, A. and M. Bjorklund, "Network Configuration Protocol (NETCONF) Access Control Model", RFC 6536, March 2012.

[Posix 1003.2] IEEE, "1003.2-1992 - IEEE Standard for Information Technology--Portable Operating System Interfaces (POSIX(R))--Part 2: Shell and Utilities", Posix 1003.2, 1992

Authors' Addresses

Clyde Wildes
Cisco Systems Inc.

Email: cwildes@cisco.com

Kiran Agrahara Sreenivasa
Brocade Communications Systems

Email: kkoushik@brocade.com