NETMOD WG C. Wildes, Ed.
Internet-Draft Cisco Systems Inc.
Intended status: Standards Track K. Koushik, Ed.
Expires: December 07, 2017 Verizon Wireless
June 07, 2017

A YANG Data Model for Syslog Configuration
draft-ietf-netmod-syslog-model-15

Abstract

This document describes a data model for the configuration of syslog.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction 2
1.1. Requirements Language 2
1.2. Terminology 2
2. Problem Statement 3
3. Design of the Syslog Model 3
3.1. Syslog Module 5

4. Syslog YANG Module 7
4.1. The ietf-syslog Module 7
5. Usage Examples 23
6. Acknowledgements 24
7. IANA Considerations 25
8. Security Considerations 25
8.1. Resource Constraints 26
8.2. Inappropriate Configuration 26
9. References 26
9.1. Normative References 26
9.2. Informative References 27
Appendix A. Implementor Guidelines 27
Appendix A.1. Extending Facilities 27
Authors' Addresses 28

1. Introduction

Operating systems, processes and applications generate messages indicating their own status or the occurrence 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, 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 RFC5424 [RFC5424] in this RFC.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

1.2. Terminology

The term "originator" is defined in [RFC5424]: an "originator"

generates syslog content to be carried in a message.

The terms "relay" and "collectors" are as defined in [RFC5424].

2. Problem Statement

This document defines a YANG [RFC6020] configuration data model that may be used to configure the syslog feature running on a system. YANG models can be used with network management protocols such as NETCONF [RFC6241] to install, manipulate, and delete the configuration of network devices.

The data model makes use of the YANG "feature" construct which allows implementations to support only those syslog features that lie within their capabilities.

This module can be used to configure the syslog application conceptual layers as implemented on the target system.

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 implementations and creates a common model, which can be augmented with proprietary features, if necessary. This model is designed to be very simple for maximum flexibility.

Optional features are used to specify functionality that is present in specific vendor configurations.

Syslog consists of originators, and collectors. The following diagram shows syslog messages flowing from an originator, to collectors where filtering can take place.

Many vendors extend the list of facilities available for logging in their implementation. An example is included in Extending Facilities (Appendix A.1).

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

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

     |                                                                |
     +----------------------------------------------------------------+
                  |
                  |
                  |
                  |
          +-------------+--------------+
          |             |              |
          v             v              v
   Collectors
     +----------+ +----------+ +----------------+
     |          | |  Log     | |Remote Relay(s)/|
     | Console  | |  File(s) | |Collector(s)    |
     +----------+ +----------+ +----------------+
```

Figure 1. Syslog Processing Flow

The leaves in the syslog model "actions" container correspond to each message collector:

```
console
log file(s)
remote relay(s)/collector(s)
```

Within each action, a selector is used to filter syslog messages. A selector consists of a list of one or more facility-severity matches, and, if supported via the select-match feature, an optional regular expression pattern match that is performed on the SYSLOG-MSG [RFC5424] field.

A syslog message is processed if:

```
 There is an element of facility-list (F, S) where
     the message facility matches F (if it is present)
     and the message severity matches S (if it is present)
 or the message text matches the regex pattern (if it is present)
```

The facility is one of a specific syslog-facility, or all facilities.

The severity is one of type syslog-severity, all severities, or none. None is a special case that can be used to disable a filter. When filtering severity, the default comparison is that messages of the specified severity and higher are selected to be logged. This is shown in the model as "default equals-or-higher". This behavior can be altered if the select-adv-compare feature is enabled to specify a compare operation and an action. Compare operations are: "equals" to select messages with this single severity, or "equals-or-higher" to select messages of the specified severity and higher. Actions are used to log the message or block the message from being logged.

3.1. Syslog Module

A simplified graphical representation of the data model is used in this document. The meaning of the symbols in these diagrams is defined in [RFC6087].

```
   module: ietf-syslog
      +--rw syslog!
         +--rw actions
            +--rw console! {console-action}?
            |  +--rw facility-filter
            |     +--rw facility-list* [facility severity]
            |     |  +--rw facility            union
            |     |  +--rw severity            union
            |     |  +--rw advanced-compare {select-adv-compare}?
            |     |     +--rw compare?   enumeration
            |     |     +--rw action?    enumeration
            |     +--rw pattern-match?   string {select-match}?
            +--rw file {file-action}?
            |  +--rw log-file* [name]
            |     +--rw name               inet:uri
            |     +--rw facility-filter
            |     |  +--rw facility-list* [facility severity]
            |     |  |  +--rw facility            union
            |     |  |  +--rw severity            union
            |     |  |  +--rw advanced-compare {select-adv-compare}?
            |     |  |     +--rw compare?   enumeration
            |     |  |     +--rw action?    enumeration
            |     |  +--rw pattern-match?   string {select-match}?
            |     +--rw structured-data?   boolean {structured-data}?
            |     +--rw file-rotation
            |        +--rw number-of-files?   uint32 {file-limit-size}?
            |        +--rw max-file-size?     uint32 {file-limit-size}?
            |        +--rw rollover?          uint32 {file-limit-duration}?
            |        +--rw retention?         uint32 {file-limit-duration}?
            +--rw remote {remote-action}?
               +--rw destination* [name]
                  +--rw name                 string
                  +--rw (transport)
                  |  +--:(tcp)
                  |  |  +--rw tcp
                  |  |     +--rw address?   inet:host
                  |  |     +--rw port?      inet:port-number
                  |  +--:(udp)
                  |  |  +--rw udp
                  |  |     +--rw address?   inet:host
                  |  |     +--rw port?      inet:port-number
                  |  +--:(tls)
                  |     +--rw tls
                  |        +--rw server-auth
                  |        |  +--rw trusted-ca-certs?       -> /ks:keystore/
trusted-certificates/name
                  |        |  +--rw trusted-server-certs?   -> /ks:keystore/
trusted-certificates/name
```

```
                  |        +--rw client-auth
                  |        |  +--rw (auth-type)?
                  |        |     +--:(certificate)
                  |        |        +--rw certificate?   -> /ks:keystore/keys/
key/certificates/certificate/name
                  |        +--rw hello-params {tls-client-hello-params-config}?
                  |        |  +--rw tls-versions
                  |        |  |  +--rw tls-version*   identityref
                  |        |  +--rw cipher-suites
                  |        |     +--rw cipher-suite*   identityref
                  |        +--rw port?            inet:port-number
                  +--rw facility-filter
                  |  +--rw facility-list* [facility severity]
                  |  |  +--rw facility             union
                  |  |  +--rw severity             union
                  |  |  +--rw advanced-compare {select-adv-compare}?
                  |  |     +--rw compare?   enumeration
                  |  |     +--rw action?    enumeration
                  |  +--rw pattern-match?   string {select-match}?
                  +--rw structured-data?     boolean {structured-data}?
                  +--rw facility-override?   identityref
                  +--rw source-interface?    if:interface-ref {remote-source-
interface}?
                  +--rw signing-options! {signed-messages}?
                     +--rw cert-signers
                        +--rw cert-signer* [name]
                        |  +--rw name             string
                        |  +--rw certificate?      -> /ks:keystore/keys/key/
certificates/certificate/name
                        |  +--rw hash-algorithm?   enumeration
                        +--rw cert-initial-repeat?   uint32
                        +--rw cert-resend-delay?     uint32
                        +--rw cert-resend-count?     uint32
                        +--rw sig-max-delay?         uint32
                        +--rw sig-number-resends?    uint32
                        +--rw sig-resend-delay?      uint32
                        +--rw sig-resend-count?      uint32
```

Figure 2. ietf-syslog Module Tree

4. Syslog YANG Module

4.1. The ietf-syslog Module

This module imports typedefs from [RFC6021], [RFC7223], [RFC draft ietf-tls-client], and [RFC draft ietf-keystore], and it references [RFC5424], [RFC5425], [RFC5426], [RFC6587], and [RFC5848].

```
   <CODE BEGINS> file "ietf-syslog.yang"
   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-tls-client {
       prefix tlsc;
     }

     import ietf-keystore {
       prefix ks;
     }

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

        Editor:   Kiran Agrahara Sreenivasa
                  <mailto:kirankoushik.agraharasreenivasa@verizonwireless.com>

        Editor:   Clyde Wildes
                  <mailto:cwildes@cisco.com>";
     description
       "This module contains a collection of YANG definitions
        for syslog configuration.

        Copyright (c) 2016 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, is permitted pursuant to, and subject to
        the license terms contained in, the Simplified BSD License set
        forth in Section 4.c of the IETF Trust's Legal Provisions
        Relating to IETF Documents
        (http://trustee.ietf.org/license-info).

        The key words 'MUST', 'MUST NOT', 'REQUIRED', 'SHALL', 'SHALL
        NOT', 'SHOULD', 'SHOULD NOT', 'RECOMMENDED', 'MAY', and
        'OPTIONAL' in the module text are to be interpreted as described
```

in RFC 2119 (http://tools.ietf.org/html/rfc2119).

This version of this YANG module is part of RFC XXXX
(http://tools.ietf.org/html/rfcXXXX); see the RFC itself for

```
        full legal notices.";

     reference
       "RFC 5424: The Syslog Protocol
        RFC 5425: Transport Layer Security (TLS) Transport Mapping for Syslog
        RFC 5426: Transmission of Syslog Messages over UDP
        RFC 6587: Transmission of Syslog Messages over TCP
        RFC 5848: Signed Syslog Messages
        RFC xxxx: Keystore Management
        RFC xxxx: Transport Layer Security (TLS) Client";

     revision 2017-06-07 {
       description
         "Initial Revision";
       reference
         "RFC XXXX: Syslog YANG Model";
     }

     feature console-action {
       description
         "This feature indicates that the local console action is
          supported.";
     }

     feature file-action {
       description
         "This feature indicates that the local file action is
          supported.";
     }

     feature file-limit-size {
       description
         "This feature indicates that file logging resources
          are managed using size and number limits.";
     }

     feature file-limit-duration {
       description
         "This feature indicates that file logging resources
          are managed using time based limits.";
     }

     feature remote-action {
       description
         "This feature indicates that the remote server action is
          supported.";
     }

     feature remote-source-interface {
       description
         "This feature indicates that source-interface is supported
          supported for the remote-action.";
     }
```

```
     feature select-adv-compare {
       description
         "This feature represents the ability to select messages
          using the additional comparison operators when comparing
          the syslog message severity.";
     }

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

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

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

     typedef syslog-severity {
       type enumeration {
         enum "emergency" {
           value 0;
           description
             "The severity level 'Emergency' indicating that the system
              is unusable.";
         }
         enum "alert" {
           value 1;
           description
             "The severity level 'Alert' indicating that an action must be
              taken immediately.";
         }
         enum "critical" {
           value 2;
           description
             "The severity level 'Critical' indicating a critical condition.";
         }
         enum "error" {
           value 3;
           description
             "The severity level 'Error' indicating an error condition.";
         }
```

```
          enum "warning" {
            value 4;
            description
              "The severity level 'Warning' indicating a warning condition.";
          }
```

```
         enum "notice" {
           value 5;
           description
             "The severity level 'Notice' indicating a normal but significant
              condition.";
         }
         enum "info" {
           value 6;
           description
             "The severity level 'Info' indicating an informational message.";
         }
         enum "debug" {
           value 7;
           description
             "The severity level 'Debug' indicating a debug-level message.";
         }
       }
       description
         "The definitions for Syslog message severity as per RFC 5424.";
     }

     identity syslog-facility {
       description
         "This identity is used as a base for all syslog facilities as
          per RFC 5424.";
     }

     identity kern {
       base syslog-facility;
       description
         "The facility for kernel messages (0) as defined in RFC 5424.";
     }

     identity user {
       base syslog-facility;
       description
         "The facility for user-level messages (1) as defined in RFC 5424.";
     }

     identity mail {
       base syslog-facility;
       description
         "The facility for the mail system (2) as defined in RFC 5424.";
     }

     identity daemon {
       base syslog-facility;
       description
         "The facility for the system daemons (3) as defined in RFC 5424.";
       }

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

```
          "The facility for security/authorization messages (4) as defined
           in RFC 5424.";
      }

      identity syslog {
        base syslog-facility;
        description
          "The facility for messages generated internally by syslogd
           facility (5) as defined in RFC 5424.";
      }

      identity lpr {
        base syslog-facility;
        description
          "The facility for the line printer subsystem (6) as defined in
           RFC 5424.";
      }

      identity news {
        base syslog-facility;
        description
          "The facility for the network news subsystem (7) as defined in
           RFC 5424.";
      }

      identity uucp {
        base syslog-facility;
        description
          "The facility for the UUCP subsystem (8) as defined in RFC 5424.";
      }

      identity cron {
        base syslog-facility;
        description
          "The facility for the clock daemon (9) as defined in RFC 5424.";
      }

      identity authpriv {
        base syslog-facility;
        description
          "The facility for privileged security/authorization messages (10)
           as defined in RFC 5424.";
      }

      identity ftp {
        base syslog-facility;
        description
          "The facility for the FTP daemon (11) as defined in RFC 5424.";
      }
```

```
     identity ntp {
       base syslog-facility;
       description
         "The facility for the NTP subsystem (12) as defined in RFC 5424.";
     }

     identity audit {
       base syslog-facility;
       description
         "The facility for log audit messages (13) as defined in RFC 5424.";
     }

     identity console {
       base syslog-facility;
       description
         "The facility for log alert messages (14) as defined in RFC 5424.";
     }

     identity cron2 {
       base syslog-facility;
       description
         "The facility for the second clock daemon (15) as defined in
          RFC 5424.";
     }

     identity local0 {
       base syslog-facility;
       description
         "The facility for local use 0 messages (16) as defined in
          RFC 5424.";
     }

     identity local1 {
       base syslog-facility;
       description
         "The facility for local use 1 messages (17) as defined in
          RFC 5424.";
     }

     identity local2 {
       base syslog-facility;
       description
         "The facility for local use 2 messages (18) as defined in
          RFC 5424.";
     }

     identity local3 {
       base syslog-facility;
       description
         "The facility for local use 3 messages (19) as defined in
          RFC 5424.";
     }
     identity local4 {
       base syslog-facility;
       description
         "The facility for local use 4 messages (20) as defined in
          RFC 5424.";
     }

     identity local5 {
       base syslog-facility;
       description
         "The facility for local use 5 messages (21) as defined in
          RFC 5424.";
     }

     identity local6 {
       base syslog-facility;
       description
         "The facility for local use 6 messages (22) as defined in
          RFC 5424.";
     }

     identity local7 {
       base syslog-facility;
       description
         "The facility for local use 7 messages (23) as defined in
          RFC 5424.";
     }

     grouping severity-filter {
       description
         "This grouping defines the processing used to select
          log messages by comparing syslog message severity using
          the following processing rules:
           - if 'none', do not match.
           - if 'all', match.
           - else compare message severity with the specified severity
             according to the default compare rule (all messages of the
             specified severity and greater match) or if the
             select-adv-compare feature is present, the advance-compare
             rule.";
       leaf severity {
         type union {
           type syslog-severity;
           type enumeration {
             enum none {
               value -2;
               description
                 "This enum describes the case where no severities
                  are selected.";
             }
             enum all {
               value -1;
               description
                 "This enum describes the case where all severities
```

```
                  are selected.";
             }
           }
         }
         mandatory true;
         description
           "This leaf specifies the syslog message severity.";
       }
       container advanced-compare {
         when '../severity != "all" and
              ../severity != "none"' {
           description
             "The advanced compare container is not applicable for severity
              'all' or severity 'none'";
         }
         if-feature select-adv-compare;
         leaf compare {
           type enumeration {
             enum equals {
               description
                 "This enum specifies that the severity comparison operation
                  will be equals.";
             }
             enum equals-or-higher {
               description
                 "This enum specifies that the severity comparison operation
                  will be equals or higher.";
             }
           }
           default equals-or-higher;
           description
             "The compare can be used to specify the comparison operator that
              should be used to compare the syslog message severity with the
              specified severity.";
         }
         leaf action {
           type enumeration {
             enum log {
               description
                 "This enum specifies that if the compare operation is true
                  the message will be logged.";
              }
             enum block {
               description
                 "This enum specifies that if the compare operation is true
                  the message will not be logged.";
             }
           }
           default log;
           description
             "The action can be used to spectify if the message should be
              logged or blocked based on the outcome of the compare
operation.";
         }
         description
           "This leaf describes additional severity compare operations that can
            be used in place of the default severity comparison. The compare
leaf
            specifies the type of the compare that is done and the action leaf
            specifies the intended result. Example: compare->equals and action-
>
            no-match means messages that have a severity that is not equal to
the
```

```
            specified severity will be logged.";
         }
       }

       grouping selector {
         description
           "This grouping defines a syslog selector which is used to
            select log messages for the log-actions (console, file,
            remote, etc.). Choose one or both of the following:
              facility [<facility> <severity>...]
              pattern-match regular-expression-match-string
            If both facility and pattern-match are specified, both must
            match in order for a log message to be selected.";
         container facility-filter {
           description
             "This container describes the syslog filter parameters.";
           list facility-list {
             key "facility severity";
             ordered-by user;
             description
               "This list describes a collection of syslog
                facilities and severities.";
             leaf facility {
               type union {
                 type identityref {
                   base syslog-facility;
                 }
                 type enumeration {
                   enum all {
                     description
                       "This enum describes the case where all
                        facilities are requested.";
                   }
                 }
               }
               description
                 "The leaf uniquely identifies a syslog facility.";
             }
             uses severity-filter;
           }
           leaf pattern-match {
             if-feature select-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. The match is performed on the RFC 5424
                SYSLOG-MSG field.";
           }
```

```
    }
  }

  grouping structured-data {
    description
```

```
          "This grouping defines the syslog structured data option
           which is used to select the format used to write log
           messages.";
        leaf structured-data {
          if-feature structured-data;
          type boolean;
          default false;
          description
            "This leaf describes how log messages are written.
             If true, messages will be written with one or more
             STRUCTURED-DATA elements as per RFC5424; if false,
             messages will be written with STRUCTURED-DATA =
             NILVALUE.";
        }
      }

      container syslog {
        presence "Enables logging.";
        description
          "This container describes the configuration parameters for
           syslog.";
        container actions {
          description
            "This container describes the log-action parameters
             for syslog.";
          container console {
            if-feature console-action;
            presence "Enables logging to the console";
            description
              "This container describes the configuration parameters for
               console logging.";
            uses selector;
          }
          container file {
            if-feature file-action;
            description
              "This container describes the configuration parameters for
               file logging. If file-archive limits are not supplied, it
               is assumed that the local implementation defined limits will
               be used.";
            list log-file {
              key "name";
              description
                "This list describes a collection of local logging
                 files.";
              leaf name {
                type inet:uri {
                  pattern 'file:.*';
                }
                description
                  "This leaf specifies the name of the log file which
                   MUST use the uri scheme file:.";
              }
              uses selector;
              uses structured-data;
              container file-rotation {
                description
                  "This container describes the configuration
                   parameters for log file rotation.";
                leaf number-of-files {
                  if-feature file-limit-size;
                  type uint32;
                  default 1;
                  description
                    "This leaf specifies the maximum number of log
                     files retained. Specify 1 for implementations
                     that only support one log file.";
                }
                leaf max-file-size {
                  if-feature file-limit-size;
                  type uint32;
                  units "megabytes";
                  description
                    "This leaf specifies the maximum log file size.";
                }
                leaf rollover {
                  if-feature file-limit-duration;
                  type uint32;
                  units "minutes";
                  description
                    "This leaf specifies the length of time that log
                     events should be written to a specific log file.
                     Log events that arrive after the rollover period
                     cause the current log file to be closed and a new
                     log file to be opened.";
                }
                leaf retention {
                  if-feature file-limit-duration;
                  type uint32;
                  units "hours";
                  description
                    "This leaf specifies the length of time that
                     completed/closed log event files should be stored
                     in the file system before they are deleted.";
                }
              }
            }
          }
          container remote {
            if-feature remote-action;
            description
              "This container describes the configuration parameters for
               forwarding syslog messages to remote relays or collectors.";
            list destination {
              key "name";
              description
                "This list describes a collection of remote logging
                 destinations.";
              leaf name {
                type string;
                description
                  "An arbitrary name for the endpoint to connect to.";
              }
              choice transport {
                mandatory true;
                description
                  "This choice describes the transport option.";
                case tcp {
                  container tcp {
                    description
                      "This container describes the TCP transport
                       options.";
                    reference
                      "RFC 6587: Transmission of Syslog Messages over TCP";
                    leaf address {
                      type inet:host;
                      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.";
                    }
                    leaf port {
                      type inet:port-number;
                      default 514;
                      description
                        "This leaf specifies the port number used to
                         deliver messages to the remote server.";
                    }
                  }
                }
                case udp {
                  container udp {
                    description
                      "This container describes the UDP transport
                       options.";
                    reference
                      "RFC 5426: Transmission of Syslog Messages over UDP";
                    leaf address {
                      type inet:host;
                      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.";
                    }
                    leaf port {
                      type inet:port-number;
                      default 514;
                      description
                        "This leaf specifies the port number used to
                         deliver messages to the remote server.";
```

```
                   }
                 }
               }
               case tls {
                 container tls {
                   description
                     "This container describes the TLS transport options.";
                   reference
                     "RFC 5425: Transport Layer Security (TLS) Transport
                      Mapping for Syslog ";
                   uses tlsc:tls-client-grouping;
                   leaf port {
                     type inet:port-number;
                     default 6514;
                     description
                       "TCP port 6514 has been allocated as the default
                        port for syslog over TLS.";
                   }
                 }
               }
             }
             uses selector;
             uses structured-data;
             leaf facility-override {
               type identityref {
                 base syslog-facility;
               }
               description
                 "If specified, this leaf specifies the facility used
                  to override the facility in messages delivered to the
                  remote server.";
             }
             leaf source-interface {
               if-feature remote-source-interface;
               type if:interface-ref;
               description
                 "This leaf sets the source interface to be used to send
                  message to the remote syslog server. If not set,
                  messages sent to a remote syslog server will
                  contain the IP address of the interface the syslog
                  message uses to exit the network element";
             }
             container signing-options {
               if-feature signed-messages;
               presence
                 "If present, syslog-signing options is activated.";
               description
                 "This container describes the configuration
                  parameters for signed syslog messages as described
                  by RFC 5848.";
               reference
                 "RFC 5848: Signed Syslog Messages";
               container cert-signers {
                 description
```

```
                   "This container describes the signing certificate
configuration
                    for Signature Group 0 which covers the case for
administrators
                    who want all Signature Blocks to be sent to a single
destination.";
                 list cert-signer {
                   key "name";
                   description
                     "This list describes a collection of syslog message
                      signers.";
                   leaf name {
                     type string;
                     description
                       "This leaf specifies the name of the syslog message
                        signer.";
                   }
                   leaf certificate {
                     type leafref {
                       path "/ks:keystore/ks:keys/ks:key/ks:certificates"
                             + "/ks:certificate/ks:name";
                     }
                     description
                      "This is the certificate that is periodically sent to the
remote
                       receiver. Selection of the certificate also implicitly
selects
                       the private key used to sign the syslog messages.";
                   }
                   leaf hash-algorithm {
                     type enumeration {
                       enum SHA1 {
                         value 1;
                         description
                           "This enum describes the SHA1 algorithm.";
                       }
                       enum SHA256 {
                         value 2;
                         description
                           "This enum describes the SHA256 algorithm.";
                       }
                     }
                     description
                       "This leaf describes the syslog signer hash
                        algorithm used.";
                   }
                 }
                 leaf cert-initial-repeat {
                   type uint32;
```

```
                  default 3;
                  description
                  "This leaf specifies the number of times each
                   Certificate Block should be sent before the first
                   message is sent.";
                }
                leaf cert-resend-delay {
                  type uint32;
                  units "seconds";
                  default 3600;
```

```
                   description
                     "This leaf specifies the maximum time delay in
                      seconds until resending the Certificate Block.";
                 }
                 leaf cert-resend-count {
                   type uint32;
                   default 0;
                   description
                     "This leaf specifies the maximum number of other
                      syslog messages to send until resending the
                      Certificate Block.";
                 }
                 leaf sig-max-delay {
                   type uint32;
                   units "seconds";
                   default 60;
                   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 sig-number-resends {
                   type uint32;
                   default 0;
                   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 sig-resend-delay {
                   type uint32;
                   units "seconds";
                   default 5;
                   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 sig-resend-count {
                   type uint32;
                   default 0;
                   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. A value of 0 means that you
                      don't resend based on the number of messages.";
                 }
               }
```

```
             }
           }
         }
       }
     }
   }
   <CODE ENDS>
```

Figure 3. ietf-syslog Module

5. Usage Examples

Requirement:
Enable console logging of syslogs of severity critical

Here is the example syslog configuration xml:

```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <syslog xmlns="urn:ietf:params:xml:ns:yang:ietf-syslog"
          xmlns:syslog="urn:ietf:params:xml:ns:yang:ietf-syslog">
    <actions>
      <console>
        <selector>
          <facility-list>
            <facility>all</facility>
            <severity>critical</severity>
          </facility-list>
        </selector>
      </console>
    </actions>
  </syslog>
</config>
```

Enable remote logging of syslogs to udp destination 2001:db8:a0b:12f0::1
for facility auth, severity error

```
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <syslog xmlns="urn:ietf:params:xml:ns:yang:ietf-syslog"
          xmlns:syslog="urn:ietf:params:xml:ns:yang:ietf-syslog">
    <actions>
      <remote>
        <destination>
          <name>remote1</name>
          <udp>
            <address>2001:db8:a0b:12f0::1</address>
          </udp>
          <selector>
            <facility-list>
              <facility>auth</facility>
              <severity>error</severity>
            </facility-list>
          </selector>
        </destination>
      </remote>
    </actions>
  </syslog>
</config>
```

Figure 4. ietf-syslog Examples

6. Acknowledgements

The authors wish to thank the following who commented on this proposal:

Andy Bierman

Martin Bjorklund
Alex Campbell
Alex Clemm
Jim Gibson
Jeffrey Haas
John Heasley
Giles Heron
Lisa Huang
Mahesh Jethanandani
Jeffrey K Lange
Jan Lindblad
Chris Lonvick
Tom Petch
Juergen Schoenwaelder
Phil Shafer
Jason Sterne
Peter Van Horne
Kent Watsen
Bert Wijnen
Dale R Worley
Aleksandr Zhdankin

7. IANA Considerations

This document registers one URI in the IETF XML registry [RFC3688].

Following the format in RFC 3688, the following registration is requested to be made:

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

prefix: ietf-syslog

reference: RFC XXXX

8. Security Considerations

The YANG module defined in this memo is designed to be accessed via the NETCONF protocol [RFC6241]. The lowest NETCONF layer is the secure transport layer and the mandatory-to-implement secure transport is SSH [RFC6242]. The NETCONF access control model

[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.

8.1. Resource Constraints

Network administrators must take the time to estimate the appropriate memory limits caused by the configuration of actions/buffer using buffer-limit-bytes and/or buffer-limit-messages where necessary to limit the amount of memory used.

Network administrators must take the time to estimate the appropriate storage capacity caused by the configuration of actions/file using file-archive attributes to limit storage used.

It is the responsibility of the network administrator to ensure that the configured message flow does not overwhelm system resources.

8.2. Inappropriate Configuration

It is the responsibility of the network administrator to ensure that the messages are actually going to the intended recipients.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5424] Gerhards, R., "The Syslog Protocol", RFC 5424, DOI 10.17487/RFC5424, March 2009, <http://www.rfc-editor.org/info/rfc5424>.

[RFC5426] Okmianski, A., "Transmission of Syslog Messages over UDP", RFC 5426, DOI 10.17487/RFC5426, March 2009, <http://www.rfc-editor.org/info/rfc5426>.

[RFC5848] Kelsey, J., Callas, J. and A. Clemm, "Signed Syslog Messages", RFC 5848, DOI 10.17487/RFC5848, May 2010, <http://www.rfc-editor.org/info/rfc5848>.

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <http://www.rfc-editor.org/info/rfc6020>.

[RFC6021] Schoenwaelder, J., Ed., "Common YANG Data Types", RFC 6021, DOI 10.17487/RFC6021, October 2010, <http://www.rfc-editor.org/info/rfc6021>.

[RFC6587] Gerhards, R. and C. Lonvick, "Transmission of Syslog Messages over TCP", RFC 6587, DOI 10.17487/RFC6587, April 2012, <http://www.rfc-editor.org/info/rfc6587>.

[RFC7223] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 7223, DOI 10.17487/RFC7223, May 2014, <http://www.rfc-editor.org/info/rfc7223>.

9.2. Informative References

[RFC3688] Mealling, M., "The IETF XML Registry", BCP 81, RFC 3688, DOI 10.17487/RFC3688, January 2004, <http://www.rfc-editor.org/info/rfc3688>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J.Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <http://www.rfc-editor.org/info/rfc6241>.

[RFC6242] Wasserman, M., "Using the NETCONF Protocol over Secure Shell (SSH)", RFC 6242, DOI 10.17487/RFC6242, June 2011, <http://www.rfc-editor.org/info/rfc6242>.

Appendix A. Implementor Guidelines

Appendix A.1. Extending Facilities

Many vendors extend the list of facilities available for logging in their implementation. Additional facilities may not work with the syslog protocol as defined in [RFC5424] and hence such facilities apply for local syslog-like logging functionality.

The following is an example that shows how additional facilities could be added to the list of available facilities (in this example two facilities are added):

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

     import ietf-syslog {
       prefix syslogtypes;
     }

     organization "Example, Inc.";
     contact
       "Example, Inc.
        Customer Service

        E-mail: syslog-yang@example.com";

     description
       "This module contains a collection of vendor-specific YANG type
        definitions for SYSLOG.";

     revision 2017-03-13 {
       description
         "Version 1.0";
       reference
         "Vendor SYSLOG Types: SYSLOG YANG Model";
     }

     identity vendor_specific_type_1 {
       base syslogtypes:syslog-facility;
     }

     identity vendor_specific_type_2 {
       base syslogtypes:syslog-facility;
     }
   }
```

Authors' Addresses

Clyde Wildes, editor
Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134
US

Phone: +1 408 527-2672
Email: cwildes@cisco.com

Kiran Koushik, editor
Verizon Wireless
500 W Dove Rd.
Southlake, TX 76092
US

Phone: +1 512 650-0210
Email: kirankoushik.agraharasreenivasa@verizonwireless.com