Draft-ietf-netmod-syslog-model-00 Review

Clyde Wildes (Cisco), Kiran Koushik (Brocade)

Agenda

- Review Comments Adopted
- Review Comments Not Adopted
- Feature Changes
- Selector Processing
- Action Processing

Review Comments Adopted

- Choose more specific leaf types:
  - Use inet:uri for the file-name instead of string.
  - Use inet:host for remote server name instead of string.
  - Use if:interface-ref for source-interface instead of string.
- Use grouping more effectively to reduce complexity.
- Add maximum file size for file logging.

Review Comments Adopted (cont.)

- Make the Syslog configuration for message processing flow more Linux like:
  - Call out selectors and actions
  - Standardize on the term “severity” instead of “severity” and “priority”
  - Expand selector processing to allow
    - Specification of all severities, or a specific severity
    - Specification of all facilities, no facilities, or one or more facilities
    - Specification of equals, and not equals operators as a feature

Review Comments Adopted (cont.)

- Include references to relevant RFCs in the reference section of the revision statement.
- Support RFC 5424 structured data for file logging as a feature.
- Implement extended message filtering as a feature as proposed by Rainer Gerhards and implemented in Rsyslog.
- Make the global-logging description clearer.

Review Comments Adopted (cont.)

- Add log archival with permissions for file-logging as a feature.
- Add support for signed syslog messages.

Review Comments Not Adopted

- Support syslogd daemon options
  - These options set various options for the syslog daemon itself
  - Review the daemon options at: http://manpages.ubuntu.com/manpages/saucy/man8/sysklogd.8.html

Feature Changes

- Features that were added:
  - feature file-logging-archive-config
  - feature selector-advanced-level-processing-config
  - feature selector-match-processing-config
  - feature file-logging-structured-data
- Features that were renamed:
  - feature global-logging to global-logging-action
  - feature use-vrf to remote-logging-use-vrf

Feature Changes (cont.)

- Features that were removed:
  - Three “facility-logging-config” features were removed because they duplicate the revised selector processing (can a facility be specified for certain actions):
    - feature console-facility-logging-config
    - feature file-facility-logging-config
    - feature terminal-facility-logging-config
  - feature file-logging was removed

Selector Processing

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> [<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.";

Selector Processing

```
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 {
    case logging-severity-all {
     …
    }
    case logging-severity {
      …
    }
  }
}
```

Selector Processing (cont.)

```
choice logging-level-scope {
  case logging-facility-all {
    uses syslog-severity;
  }
  case logging-facility {
    list logging-facilities {
      key "facility";
      leaf facility {
        …
      }
      uses syslog-severity;
    }
  }
  case logging-facility-none {
    …
  }
}
```

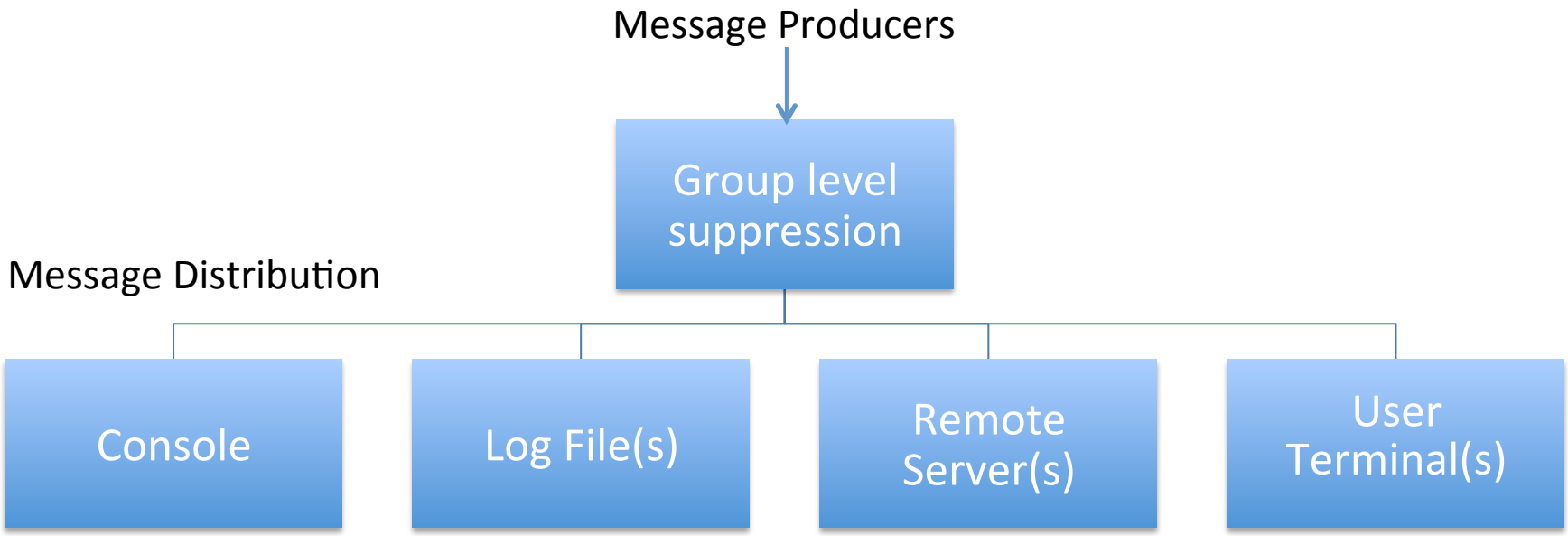
Selector Processing (cont.)

```
container logging-advanced-level-processing {
  if-feature selector-advanced-level-processing-config;
  description
    "This container describes the configuration parameters for advanced Syslog selector severity.";
  choice logging-severity-operator {
    case default {
      description
        "All messages of the specified severity and higher are logged";
      …
    }
    case equals {
      description
        "All messages of the specified severity are logged";
      …
    }
    case not-equals {
      description
        "All messages that are not of the specified severity are logged";
      …
    }
  }
}
```

Selector Processing (cont.)

```
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 desribes a Posix 1003.2 regular expression
        string that can be used to select a Syslog message
        for logging.";
    }
  }
}
```

Action Processing



Action Processing

+--rw syslog

    +--rw global-logging-action

    +--rw console-logging-action

    +--rw file-logging-action

    +--rw remote-logging-action

    +--rw terminal-logging-action

Status and Next steps

- Special thanks to the people who have provided feedback:
  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