The syslog protocol

The following sections provide information about the syslog protocol:

- Syslog Facilities
- Syslog Levels
- Syslog Priority values
- Transport
- Syslog RFC 3164 header format

Syslog Facilities

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value. The priority is enclosed in "<>" delimiters.

A BSD Unix Syslog message looks like this: <pri>HEADER MESSAGE</pri>

The priority is a value from 0 to 191 and is not space or leading zero padded.

For more information on the Syslog message format, please read the RFC.

The Facility value is a way of determining which process of the machine created the message. Since the Syslog protocol was originally written on BSD Unix, the Facilities reflect the names of Unix processes and Daemons. The priority value is calculated using the following formula:

Priority = Facility * 8 + Level

The list of Facilities available:

- 0 - kernel messages
- 1 - user-level messages
- 2 - mail system
- 3 - system daemons
- 4 - security/authorization messages
- 5 - messages generated internally by syslogd
- 6 - line printer subsystem
- 7 - network news subsystem
• 8 - UUCP subsystem
• 9 - clock daemon
• 10 - security/authorization messages
• 11 - FTP daemon
• 12 - NTP subsystem
• 13 - log audit
• 14 - log alert
• 15 - clock daemon
• 16 - local use 0 (local0)
• 17 - local use 1 (local1)
• 18 - local use 2 (local2)
• 19 - local use 3 (local3)
• 20 - local use 4 (local4)
• 21 - local use 5; (local5)
• 22 - local use 6 (local6)
• 23 - local use 7 (local7)

If you are receiving messages from a Unix system, it is suggested you use the 'User' Facility as your first choice. Local0 through to Local7 are not used by Unix and are traditionally used by networking equipment. Cisco routers for example use Local6 or Local7.

Syslog Levels

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value. The priority is enclosed in "<>" delimiters.

A BSD Unix Syslog message looks like this: <pri>HEADER MESSAGE</pri>

The priority is a value from 0 to 191 and is not space or leading zero padded.

For more information on the Syslog message format, please read the RFC.

The priority value is calculated using the following formula:

Priority = Facility * 8 + Level

The list of severity Levels:

• 0 - Emergency: system is unusable
• 1 - Alert: action must be taken immediately
• 2 - Critical: critical conditions
• 3 - Error: error conditions
• 4 - Warning: warning conditions
• 5 - Notice: normal but significant condition
• 6 - Informational: informational messages
• 7 - Debug: debug-level messages

Recommended practice is to use the Notice or Informational level for normal messages.

**A detailed explanation of the severity Levels:**

**DEBUG:**

Info useful to developers for debugging the app, not useful during operations

**INFORMATIONAL:**

Normal operational messages - may be harvested for reporting, measuring throughput, etc - no action required

**NOTICE:**

Events that are unusual but not error conditions - might be summarized in an email to developers or admins to spot potential problems - no immediate action required

**WARNING:**

Warning messages - not an error, but indication that an error will occur if action is not taken, e.g. file system 85% full - each item must be resolved within a given time

**ERROR:**

Non-urgent failures - these should be relayed to developers or admins; each item must be resolved within a given time

**ALERT:**

Should be corrected immediately - notify staff who can fix the problem - example is loss of backup ISP connection

**CRITICAL:**

Should be corrected immediately, but indicates failure in a primary system - fix CRITICAL problems before ALERT - example is loss of primary ISP connection

**EMERGENCY:**

A "panic" condition - notify all tech staff on call? (earthquake? tornado?) - affects multiple apps/servers/sites...

---

**Syslog Priority values**

Each Syslog message includes a priority value at the beginning of the text. The priority value ranges from 0 to 191 and is made up of a Facility value and a Level value. The priority is enclosed in "<>" delimiters.
A BSD Unix Syslog message looks like this: <pri>HEADER MESSAGE</pri>

The priority is a value from 0 to 191 and is not space or leading zero padded.

For more information on the Syslog message format, please read the RFC.

The priority value is calculated using the following formula:

Priority = Facility * 8 + Level

To manually set a particular priority number, enter a number into the Priority value field and check the 'Use this value' box. This value will be sent in the <pri> field of the Syslog message. This allows you to use values above 191 (up to 255). Values above 191 are illegal and could cause unknown results.</pri>

**Transport**

Kiwi Syslog Server can listen for UDP messages and TCP messages. Normally Syslog messages are sent using UDP. Some networking devices such as the Cisco PIX firewall can send messages using TCP to ensure each packet is received and acknowledged by the Syslog Server.

When sending messages using UDP the destination port is usually 514

When sending messages using TCP the destination port is usually 1468

Ports used by Kiwi Syslog Server are documented here.

**Syslog RFC 3164 header format**

The HEADER part contains a timestamp and an indication of the hostname or IP address of the device. The HEADER contains two fields called the TIMESTAMP and the HOSTNAME.

The TIMESTAMP will immediately follow the trailing “>” from the PRI part and single space characters MUST follow each of the TIMESTAMP and HOSTNAME fields.

HOSTNAME will contain the hostname, as it knows itself. If it does not have a hostname, then it will contain its own IP address.

The TIMESTAMP field is the local time and is in the format of: "Mmm dd hh:mm:ss" (without the quote marks).

The MSG part has two fields known as the TAG field and the CONTENT field. The value in the TAG field will be the name of the program or process that generated the message. The CONTENT contains the details of the message. This has traditionally been a freeform message that gives some detailed information of the event. The TAG is a string of ABNF alphanumeric characters that MUST NOT exceed 32 characters. Any non-alphanumeric character will terminate the TAG field and will be assumed to be the starting character of the CONTENT field. Most commonly, the first character
of the CONTENT field that signifies the conclusion of the TAG field has been seen to be the left square bracket character ("[") , a colon character (":"), or a space character

Kiwi SyslogGen uses the following format for its messages:

<pri>Jul 10 12:00:00 192.168.1.1 SyslogGen MESSAGE TEXT</pri>

The BSD Syslog protocol is discussed in RFC 3164. Check out their community discussion on Roxen website.

For a comprehensive description of the syslog protocol, see Sans Institute website.