APNIC 44

Syslog and RSyslog

TAICHUNG, TAIWAN
7-14 September 2017

#apnic44

What is Syslog?

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is label with a facility code, indicating the software type generating the message, and assigned a serverity level.

A variety devices can generate the standard log message across platform such as router, switch, printer, computer etc.,

Syslog components

- Facility
- Severity
- Timestamp
- Host
- Tag
- Message

Facility

A facility code is used to specify the type of program that is logging the message.

Messages with different facilities may be handled differently. The list of facilities available is defined by RFC 3164

Facility Table (RFC3164)

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

Severity Level (RFC5424)

Value	Severity	Keyword	Deprecated keywords	Description
0	Emergency	emerg	panic	System is unusable. A panic condition.
1	Alert	alert		Action must be taken immediately. A condition that should be corrected immediately, such as a corrupted system database.
2	Critical	crit		Critical conditions, such as hard device errors.
3	Error	err	error	Error conditions.
4	Warning	warning	warn	Warning conditions.
5	Notice	notice		Normal but significant conditions. Conditions that are not error conditions, but that may require special handling.
6	Informational	info		Informational messages.
7	Debug	debug		Debug-level messages. Messages that contain information normally of use only when debugging a program.

Timestamp

- If present, most often a timestamp with just the date and day of month, hour, minutes and seconds
- Most often no time zone, year or better-than second resolution
- Often wrong! ... due to out-of-sync internal device clocks (e.g. clock always starts at Jan, 1st 1997 after power up)

  – If supported (by device), plan for NTP or similar mechanism to solve this.

- Improved in upcoming standards

Host

- Name or IP-Address of the sender
- Sometimes missing, sometimes present, sometimes meaningless or invalid (depending on configuration)
- Often duplicate if multiple networks are being monitored (e.g. a service provider monitoring customer networks)
- Intention is to provide the name of the original sender when passing through syslog relays.

Message and Tag

From RFC 3164, the message component (known as MSG) was specified as having these fields: TAG, which should be the name of the program or process that generated the message, and CONTENT which contains the details of the message.

Described in RFC 5424 (March 2009), "MSG is what was called CONTENT in RFC 3164". This RFC states: “The TAG is now part of the header, but not as a single field. The TAG has been split into APP-NAME, PROCID, and MSGID. This does not totally resemble the usage of TAG, but provides the same functionality for most of the cases”.

What is syslog being used for?

- Troubleshooting Routers/Firewalls/Devices
  - during installation
  - in problem situations
- Intrusion Detection
- Operations Management
- Long Term Auditing
- Tracking user and admin activity

Syslog role

- Device – generates message
- Collector – receives and optionally stores messages commonly known as syslog daemon or server.
- Relay – receives and forwards message
- Sender – anyone who sends syslog messages (device & relay)
- Receiver – anyone who receives syslog messages (relay & collector)

Log Management

- Keep your logs in a secure place where they can be easily inspected
- Watch your log files
- They contain important information:

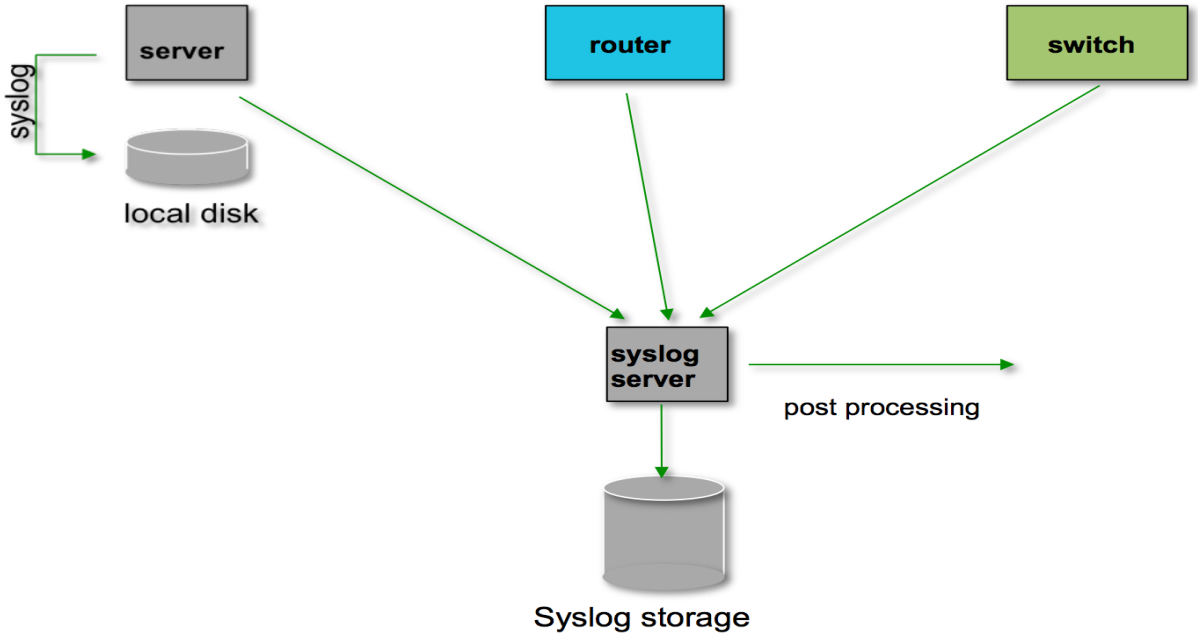
  - Lots of things happen and someone needs to review them

  - It’s not practical to do this manually.

Log Management

- Centralize and consolidate log files
- Send all log messages from your routers, switches and servers to a single node – a log server.
- All network hardware and UNIX/Linux servers can be monitored using some version of syslog
- Windows can, also, use syslog with extra tools.
- Save a copy of the logs locally, but, also, save them to a central log server.

Centralize log



Rsyslog

- Rsyslog is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. It implements the basic syslog protocol, extends it with content-based filtering, rich filtering capabilities, flexible configuration options and adds features such as using TCP for transport.
- The official RSYSLOG website defines the utility as **"the rocket-fast system for log processing"**

Rsyslog

Rsyslog is a drop-in replacement for regular syslog. It adds a bunch of features:

- Better security controls
- More filtering options/syntax
- More reliable transport mechanisms
- Writing to databases

Rsyslog Protocol

- Rsyslog uses the standard BSD syslog protocol, specified in RFC 3164 (RFC 5424).
- Rsyslog supports many of these extensions. The format of relayed messages can be customized.

The most important extensions of the original protocol supported by rsyslog are:

- ISO 8601 timestamp with millisecond granularity and timezone information
- The addition of the name of relays in the host fields to make it possible to track the path a given message has traversed
- Reliable transport using TCP
- Support GSS-API and TLS - Generic Security Services Application Program Interface
- Logging directly into various database engines.
- Support for RELP - Reliable Event Logging Protocol
- Support for buffered operation modes where messages are buffered locally if the receiver is not ready
- Complete input/output support for systemd journal

APNIC 44

#apnic44

TAICHUNG, TAIWAN

7–14 September 2017