Contribution ID: **6** Type: **not specified**

Flexible, scalable and secure logging using syslog-ng

Thursday 27 April 2017 16:40 (25 minutes)

Event logging is a central source of information for IT.
The syslog-ng application collects logs from many different
sources, performs real-time log analysis by processing and filtering them,
and finally it stores the logs or routes them for further analysis.

In an ideal world, all log messages come in a structured format, ready to
be used for log analysis, alerting or dashboards. But in a real world only
part of the logs belong to this category. Traditionally, most of the log
messages come as free format text messages. These are easy to be read by
humans, which was the original use of log messages. However, today logs are
rarely processed by the human eye. Fortunately syslog-ng has several tools
to turn unstructured and many of the structured message formats into
name-value pairs, and thus delivers the benefits of structured log messages.

Once you have name-value pairs, log messages can be further enriched with
additional information in real-time, which helps responding to security incidents
in due time. One way is adding geo-location based on IP addresses.
Another way is adding contextual data from external files, like the role of
a server based on the IP address or the role of the user based on the name.
Data from external files can also be used to filter messages, for example
to check firewall logs to determine whether certain IP addresses are
contained in various black lists for malware command centers, spammers, and
so on.

Logging is subject to an increasing number of compliance regulations.
PCI-DSS or many European privacy laws require removing sensitive data from
log messages. I will demonstrate how logs can be anonymized in a way that
they are still useful for security analitics.

At the end I would like to introduce you to the basics of syslog-ng
configuration, and demonstrate how the collected logs can be used for
alerting or visualized on a dashboard.

Length of talk (minutes)

20

Scheduling constraints / preferences

This talk would be best scheduled just before Fabien Wernli's talk on syslog-ng viewed from a Tier-1' perspective

Author: Mr CZANIK, Péter (Balabit)

Presenter: Mr CZANIK, Péter (Balabit)

Session Classification: Basic IT services

Track Classification: Basic IT Services