Contribution ID: **2** Type: **not specified**

Typical syslog-ng use-cases at our Tier-1

Thursday, 27 April 2017 17:05 (25 minutes)

We present the log infrastructure at CCIN2P3 and illustrate how syslog-ng plays a central part in it.
Following up on Balabit's talk on syslog-ng's features, we present several use-cases which are likely to be of interest to the HEPiX community.
For instance, we present real-life examples on how to parse and correlate operating system and batch scheduler events.
We present its integration with common alerting backends like Nagios, as well as modern indexing solutions like Elasticsearch, Kibana and Riemann.
Moreover, in order to emphasize the software's high order of flexibility and upgradability, we provide some feedback from our interaction with the core developers.
We finally present our past and present code contributions to the syslog-ng codebase, and our plans for the logging infrastructure's future.

Length of talk (minutes)

20

Scheduling constraints / preferences

Would like to add this talk right after Péter Czanik's (Balabit).
Péter's talk is a general overview of the software's features, and mine shows more specific use-cases in our Tier-1.

Primary author: WERNLI, Fabien (CCIN2P3)

Presenter: WERNLI, Fabien (CCIN2P3)

Session Classification: Basic IT services

Track Classification: Basic IT Services