ID de Contribution: **8** Type: **Présentation longue**

Architecture de gestion des événements (journaux) au CCIN2P3

jeudi 8 octobre 2015 15:10 (30 minutes)

Nous présentons la nouvelle architecture de gestion des événements (”logs”) au Centre de Calcul. Chaque jour, plus de 100 millions de messages sont générés par les composants logiciels et matériels au CCIN2P3. Ils sont conservés pendant un an, et outre leur valeur légale, ils représentent une source d'informations cruciale pour la gestion quotidienne de nos infrastructures. La nouvelle plateforme est basée sur les logiciels libres collectd, syslog-ng, Elasticsearch, Riemann, et pilotée par puppet. Nous présentons chacun d'entre eux, avec leur place dans le système. Plusieurs fonctionnalités sont abordées:

- Identifier, classifier et structurer
- Établir des corrélations
- Router
- Visualiser les événements en temps-réel dans un navigateur web
- Émettre des alertes asychrones p. ex. dans Nagios
- Enregistrer et archiver les données sur disque
- Exposer une API riche permettant de déposer des requêtes complexes
- Explorer visuellement les journeaux

Une démonstration de ces différents outils est effectuée tout au long de la présentation.

Auteur principal: WERNLI, Fabien (CC-IN2P3)

Orateur: WERNLI, Fabien (CC-IN2P3)

Classification de Session: ASR présentations ciblées 2

Classification de thématique: ASR